The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 10.0

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo, ActiveAdmin, BindView, bv-Control, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

**Licensing and registration**

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

**Customer service**

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan  
customercare_apac@symantec.com
Europe, Middle-East, and Africa  
semea@symantec.com
North America and Latin America  
supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services  
Managed Services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services  
Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.

Education Services  
Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.
## Technical Support

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Introducing Control Compliance Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About the Control Compliance Suite</td>
</tr>
<tr>
<td></td>
<td>What Control Compliance Suite can do for you</td>
</tr>
<tr>
<td></td>
<td>How Control Compliance Suite works</td>
</tr>
<tr>
<td></td>
<td>Control Compliance Suite server components</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Application Server</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Directory Server</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Directory</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Data Processing Service</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite production database</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite reporting database</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite evidence database</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Web Console server</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Encryption Management Service</td>
</tr>
<tr>
<td></td>
<td>Control Compliance Suite client software</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Console</td>
</tr>
<tr>
<td></td>
<td>About the Control Compliance Suite Web Console</td>
</tr>
<tr>
<td></td>
<td>About accessing the Control Compliance Suite Web Console</td>
</tr>
<tr>
<td></td>
<td>Control Compliance Suite infrastructure requirements</td>
</tr>
<tr>
<td></td>
<td>Control Compliance Suite server requirements</td>
</tr>
<tr>
<td></td>
<td>Control Compliance Suite Client requirements</td>
</tr>
<tr>
<td></td>
<td>Where to get more information</td>
</tr>
<tr>
<td></td>
<td>Where to get Symantec Enterprise Security Manager information</td>
</tr>
<tr>
<td></td>
<td>Where to get Response Assessment module information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Using the Control Compliance Suite Console</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About the console features</td>
</tr>
<tr>
<td></td>
<td>About the menu bar</td>
</tr>
<tr>
<td></td>
<td>About the tree pane</td>
</tr>
<tr>
<td></td>
<td>About the Filter by pane</td>
</tr>
</tbody>
</table>
Deleting user accounts .......................................................... 184
Updating user accounts .......................................................... 185
Configuring the SQL Server settings ............................................. 185
Configuring the production database connection settings ............ 186
Configuring the reporting database connection .......................... 187
Configuring the application server credentials .......................... 189
Configuring service accounts with unconstrained delegation ......... 189
Configuring the S4U and constrained delegation ......................... 190
About using special characters in credentials ............................ 191
Updating Control Compliance Suite ........................................... 192
How LiveUpdate works in Control Compliance Suite .................... 193
About the LiveUpdate view ...................................................... 194
Enabling and scheduling LiveUpdate ........................................ 194
About the host file for Windows LiveUpdate clients .................... 195
About the LiveUpdate staging location ..................................... 195
Performing LiveUpdate on demand .......................................... 196
Configuring Response Assessment Module in Control Compliance
Suite .......................................................... 196
About Response Assessment Module ....................................... 199
Adding a link to Control Compliance Suite .............................. 201
Adding a Response Assessment Module user-defined property .... 201
Publishing a questionnaire with invitations in Response Assessment Module ...................................................... 202
About configuring the Web Console to contact RAM .................. 203
About logs and configuration files .......................................... 204
About log messages ...................................................... 206
About log levels ...................................................... 206

Chapter 4 Performing the IT governance tasks with Control
Compliance Suite ...................................................... 209
Preparing for risk assessment .............................................. 209
Assessing the compliance and the risk posture of the system ........ 214
Simplifying the remediation process ...................................... 218
Identifying possible threats in the access control system ............ 219

Chapter 5 Managing assets ...................................................... 225
Getting started with the asset system ...................................... 225
About the Asset System view .......................................... 228
About the Reconciliation Rules view .................................. 230
Concepts in assets ...................................................... 232
Contents

About assets ........................................................................ 233
Site as scope in asset import ................................................... 234
Asset folder hierarchy ........................................................... 234
Predefined platforms ............................................................ 235
Asset types .......................................................................... 235
Primary and secondary assets ................................................. 275
Reconciliation rules and rule types .......................................... 276
Asset import ........................................................................ 288
Asset tagging ....................................................................... 296
Asset groups ........................................................................ 296
Active assets ........................................................................ 306
Creating reconciliation rules ........................................................ 306
Creating reconciliation rules without manual review ................... 306
Creating reconciliation rules using the manual review ................. 307
Working with reconciliation rules scenarios .............................. 308
Importing assets ........................................................................ 313
About the first time asset import ............................................. 316
Importing the assets for the first time ...................................... 319
Working with asset import scenarios ....................................... 321
Importing assets from a CSV file ............................................. 353
Importing assets from an ODBC database table .......................... 362
Reviewing the assets manually ................................................ 367
Creating asset groups ............................................................ 369
Creating a dynamic asset group .............................................. 370
Creating a static asset group ................................................... 372
Deleting inactive assets using the asset groups .......................... 373
Operators ( , ), AND, OR .......................................................... 374
Performing the tasks in the Asset System view ................................ 375
Creating the asset folders ....................................................... 375
Performing the asset group tasks ............................................ 376
Performing the global tasks .................................................... 377
Performing the asset tasks ..................................................... 391
Performing the common tasks ................................................ 393
Viewing asset information in the details pane ............................ 394
Using the Filter by pane in the Asset System view ...................... 402
Performing the tasks in the Reconciliation Rules view ....................... 404
Editing a reconciliation rule ................................................... 405
Moving a reconciliation rule .................................................. 405
Copying and pasting a reconciliation rule .................................. 406
Deleting a reconciliation rule ................................................ 406
Viewing rules information in the details pane ............................ 406
Marking a rule as default ...................................................... 406
Unmarking a rule as default .................................................. 407
Chapter 6  Importing assets from Altiris ................................. 411
   About importing assets from Altiris .................................... 411
   Supported asset types for Altiris ......................................... 412
   Prerequisites for installing Control Compliance Suite Asset Export
      Task .................................................................................. 413
   Installing Asset Export Task on Altiris Notification Server .......... 413
   Working with the Altiris Asset Export Task solution .................. 414
   Creating the Altiris asset import jobs in Control Compliance Suite
      Console .............................................................................. 415
   Specifying the asset export settings in the Altiris Symantec
      Management Console .......................................................... 416
   Creating a asset export task in the Altiris Symantec Management
      Console .............................................................................. 417
   Scheduling asset export task in the Altiris Symantec Management
      Console .............................................................................. 418
   About the CSV files on Altiris Notification Server ..................... 419

Chapter 7  Importing incident data from Symantec Data Loss
            Prevention ................................................................. 421
   About importing incident data from Symantec Data Loss
      Prevention .......................................................................... 421
   About the Symantec Data Loss Prevention Connector ............... 422
   Roles and permissions for the Symantec Data Loss Prevention
      Connector .............................................................................. 422
   Configuring the Symantec Data Loss Prevention Connector ........ 423
   Installing a certificate for the Symantec Data Loss Prevention
      Connector .............................................................................. 427
   About Symantec Data Loss Prevention Connector email
      notification configurations and logging ................................. 428
   Symantec Data Loss Prevention Connector incident data batch
      size ...................................................................................... 429
   Scheduled task configurations for Symantec Data Loss Prevention
      Connector incident data collection ...................................... 430
   About Symantec Data Loss Prevention and Control Compliance
      Suite result mapping ............................................................ 430
   About the Symantec Data Loss Prevention Connector incident
      and Control Compliance Suite asset mapping ...................... 431
   About rules-based action execution ......................................... 432
   About predefined rules-based actions ..................................... 433
   About custom rules-based actions ......................................... 436
Chapter 8  Managing custom schema ......................................................... 443

About the custom schema ........................................................................ 443
  About the Schema Manager view .......................................................... 444
  About the asset type schema ............................................................... 444
  About the entity schema ..................................................................... 445
  About the target type schema .............................................................. 445

Working with custom asset types ............................................................. 446
  Creating a new asset type .................................................................. 446
  Registering a platform ...................................................................... 448
  Importing an asset type ..................................................................... 449
  Exporting an asset type ..................................................................... 450
  Viewing the custom asset type and the custom fields in the asset system .................................................................................. 450
  Extending an existing asset type ........................................................ 451
  Editing an existing asset type ............................................................. 452
  Creating an external field to add to the asset type .............................. 453
  About the predefined platforms and the primary entities ................. 454
  About the primary, mandatory, and optional fields ......................... 454
  About referenced entity fields ............................................................ 454
  About separators in name fields ......................................................... 455

Working with custom entity ................................................................ 456
  About platforms ................................................................................. 456
  About entities ..................................................................................... 457
  About fields of an entity .................................................................... 457
  About setting tasks to roles for entity schema ................................... 458
  About relationships between the predefined entities ....................... 458
  Creating a new entity schema ............................................................ 461
  Editing an existing entity schema ........................................................ 465

Working with custom target type ........................................................... 466
  Creating a new target type ................................................................. 466
  Editing a target type ......................................................................... 467

Working with custom schema scenarios .............................................. 468
  Creating a custom asset type - Windows Service ............................... 469
  Extending the predefined asset type - Windows Machine ................. 471
Chapter 10  Managing exceptions ........................................................... 529

Concepts in exception ................................................................. 529
  About exceptions .................................................................. 530
  About the exception management system ................................ 530
  About exception validity .................................................... 531
  About exception templates .................................................. 532
  About exception states ....................................................... 533
  About the exception filters ................................................ 534
About the Exceptions view ......................................................... 535

Working with exceptions ............................................................. 535
  Viewing exception information in the details pane ................. 535
  Requesting an exception ..................................................... 538
  Launching the Request Exception Wizard ............................... 541
  Approving an exception ...................................................... 542
  Setting the exception state to In Review ............................... 545
  Setting the exception state to Request Clarification ............... 545
  Setting the exception state to Deny ..................................... 546
  Setting the exception state to Expire .................................... 546
Chapter 11  Managing standards .......................................................... 549

- Concepts in standards management .................................................. 549
  - About standards ................................................................. 550
  - About predefined standards .................................................. 550
  - About sections ................................................................. 556
  - About checks .................................................................. 556
  - About data collection jobs ................................................... 556
  - About advanced options for data collection ............................ 557
  - About evaluation jobs ........................................................ 557
  - About target types ............................................................ 558
  - About compliance score ..................................................... 569
  - About risk score ................................................................ 569
  - About versioning scheme .................................................... 569
  - About the standards filters .................................................. 571
  - About policy mapping in ESM .............................................. 571
  - About changing an ESM policy name .................................... 572
  - List of standards ............................................................... 572

- Concepts in checks ........................................................................ 579
  - Field expression ................................................................... 580
  - Check expression .................................................................. 581
  - Check formula ...................................................................... 581
  - Preconditions ....................................................................... 582
  - Data Items filter .................................................................. 582
  - Missing data items ............................................................. 583
  - Multiple data items ............................................................... 583
  - Check risk attributes .......................................................... 584
  - Check Advanced Settings ...................................................... 587
  - About operators ................................................................... 590

- About the Standards view ............................................................... 595
- About the standard migration utility for ESM and CCS .................. 597

- Working with standards .............................................................. 598
  - Viewing standard information in the details pane .................. 598
  - About multi-select functionality ........................................... 602
  - Creating a new standard ..................................................... 603
  - Copying and pasting a standard .......................................... 603
  - Moving a standard ........................................................... 604
  - Importing a standard .......................................................... 605
  - Exporting a standard .......................................................... 605
  - Renaming a standard ......................................................... 606
  - Deleting a standard ........................................................... 606
Running an evaluation job from the Standards view ................. 607
Setting up a data collection job from the Standards view .......... 609
Running a collection-evaluation-reporting job from the Standards
view ................................................................................... 612
Sizing guidelines for Collection-Evaluation-Reporting job ......... 617
Changing an ESM policy name at the standard level ............... 618

Working with sections ......................................................... 618
Viewing section information in the details pane .................... 619
Creating a new section ......................................................... 621
Copying and pasting a section ............................................. 621
Moving a section ............................................................... 622
Renaming a section .......................................................... 623
Deleting a section ............................................................ 623
Changing an ESM policy name at the section level ............... 623

Working with checks ........................................................... 624
Viewing check information in the details pane ..................... 624
Copying and pasting a check ................................................. 631
Moving a check ............................................................... 632
Renaming a check ............................................................ 632
Deleting a check ............................................................. 633
Creating a new check ......................................................... 633
Editing a check ............................................................... 636
Changing an ESM policy name at the check level ............... 637
Creating an ESM check ....................................................... 638

Working in the details pane .................................................. 648
Specifying or editing the description ..................................... 649
Specifying or editing the check issue .................................... 649
Specifying or editing the remediation information ............... 650
Adding the CVE information ............................................. 650
Editing the CVE information .............................................. 651
Specifying or editing the check attributes ......................... 651
Adding reference information ......................................... 651
Editing reference information ........................................... 652
Deleting reference information ......................................... 653

Working with Evaluation Results .......................................... 653
About exporting the evaluation results ............................... 654
Exporting the evaluation results ....................................... 655
Requesting an exception using the Evaluation Result Details
dialog box ................................................................. 656
Viewing the evidence details ............................................ 657

About risk score calculation ............................................... 658
Base score calculation ....................................................... 658
Adjusted base score calculation ........................................ 658
Chapter 12 Remediating assets ................................................................. 661
  About remediation ........................................................................... 661
  About automatic remediation ....................................................... 662
  About manual remediation ........................................................... 663
  About closed-loop verification ...................................................... 664
  Remediating the assets manually from the evaluation results .......... 665
  Remediating the assets automatically ............................................ 667

Chapter 13 Managing baselines ............................................................ 669
  About baseline .............................................................................. 669
  About the baselines workflow ....................................................... 670
  About the Baselines view ............................................................. 671
  About setting tasks to roles of baselines ........................................ 671
  Creating a baseline job ................................................................. 672
  Viewing the comparison results in the Baselines view ....................... 673
  Exporting the comparison results .................................................. 674
  Deleting the baseline record ......................................................... 675

Chapter 14 Managing tags ................................................................. 677
  About tags ................................................................................. 677
  About the Tags view ...................................................................... 678
  Creating a new tag ...................................................................... 678
  Creating a new tag category .......................................................... 678
  Editing a tag category .................................................................. 679
  Deleting a tag category ................................................................ 679
  Moving a tag .............................................................................. 680
  Deleting a tag ............................................................................ 680
  Renaming a tag .......................................................................... 680

Chapter 15 Managing policies ............................................................ 683
  About policies .............................................................................. 683
  About the policy life cycle ........................................................... 684
  About policy versioning .............................................................. 684
  About policy status ...................................................................... 685
  About editing policies .................................................................. 687
  What is a control statement? ......................................................... 687
  About mapping policies ............................................................ 688
About policy reviewers .......................................................... 688
About policy approvers .......................................................... 688
About the policy audience ...................................................... 688
About selecting the policy audience ......................................... 689
About audience interaction with policies .................................. 690
About the Policies view .......................................................... 690
Working with policies ............................................................. 693
  Creating a new policy ........................................................ 693
  Importing a Word policy ...................................................... 695
  Editing a policy .............................................................. 696
  Deleting a policy ............................................................ 697
  Moving, copying, and pasting a policy .................................. 698
  Submitting a policy for review ............................................. 698
  Submitting a policy for approval ........................................... 699
Reviewing and approving policies ............................................. 700
  About policy review ........................................................ 700
  Reviewing a policy ........................................................... 701
  Viewing the reviewer comments ........................................ 702
  About policy approval ........................................................ 702
  Approving a policy ............................................................ 703
Publishing and unpublishing policies ........................................ 704
  Publishing a policy ........................................................... 704
  Unpublishing a policy ........................................................ 705
How audiences interact with policies ........................................ 706
Managing clarifications ........................................................... 706
  About clarifications .......................................................... 706
  About the Clarifications view .............................................. 707
  Managing clarification requests ......................................... 708

Chapter 16 Monitoring jobs ........................................................... 711
About jobs ................................................................. 711
  About the job types ........................................................ 712
  About the job filters ........................................................ 714
  About the Jobs view ........................................................ 715
Managing jobs ................................................................. 716
  Editing a job .............................................................. 717
  Scheduling jobs ............................................................ 718
  Deleting jobs ............................................................... 718
  Running a job now .......................................................... 719
  Searching for a job .......................................................... 720
  Refreshing the jobs view ................................................... 720
  Creating jobs .............................................................. 721
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing job runs</td>
<td>722</td>
</tr>
<tr>
<td>Canceling a job run</td>
<td>722</td>
</tr>
<tr>
<td>Deleting a job run</td>
<td>723</td>
</tr>
<tr>
<td>Viewing jobs information in the details pane</td>
<td>724</td>
</tr>
<tr>
<td>Jobs details pane- General tab</td>
<td>724</td>
</tr>
<tr>
<td>Jobs details pane- Schedule tab</td>
<td>725</td>
</tr>
<tr>
<td>Jobs details pane - Wizard Summary</td>
<td>725</td>
</tr>
<tr>
<td>Job run details pane- Summary tab</td>
<td>725</td>
</tr>
<tr>
<td>Job run details pane- Failures tab</td>
<td>725</td>
</tr>
<tr>
<td>Jobs details pane- Template tab</td>
<td>725</td>
</tr>
<tr>
<td>Chapter 17 Monitoring evaluation results</td>
<td>727</td>
</tr>
<tr>
<td>About the Evaluation Results view</td>
<td>727</td>
</tr>
<tr>
<td>About the evaluation result filters</td>
<td>728</td>
</tr>
<tr>
<td>Viewing evaluation jobs in the details pane</td>
<td>728</td>
</tr>
<tr>
<td>Evaluation Results details pane - General tab</td>
<td>729</td>
</tr>
<tr>
<td>Evaluation Results details pane - Evaluation Summary tab</td>
<td>729</td>
</tr>
<tr>
<td>Evaluation Results details pane - Assets Evaluated tab</td>
<td>729</td>
</tr>
<tr>
<td>Chapter 18 Managing reports and dashboards</td>
<td>731</td>
</tr>
<tr>
<td>About the reports and dashboards</td>
<td>731</td>
</tr>
<tr>
<td>About the Reports Templates view</td>
<td>732</td>
</tr>
<tr>
<td>About the My Reports view</td>
<td>733</td>
</tr>
<tr>
<td>About the My Dashboards view</td>
<td>734</td>
</tr>
<tr>
<td>About types of dashboards</td>
<td>736</td>
</tr>
<tr>
<td>About predefined report templates</td>
<td>737</td>
</tr>
<tr>
<td>About data synchronization</td>
<td>737</td>
</tr>
<tr>
<td>About creating user-defined templates</td>
<td>737</td>
</tr>
<tr>
<td>About the prerequisites for user-defined report templates</td>
<td>738</td>
</tr>
<tr>
<td>About the Report Management jobs</td>
<td>741</td>
</tr>
<tr>
<td>About the View My Reports filter option</td>
<td>741</td>
</tr>
<tr>
<td>Predefined report descriptions</td>
<td>741</td>
</tr>
<tr>
<td>Working with reports</td>
<td>745</td>
</tr>
<tr>
<td>Scheduling a report</td>
<td>746</td>
</tr>
<tr>
<td>Viewing a report</td>
<td>747</td>
</tr>
<tr>
<td>Refreshing a report</td>
<td>748</td>
</tr>
<tr>
<td>Removing a report</td>
<td>748</td>
</tr>
<tr>
<td>Printing a report</td>
<td>748</td>
</tr>
<tr>
<td>Exporting a report</td>
<td>749</td>
</tr>
<tr>
<td>Copying a report template</td>
<td>750</td>
</tr>
<tr>
<td>Customizing a report template</td>
<td>750</td>
</tr>
<tr>
<td>Customizing a report in report viewer</td>
<td>751</td>
</tr>
</tbody>
</table>
About evidence ................................................................. 814
About methods to import the extended controls ................. 815
About methods to import the evidence .................. 815
About compliance score contribution from an evidence
source ................................................................. 816
About risk score contribution from an evidence source ........ 817
About compliance score calculation from evidence .......... 818
About risk score calculation from evidence ..................... 818
End-to-end sequence of evidence import ..................... 819
Working with evidence sources ........................................ 821
Adding an evidence source ............................................ 822
Editing an evidence source ............................................ 824
Deleting an evidence source .......................................... 824
Working with extended controls .................................... 825
Adding an extended control .......................................... 826
About CSV file format for extended controls ................. 826
Importing extended controls from a CSV file ............... 830
Editing an extended control .......................................... 831
Deleting an extended control ........................................ 831
Working with evidence .................................................... 832
Setting tasks to roles for evidence collection ................. 833
About CSV file format for evidence ...................... 833
About evidence field format for predefined asset types ...... 839
About ODBC mappings for evidence ......................... 844
Importing evidence from CSV files or ODBC compliant
databases ......................................................... 849
Importing evidence from Response Assessment Module ..... 850
Mapping custom questionnaires to evidence ................. 851
Viewing the imported evidence .................................. 853

Chapter 21  Understanding the integration services APIs ......... 855
About the integration interfaces ...................................... 855
Control Compliance Suite APIs .................................. 855

Chapter 22  Migration utilities ............................................. 859
About the Standard Migration Utility ............................... 859
About the Standard Migration Utility system requirements .... 860
About the Standard Migration Utility packaging and
deployment ......................................................... 861
Standard Migration Utility ........................................... 861
How to use the Standard Migration Utility .................... 863
About the log file configuration settings ........................ 864
Appendix B  Troubleshooting ................................................................. 901
About troubleshooting ......................................................................... 901
Deployment troubleshooting ............................................................ 902
  Troubleshooting a failed Directory Server Installation ................ 903
  Troubleshooting when the Certificate does not match a specified
  computer during deployment ...................................................... 903
  Troubleshooting when the Application Server installation wizard
  rejects the Directory Server credentials .................................... 904
  Troubleshooting when the Application Server, Directory Server,
  or Data Processing Service fail to start ..................................... 904
  Troubleshooting when installation logs are deleted when the
  user logs off after using Remote Desktop Connection to
  install .................................................................................... 905
  Troubleshooting when an error message that indicates that the
  state of the secure channel cannot be verified appears during
  installation ............................................................................. 906
  Troubleshooting when an error message indicates the SSPI
  context cannot be generated during installation ..................... 906
  Troubleshooting when you encounter problems installing the
  Control Compliance Suite Console ........................................... 906
  Troubleshooting when a warning appears about the minimum
  required screen resolution ........................................................ 906
Configuration troubleshooting ......................................................... 907
  Troubleshooting when the user is unable to start the Certificate
  Management Console .............................................................. 907
  Troubleshooting when synchronization jobs fail to complete
  after migration ........................................................................ 907
Asset import troubleshooting .......................................................... 908
  Troubleshooting when asset imports fail to complete ................ 908
  Troubleshooting when asset import jobs from a single site run
  slowly .................................................................................... 909
  Troubleshooting when asset import jobs fail and report an
  exception ................................................................................ 909
  Troubleshooting when deleted ODBC data locations appear in
  the Data Processing Service settings ....................................... 910
Data collection troubleshooting ....................................................... 910
  Troubleshooting when data collection jobs fail to run ................ 911
  Troubleshooting when data collection jobs from a single site run
  slowly .................................................................................... 911
  Troubleshooting when an exception appears during data
  collection for Oracle assets ...................................................... 912
Troubleshooting when data collection jobs fail with the error
  Login failed for user ................................................................. 912
Troubleshooting when data collection jobs fail with an exception .................................................. 912
Troubleshooting when “Computer Unreachable” errors appear for Windows computers that do not have Internet Information Services installed .............................................. 913
Console and Web Console troubleshooting ........................................................... 913
Troubleshooting when the user cannot start the Control Compliance Suite Console ........................................ 915
Troubleshooting when the Web Console is unable to connect to the Response Assessment module ........................................ 916
Troubleshooting when the Web Console does not correctly display Response Assessment module pages .......................................................... 916
Troubleshooting when configuration changes do not appear .......................................................... 916
Troubleshooting when the correct time does not appear on reports ................................................ 916
Troubleshooting when reports cause a system slowdown or reports fail ........................................... 917
Troubleshooting when the error HTTP Error 401.1 - Unauthorized: Access is denied appears when you open the Web Console ................................................................. 917
Troubleshooting when blank reports appear .......... 917
Troubleshooting when an error appears while viewing a dashboard on the Web Console ....................... 918
Troubleshooting when you cannot create a custom asset type .............................................................. 918
Troubleshooting when the message “The server is not operational” appears in the console ....................... 918
Troubleshooting when the message “Login failed for user <user name>” appears in the Web console ........................................................................ 919
Troubleshooting when -1 value is displayed in a chart for an asset risk score ........................................ 919
Troubleshooting when an error message appears while navigating to the Policies page in the Web console ........................................................................ 920
Troubleshooting when the dashboard panel data is incorrect .................................................................... 920
Troubleshooting when expected data is not displayed in the policy panels ............................................. 920
Troubleshooting when launching the Control Compliance Suite Console is slow ....................................... 921
Troubleshooting when an error message appears on the Control Compliance Suite console or in the logs of DPS .............................. 921
Troubleshooting when there is a delay in permission changes in the Web Console ........................................................................ 922
Troubleshooting when the Web console does not start after upgrading to version 10.0 ................................................................ 922
Policy Module troubleshooting ................................................................................................................................. 922
Troubleshooting when you cannot assign a reviewer or approver for a policy ................................................................. 923
Symantec ESM troubleshooting ......................................................................................................................................... 923
Troubleshooting when you cannot classify ESM 6.0 agents as different UNIX computers .............................................................. 923
Reports troubleshooting ................................................................................................................................. 924
Troubleshooting a failed report generation job for an Entitlements Management report ......................................................... 924
Troubleshooting performance slowdown in execution of report generation jobs ................................................................. 925
Troubleshooting an error "XML document could not be created because server memory is very low" appears in a reporting database synchronization job ...................................................................................... 925
Evidence import troubleshooting ......................................................................................................................................... 926
Troubleshooting when Evidence collection job fails to run .......................................................................................... 926
Troubleshooting when score contribution from an evidence source is not displayed in the Asset Details pane .................. 926

Glossary terms ......................................................................................................................................................................... 929

Index ..................................................................................................................................................................................... 935
Introducing Control Compliance Suite

This chapter includes the following topics:

- About the Control Compliance Suite
- What Control Compliance Suite can do for you
- How Control Compliance Suite works
- Control Compliance Suite server components
- Control Compliance Suite client software
- Control Compliance Suite infrastructure requirements
- Where to get more information

About the Control Compliance Suite

The Control Compliance Suite (CCS) automates key IT risk and compliance management tasks. The CCS ensures the coverage of external mandates through written policy creation, dissemination, acceptance logs, and exception management. CCS demonstrates compliance to both external regulatory mandates and internal policies. The CCS allows customers to link the written policy to specific technical and procedural standards. Customers can assess those policies using a highly scalable agentless or agent-based tool. The CCS scores assessment results against specified risk criteria. The CCS supports automated assessment of the system security configuration, permissions, patches, and vulnerabilities. The CCS includes system reporting capabilities. CCS also supports the assessment of procedural controls and entitlement review through a manual attestation process.
What Control Compliance Suite can do for you

The Control Compliance Suite (CCS) is an IT risk and compliance management solution.

CCS provides a comprehensive framework that allows customers to do the following:

- Lower the cost of risk and compliance posture assessment.
- Use automated agentless or agent-based capabilities to audit and scan technical controls.
- Provide an ability to attest procedural controls.
- Identify problems with system configuration or internal controls.
- Guard against policy compliance failure or data breach.
- Define, review, and disseminate written policies to end-users as mapped to specific, measurable controls.
- Determine coverage gaps for multiple, overlapped regulatory, industry-specific, or best practices frameworks.
- Produce evidence of due care in an IT audit process.
- Simplify the remediation process.
- Pull in third-party checks and controls data as evidence and for the integrated assessment of technical standards.
- Help ensure a working review process for the entitlements that are granted to the file system assets and membership of groups.
- Integrate the compliance process with existing asset management systems.

See “About the Control Compliance Suite” on page 29.
See “How Control Compliance Suite works” on page 30.

How Control Compliance Suite works

The Control Compliance Suite (CCS) Console lets you create written policies and distribute these policies to users. The console also lets you track user acceptance of policies and lets you manage exceptions to those policies. The console also lets you define evidence of your compliance with the policies.

When you define policy evidence, you use the CCS Console to create jobs to collect data from your network. Servers and other computers on your network are referred to as assets. Data collectors process jobs and gather information from the assets.
on your network. Collected data is stored in an SQL Server database. The collected data can then be evaluated against the parameters that you specify. Evaluation results are stored in the database. These evaluation results can be reviewed within the CCS Console. Evaluation results are also synchronized to the reporting database immediately or on a schedule that you specify. The evaluation results in the reporting database can be processed into reports and printed or displayed in the dashboard.

Figure 1-1 outlines the steps to install, configure, and use the CCS.

Figure 1-1  Using the Control Compliance Suite

See “About the Control Compliance Suite” on page 29.
See “What Control Compliance Suite can do for you” on page 30.
Control Compliance Suite server components

The Control Compliance Suite (CCS) consists of a number of components that work together. The components collect, store, and analyze data from the network, then transmit that data to clients in a usable form. In some instances, a single computer can serve in more than one role. Other roles require a dedicated server.

Figure 1-2 illustrates how the CCS components work together.

The CCS components include the following:

- Control Compliance Suite Application Server
  See “About the Control Compliance Suite Application Server” on page 33.

- Control Compliance Suite Directory Server
  See “About the Control Compliance Suite Directory Server” on page 34.

- Control Compliance Suite Directory
  See “About the Control Compliance Suite Directory” on page 35.

- Control Compliance Suite Certificate Management Console

- Control Compliance Suite Encryption Management Service
  See “About the Control Compliance Suite Encryption Management Service” on page 43.

- Control Compliance Suite Data Processing Service
  See “About the Control Compliance Suite Data Processing Service” on page 37.

- Control Compliance Suite Data Processing Service Load Balancer
  See “About the Data Processing Service Load Balancer” on page 38.

- Control Compliance Suite Data Processing Service Collector
  See “About the Data Processing Service Collector” on page 40.

- Control Compliance Suite Data Processing Evaluator
  See “About the Data Processing Service Evaluator” on page 41.

- Control Compliance Suite Data Processing Reporter
  See “About the Data Processing Service Reporter” on page 39.

- Control Compliance Suite production database
  See “About the Control Compliance Suite production database” on page 41.

- Control Compliance Suite reporting database
  See “About the Control Compliance Suite reporting database” on page 41.

- Control Compliance Suite evidence database
  See “About the Control Compliance Suite evidence database” on page 42.

- Control Compliance Suite Web Console server
About the Control Compliance Suite Application Server

The Control Compliance Suite (CCS) Application Server is the hub of CCS. CCS jobs flow from the CCS Console to the Application Server and then to one of the Data Processing Service Load Balancers. When reports are complete, the Application Server retrieves the report from the reporting database and sends it to the console for display to the user. In addition, the Application Server manages data storage in the Control Compliance Suite Directory, and manages the scheduled jobs and workflow in the production database.

When you install the Application Server, you must have local administrator-equivalent privileges. In addition, you must have the privileges to read from and write to the Microsoft SQL Servers that host the database components.

The Application Server runs as a service on the server that you specify. The Application Server appears in the Services control panel as Symantec Application
Server Service. The account that you use for the Application Server must be a local administrator equivalent on the computer that hosts the service. The account can be an Active Directory domain account or a local Windows user account. The same computer hosts both the Application Server and the Web Console server.

**Note:** The Application Server and the Directory Server must be located in the same domain.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite Web Console server” on page 42.

### About the Control Compliance Suite Directory Server

The Control Compliance Suite (CCS) Directory Server stores information about business objects, preferences, and other information. In addition, the Control Compliance Suite Directory Server hosts the certificate authority for the CCS system, and issues and validates certificates. Certificates are used to ensure secure communications between the CCS components.


Some CCS components contact the Directory Server with no mediation. Other components use the Encryption Management Service and the Directory Support Service to communicate with the Directory Server. The Certificate Management Console is used to create, store, bind, unbind, and renew certificates.

When you install CCS, the Directory Server is installed on a server that you specify. If necessary, you can extend the default schema that ships with CCS. You must have local administrator-equivalent privileges when you install the Directory Server. The account you use for the Directory Server must be a local administrator-equivalent account on the computer that hosts the service. The account can be an Active Directory domain account or a local Windows user account.

**Note:** The Application Server and the Directory Server must be located in the same domain.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite Directory” on page 35.

See “About the Control Compliance Suite Encryption Management Service” on page 43.
About the Control Compliance Suite Directory

Control Compliance Suite (CCS) stores information about preferences and roles as well as some business objects and other information in the Control Compliance Suite Directory. For other business objects or other information, the object is stored in the production database or the reporting database. The object security descriptor is stored in the Control Compliance Suite Directory. The Control Compliance Suite Directory stores information in a structured way. You can extend the default directory schema to store additional information.

The Application Server can retrieve information from the Control Compliance Suite Directory. For extended permissions, the Application Server also contacts the Directory Support Service. Like the directory, the Directory Support Service runs on the Directory Server. The Directory Support Service is installed automatically when you install the Directory Server. The Directory Support Service has minimal configuration needs.

On Windows Server 2003, the Microsoft Active Directory Application Mode (ADAM) service hosts the Directory Server. ADAM runs as an independent user service, as opposed to an operating system service. ADAM is designed to meet the specific needs of organizations that use directory-enabled applications. ADAM is a directory service subset of the Microsoft Active Directory. ADAM does not replace any existing directory service on your network. This ADAM installation is for the sole use of CCS.

On Windows Server 2008, the Microsoft Active Directory Lightweight Directory Service (AD LDS) hosts the Directory Server. Like ADAM, AD LDS runs as an independent user service, as opposed to an operating system service. AD LDS is a directory service subset of the Microsoft Active Directory. AD LDS does not replace any existing directory service on your network. This AD LDS installation is for the sole use of CCS.

The directory is installed and created automatically when you install the Directory Server.

The account you use for the Directory Support Service must be a local administrator-equivalent account on the computer that hosts the service. The account can be an Active Directory domain account or a local Windows user account.

See “About objects in the directory” on page 36.

See “About organizing objects in the directory” on page 36.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite Directory Server” on page 34.
About objects in the directory

When you install the Control Compliance Suite, a default hierarchical structure is created to store objects in the directory. All objects are stored under the root folder. The root folder holds subfolders for each object type. For example, a folder is used for assets, for policies, and for standards. Under the individual object type folder, the user can create a hierarchical structure to store the objects that best suits the organizational needs. For example, in the Assets folder, assets can be stored in a hierarchy that is based on the geographical locations of the organization.

See “About organizing objects in the directory” on page 36.

The following is a list of folders under the root folder:

- Assets
- Exceptions
- Policies
- Reconciliation
- Reporting
- Shared
- Standards
- Tags

See “About the Control Compliance Suite Directory” on page 35.

About organizing objects in the directory

The Control Compliance Suite (CCS) directory is hierarchical in nature, which allows users to create folders and objects in an inverted tree-like structure. This structure provides flexibility to create a hierarchy that allows the user to model the tree that is based on the organizational requirements.

When you install CCS, a default hierarchy is created to store objects. Users should organize the tree to follow the flow of control in the organization.

Beyond the default hierarchy users should organize the tree to follow the flow of control in the organization. This flow is natural for the users to administer permissions on the folders and objects where needed in the tree.

Organizations with branches all over the world, with local administrators responsible for their geographical area, benefit by a hierarchy that mimics their geographical locations. This design helps organizations to administer permissions and roles for the local administrators by following their organizational structure.
The Control Compliance Suite (CCS) Data Processing Service (DPS) is a single service that performs up to four different duties in CCS. Each of these duties is called a role. Which role the DPS serves depends on how the DPS is registered. The DPS runs as a Windows Service. A single instance of the service can provide more than one role simultaneously. Normally, a CCS deployment includes many
servers that each hosts a DPS installation. When a deployment contains multiple DPS installations, each DPS performs a single role.

In the Services control panel, the service is listed as the Symantec Data Processing Service.

The Data Processing Service performs the following roles:

■ Load Balancer
  See “About the Data Processing Service Load Balancer” on page 38.

■ Collector
  See “About the Data Processing Service Collector” on page 40.

■ Evaluator
  See “About the Data Processing Service Evaluator” on page 41.

■ Reporter
  See “About the Data Processing Service Reporter” on page 39.

When you install a Data Processing Service, you must have local administrator-equivalent privileges.

The account you provide for a Data Processing Service to use must be a local administrator-equivalent account on the computer that hosts the service. The account can be an Active Directory user account or a local Windows user account.

See “Control Compliance Suite server components” on page 32.

**About the Data Processing Service Load Balancer**

When the Data Processing Service (DPS) acts as a load balancer, the DPS routes data collection jobs from the Application Server to a DPS Collector. In addition, a load balancer routes the evaluation jobs to the DPS Evaluator and the reporting jobs to the DPS Reporter. If your deployment includes multiple load balancers, the Application Server automatically uses each in turn. If a load balancer fails, the Application Server automatically skips the failed load balancer and uses another load balancer. This round robin assignment gives limited fault tolerance.

See “About the Data Processing Service Collector” on page 40.

See “About the Data Processing Service Evaluator” on page 41.

See “About the Data Processing Service Reporter” on page 39.

The DPS Collector retrieves the data from the network. Potentially, your installation of Control Compliance Suite (CCS) can have a large number of DPS Collectors and the associated data collectors. The load balancer assigns jobs to eligible collectors sequentially. The load balancer does not base job assignments on the current load of the collector. If a query requires input from several DPS Collectors, the load balancer distributes the query appropriately. When the DPS
Collectors complete the query, the load balancer combines the results and returns the results to the Application Server for storage.

An eligible DPS Collector is any collector that has the ability to complete the data collection job. The collector site assignment and the installed RMS snap-in modules determine the collector eligibility.

The DPS Evaluator compares collected data to the standards that you specify and saves the results for later use. Potentially, your installation of CCS can have multiple DPS Evaluators. The load balancer assigns jobs to evaluators sequentially. The load balancer does not base job assignments on the current load of the evaluator.

The first DPS registered when you deploy CCS should be assigned to the Load Balancer role.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite Data Processing Service” on page 37.

About the Data Processing Service Reporter

The Data Processing Service (DPS) Reporter generates reports and dashboards for display by the Control Compliance Suite (CCS) Console. In addition, a single DPS Reporter is assigned to perform database synchronization between the production database and the reporting database.

The reporter executes the list of queries that are specific to the selected dashboard or the selected report. On the basis of these queries, the reporter retrieves data from the reporting database and creates the report.

The DPS Reporter that is assigned to synchronize data synchronizes the contents of the reporting and the production databases. Synchronization occurs based on a schedule that you specify or when an evaluation job triggers the synchronization.

The computer that hosts the DPS Reporter must have the Crystal Reports engine installed. The Crystal Reports installer is available on the CCS product disc.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite Data Processing Service” on page 37.

See “About the Data Processing Service Load Balancer” on page 38.

See “About the Data Processing Service Collector” on page 40.

See “About the Data Processing Service Evaluator” on page 41.
About the Data Processing Service Collector

The Data Processing Service (DPS) Collector is the interface to the programs that do the actual work of collecting data from the network. Your Control Compliance Suite (CCS) deployment can include multiple data collectors, each linked with a DPS Collector. The DPS Collector receives data collection jobs from the DPS Load Balancer and formats the job for the data collector. When the data collector processes the job and collects the data, the data collector transfers the data to the DPS Collector. The DPS Collector then returns the collected data to the DPS Load Balancer. If necessary, the DPS Load Balancer combines the data with data from one or more other DPS Collectors. Finally, the DPS Load Balancer sends the data to the Application Server for storage in the production database for use by the DPS Evaluator.

The DPS Collector collects the data from the data collectors, which in turn collect data from the network. Potentially, your installation of CCS can have a large number of DPS Collectors and associated data collectors. The DPS Load Balancer assigns jobs to the eligible DPS Collectors sequentially. The DPS Load Balancer does not base job assignments on the current load of a DPS Collector. If an eligible DPS Collector is unavailable, the DPS Load Balancer skips it and uses another eligible DPS Collector. This round robin assignment gives limited fault tolerance.

An eligible DPS Collector is any collector that has the ability to complete the data collection job. The DPS Collector site assignment or installed RMS snap-in modules can make the DPS Collector ineligible.

CCS supports the following data collectors:

- Symantec RMS
- Symantec Enterprise Security Manager (ESM)
- CSV files
- ODBC databases

Used with a custom schema, the CSV files let you create any custom data collector and schema. This ability lets you use any custom data on your network, including data not ordinarily supported by CCS.

The data that the DPS Collector collects is compressed before the data is returned to the other CCS components.

See “Control Compliance Suite server components” on page 32.
See “About the Control Compliance Suite Data Processing Service” on page 37.
See “About the Data Processing Service Load Balancer” on page 38.
See “About the Data Processing Service Evaluator” on page 41.
See “About the Data Processing Service Reporter” on page 39.
About the Data Processing Service Evaluator

Evaluation jobs are sent from the Application Server to one of the Data Processing Service (DPS) Load Balancers. The DPS Load Balancer then sends the evaluation job to the DPS Evaluator. The evaluator compares the data to the specifications in the Standards that you select and then stores the evaluation results in the production database.

If you have more than one evaluator, the DPS Load Balancer assigns evaluation jobs to the evaluators sequentially. If a DPS Evaluator is unavailable, the load balancer skips it and uses the next available evaluator. This round robin assignment gives limited fault tolerance.

See “Control Compliance Suite server components” on page 32.
See “About the Control Compliance Suite Data Processing Service” on page 37.
See “About the Data Processing Service Load Balancer” on page 38.
See “About the Data Processing Service Collector” on page 40.
See “About the Data Processing Service Reporter” on page 39.

About the Control Compliance Suite production database

A Microsoft SQL Server instance hosts the production database. The database stores the data that is collected from the assets. The database also stores the results of evaluation jobs. The database stores information about the policies that you create and about the entitlement control points. If you use the Symantec Response Assessment module with the Control Compliance Suite (CCS), the Response Assessment data is also stored in the production database.

The production database requires Microsoft SQL Server 2005 SP2 or Microsoft SQL Server 2008. CCS requires a single production database. The production database can share a host server with the Control Compliance Suite Directory, or you can use a dedicated server as the host. The production database can be hosted on the same SQL Server as the reporting database, or on another SQL Server.

See “Control Compliance Suite server components” on page 32.
See “About the Control Compliance Suite reporting database” on page 41.
See “About the Control Compliance Suite evidence database” on page 42.

About the Control Compliance Suite reporting database

A Microsoft SQL Server instance hosts the reporting database. The reporting database is periodically synchronized with the data that is stored in the production database and the evidence database. In addition, the database stores data specific
to individual dashboards or reports. The DPS Reporter monitors the synchronization of data between the production database, evidence database and the reporting database.

The reporting database requires Microsoft SQL Server 2005 SP2 or Microsoft SQL Server 2008. CCS requires a single reporting database. The reporting database can share a host server with the Control Compliance Suite Directory, or you can use a dedicated server as the host. The reporting database can be hosted on the same SQL Server as the production database, or on another SQL Server.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite production database” on page 41.

See “About the Control Compliance Suite evidence database” on page 42.

About the Control Compliance Suite evidence database

A Microsoft SQL Server instance hosts the evidence database. The evidence database stores the evidence gathered from the extended evidence sources that are registered with Control Compliance Suite (CCS) such as Symantec Data Loss Prevention, Response Assessment Module etc. The Data Processing Service Evaluator stores the evidence in this database.

The evidence database requires Microsoft SQL Server 2005 SP2 or Microsoft SQL Server 2008. CCS requires a single evidence database. The evidence database must share a host SQL Server with the production database.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite production database” on page 41.

See “About the Control Compliance Suite reporting database” on page 41.

See “About the Control Compliance Suite evidence database” on page 42.

About the Control Compliance Suite Web Console server

The computer that hosts the CCS Web Console server host must have the Microsoft Internet Information Server (IIS). The CCS Web Console allows access to some CCS content without requiring the full CCS Console. The same computer hosts the Web Console server and the Application Server.

The CCS Web Console lets users do the following:

■ Accept or reject policies.

■ Request policy exceptions.

■ Request policy clarifications.
Review policies.

Approve policies.

Respond to Response Assessment module questions.

Review data in dashboards.

Connect to the Response Assessment module Web client to respond to questionnaires.

Set Web console user preferences.

Download Control Compliance Suite thick console from the Downloads page.

The computer that hosts the Application Server also always hosts the CCS Web Console server.

If the same computer hosts the Web console, the Application Server, and the Directory Server, CCS uses Windows NTLM authentication. If the Web console, the Application Server, and the Directory Server are hosted on multiple computers, you must enable Kerberos authentication on all components. Kerberos authentication lets credentials be passed from the Web Console client to the Web Console server which is the same as the Application Server. The Application Server can then pass the credentials to the Directory Server.

For information about Kerberos authentication, see the Microsoft knowledge base. http://support.microsoft.com/kb/326985.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite Application Server” on page 33.

See “About the Control Compliance Suite Web Console” on page 44.

About the Control Compliance Suite Encryption Management Service

The Control Compliance Suite (CCS) Encryption Management Service reencrypts the data that is sent to the Directory Server by the Application Server. The Encryption Management Service then passes the data to the Directory Server for storage. When the Application Server needs encrypted data from the Directory Server, the Encryption Management Service performs the first stage of decryption. The Encryption Management Service then passes the data on to the Application Server.

The Directory Server hosts the Encryption Management Service. The Encryption Management Service is installed and configured automatically when you install the Directory Server. The Encryption Management Service has no user interface.

See “Control Compliance Suite server components” on page 32.
Control Compliance Suite client software

The ways in which the Control Compliance Suite (CCS) interacts with the user depends on the user role and other factors. The CCS Console provides access to the full range of CCS capabilities. In addition, users can review policies and request exceptions using the Web client.

See “Control Compliance Suite server components” on page 32.
See “About the Control Compliance Suite Console” on page 44.
See “About the Control Compliance Suite Web Console” on page 44.

About the Control Compliance Suite Console

The Control Compliance Suite (CCS) Console is a Windows application that runs on a client computer. The console allows access to the full range of CCS activities. Only users who have been assigned to roles that allow them to work in the console can perform activities in the console.

The computer that hosts the CCS Console and the computer that hosts the Application Server can be in the same domain. If the console and the Application Server are in different domains, the components can communicate successfully if the domains have a two-way trust relationship. Both domains must be a Windows Server 2003 domain or a Windows Server 2008 domain. In addition, the trust relationship must be set up to use Kerberos authentication instead of the default NTLM authentication. Finally, only constrained delegation is supported. Unconstrained delegation is not supported.

For information on setting up delegation, see the Symantec Control Compliance Suite Installation Guide.

See “Control Compliance Suite server components” on page 32.
See “Control Compliance Suite client software” on page 44.
See “About the Control Compliance Suite Web Console” on page 44.

About the Control Compliance Suite Web Console

The Control Compliance Suite (CCS) Web Console lets users access a subset of the CCS functionality using Internet Explorer 7.0 or Internet Explorer 8.0.

In the Web console, users can do the following:

■ Accept or reject policies.
■ Request policy exceptions.
■ Request policy clarifications.
- Review policies.
- Approve policies.
- Respond to Response Assessment module questions.
- Review data in dashboards.
- Create dashboards.
- Connect to the Response Assessment module Web client to respond to questionnaires.
- Set Web console user preferences.
- Download Control Compliance Suite thick console from the Downloads page.

For complete information about using the CCS Web Console, see the Control Compliance Suite Web Console Help.

See “Control Compliance Suite server components” on page 32.

See “About the Control Compliance Suite Web Console server” on page 42.

See “Control Compliance Suite client software” on page 44.

See “About the Control Compliance Suite Console” on page 44.

See “About accessing the Control Compliance Suite Web Console” on page 45.

About accessing the Control Compliance Suite Web Console

The Web console is accessed using the following URL:

http://<servername>/CCS_Web

If you have problems opening the Web console or viewing any of the pages in the Web console, you may have set the Service Principal Names incorrectly on the application server. Refer to the troubleshooting section or the Control Compliance Suite Installation Guide for information on how to resolve the issue.

See “Troubleshooting when an error appears while viewing a dashboard on the Web Console” on page 918.

If you make changes to the SQL Server credentials in the Control Compliance Suite Console, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

See “Troubleshooting when the message “Login failed for user <user name>” appears in the Web console” on page 919.

See “About the Control Compliance Suite Web Console” on page 44.
Control Compliance Suite infrastructure requirements

The Control Compliance Suite (CCS) components have minimum requirements for hardware and software. Symantec recommends that you do not install the CCS on computers that do not meet these requirements.

You must ensure that the computers that you use for your CCS deployment meet the following minimum requirements:

■ CCS server requirements
  See “Control Compliance Suite server requirements” on page 46.

■ CCS client requirements
  See “Control Compliance Suite Client requirements” on page 50.

In addition to these minimum requirements, each component has recommendations to ensure optimal performance. Some recommendations vary with the size of the deployment.

See “Control Compliance Suite server requirements” on page 46.
See “Control Compliance Suite Client requirements” on page 50.

Control Compliance Suite server requirements

You must ensure that the computers that host the Control Compliance Suite (CCS) infrastructure components meet the minimum requirements. These requirements are for a minimum system, and are sufficient only to run the components and experiment with a limited test environment. Before you plan your CCS deployment, review the component recommendations individually.

For a minimum system in a lab setting, you can install all components on one or two servers. If you do so, CCS performance diminishes. Any production CCS deployment should plan for separate servers for separate roles.

In addition to these minimum requirements, each component has recommendations to ensure optimal performance. Some recommendations vary with the size of the deployment. In particular, multiple SQL Servers are normally used to host the databases.

These server requirements do not take into account the needs of the data collector deployments that collect data from the network.

Note: You must deploy the CCS Application Server and Directory Server in a Windows Active Directory domain. You should deploy the Data Processing Service in an Active Directory domain, although you can deploy the service in a Windows workgroup when required.
The domain where you install the Application Server and the Directory Server must be a Windows Server 2003 or a Windows Server 2008 domain. The functional level of the domain can be any of the following:

- Windows Server 2008
- Windows Server 2003

CCS has not been validated on Windows Server 2008 “Server Core only” installations.

If you install multiple CCS server components on a single host computer, the minimum disk space requirements are cumulative.

Table 1-1 contains the minimum requirements for each component.

<table>
<thead>
<tr>
<th>Component name</th>
<th>Minimum memory</th>
<th>Minimum processor</th>
<th>Required hard disk size</th>
<th>Required operating system</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server and Web Console server</td>
<td>2 GB</td>
<td>2.8 GHz</td>
<td>80 GB</td>
<td>Windows Server 2003 SP2&lt;br&gt;Windows Server 2003 SP2 x64&lt;br&gt;Windows Server 2003 R2 SP2&lt;br&gt;Windows Server 2003 R2 SP2 x64&lt;br&gt;Windows Server 2008&lt;br&gt;Windows Server 2008 SP2&lt;br&gt;Windows Server 2008 x64&lt;br&gt;Windows Server 2008 SP2 x64&lt;br&gt;Windows Server 2008 R2 x64</td>
<td>Microsoft .NET 3.5 SP1&lt;br&gt;Internet Information Services (IIS) 6.0 or 7.0. The 32-bit version and the 64-bit version are both supported.&lt;br&gt;If the computer that hosts the Control Compliance Suite Web Console server uses Windows Server 2008, the computer must have the <strong>Window Authentication</strong> role added.</td>
</tr>
<tr>
<td>Component name</td>
<td>Minimum memory</td>
<td>Minimum processor</td>
<td>Required hard disk size</td>
<td>Required operating system</td>
<td>Other requirements</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Directory Server</td>
<td>2 GB</td>
<td>2.8 GHz</td>
<td>80 GB</td>
<td>Windows Server 2003 SP2&lt;br&gt;Windows Server 2003 SP2 x64&lt;br&gt;Windows Server 2003 R2 SP2&lt;br&gt;Windows Server 2003 R2 SP2 x64&lt;br&gt;Windows Server 2008&lt;br&gt;Windows Server 2008 SP2&lt;br&gt;Windows Server 2008 x64&lt;br&gt;Windows Server 2008 SP2 x64&lt;br&gt;Windows Server 2008 R2 x64</td>
<td>Microsoft .NET 3.5 SP1</td>
</tr>
<tr>
<td>Production database or reporting database</td>
<td>2 GB</td>
<td>2.8 GHz</td>
<td>160 GB</td>
<td>Windows Server 2003 SP2&lt;br&gt;Windows Server 2003 SP2 x64&lt;br&gt;Windows Server 2003 R2 SP2&lt;br&gt;Windows Server 2003 R2 SP2 x64&lt;br&gt;Windows Server 2008&lt;br&gt;Windows Server 2008 SP2&lt;br&gt;Windows Server 2008 x64&lt;br&gt;Windows Server 2008 SP2 x64&lt;br&gt;Windows Server 2008 R2 x64</td>
<td>Microsoft SQL Server 2005 SP2&lt;br&gt;Microsoft SQL Server 2005 SP3&lt;br&gt;Microsoft SQL Server 2008&lt;br&gt;Microsoft SQL Server 2008 SP1</td>
</tr>
</tbody>
</table>

**Note:** You must install the latest service packs along with the cumulative update package (if any) on the computer that hosts the SQL server. For example, if you have SQL 2005 SP2, you need to deploy the cumulative update package 17 for SQL Server 2005 Service Pack 2. ( [http://support.microsoft.com/kb/976952](http://support.microsoft.com/kb/976952) )
Table 1-1  Control Compliance Suite server requirements (continued)

<table>
<thead>
<tr>
<th>Component name</th>
<th>Minimum memory</th>
<th>Minimum processor</th>
<th>Required hard disk size</th>
<th>Required operating system</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Processing Services</td>
<td>2 GB</td>
<td>2.8 GHz</td>
<td>80 GB</td>
<td>Windows Server 2003 SP2</td>
<td>Microsoft .NET 3.5 SP1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 R2 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 R2 SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 R2 x64</td>
<td></td>
</tr>
</tbody>
</table>

If .NET is not installed, the Control Compliance Suite installer prompts you to install it.

Before you install the CCS components, you should run Windows Update to ensure that the latest Windows security updates are installed.

The computers that host the following components must be in the same LAN segment:

- Application Server and the CCS Web Console server
- Directory Server
- Data Processing Service Load Balancer
- Data Processing Service Evaluator
- Data Processing Service Reporter
- Control Compliance Suite Production database
- Control Compliance Suite Reporting database
- Control Compliance Suite Evidence database

See “Control Compliance Suite infrastructure requirements” on page 46.

See “Control Compliance Suite Client requirements” on page 50.
Control Compliance Suite Client requirements

Before you install the Control Compliance Suite (CCS) clients, you must ensure that the target computers meet the minimum requirements.

*Table 1-2* contains the minimum requirements for the CCS clients.

<table>
<thead>
<tr>
<th>Component name</th>
<th>Minimum memory</th>
<th>Minimum processor</th>
<th>Required hard disk size</th>
<th>Required operating system</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Compliance Suite client</td>
<td>1 GB</td>
<td>2.8 GHz</td>
<td>80 GB</td>
<td>Windows XP Professional SP2</td>
<td>Microsoft Office Primary Interop Assemblies</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows XP Professional SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows XP Professional SP3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows XP Professional SP3 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP1 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows 7 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 R2 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 R2 SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 R2 x64</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-2  Control Compliance Suite client requirements (continued)

<table>
<thead>
<tr>
<th>Component name</th>
<th>Minimum memory</th>
<th>Minimum processor</th>
<th>Required hard disk size</th>
<th>Required operating system</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Compliance Suite Web Console</td>
<td>512 MB</td>
<td>1.2 GHz</td>
<td>40 GB</td>
<td>Windows XP Professional SP2</td>
<td>Internet Explorer 7.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows XP Professional SP2 x64</td>
<td>or Internet Explorer 8.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows XP Professional SP3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows XP Professional SP3 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP1 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Vista Business or Enterprise SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows 7 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 R2 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2003 R2 SP2 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2008 R2 x64</td>
<td></td>
</tr>
</tbody>
</table>

CCS has not been validated on Windows Server 2008 “Server Core only” installations.

You must ensure that the connection between the CCS and the Application Server has at least 256 Kbps of bandwidth.
Before you install the CCS components, you should run Windows Update to ensure that the latest Windows security updates are installed.

Microsoft Office and the Microsoft Office Primary Interop Assembly are required to import Microsoft Word documents as policies. You can use Microsoft Office XP, Microsoft Office 2003, or Microsoft Office 2007.

See “Importing a Word policy” on page 695.

To create user-defined reports, you must install Crystal Reports Developer 2008, part of the third-party Crystal Reports 2008 product. Crystal Reports Developer is required only on the CCS client that you use to create the user-defined reports.

See “Control Compliance Suite infrastructure requirements” on page 46.

See “Control Compliance Suite server requirements” on page 46.

Where to get more information

You can access the Control Compliance Suite documents from the product disc and the Symantec Web site. The documents are also installed at the `<install directory>\Documentation` folder.

Control Compliance Suite (CCS) provides the following documents:

- **Control Compliance Suite Planning and Deployment Guide**: The guide informs users about the decisions that they need to make before the installation.
- **Control Compliance Suite Installation Guide**: The guide assists users in installing the product and its components.
- **Control Compliance Suite User’s Guide**: The guide describes the various features and indicates when they are performed. The user’s guide contains procedures for all the key tasks.
- **Control Compliance Suite Online Help**: The Help file describes the various features and indicates when they are performed. The help file contains procedures for all the key tasks. The Help file is accessible from within the Control Compliance Suite Console.
- **Control Compliance Suite Release Notes**: The release notes contain any installation or other issues that users should know before they install the Control Compliance Suite product.
- **Control Compliance Suite Quick Reference Card**: The quick reference card provides users with enough information to prepare to deploy the product.
The reference guide provides APIs to integrate the third-party clients to the core functionality of CCS within their own business processes.

The Control Compliance Suite user's guide, planning and deployment guide, installation guide, quick reference card, and release notes are available in a PDF format.

**Note:** To view the online documentation, you must have Acrobat Reader 5.0 or later.

You can also check the Symantec Web site and the Knowledge Base for answers to frequently asked questions, troubleshooting tips, and the latest product information.

On the Internet, go to: [www.symantec.com/support/](http://www.symantec.com/support/)

See “About the Control Compliance Suite” on page 29.

See “Where to get Symantec Enterprise Security Manager information” on page 53.

See “Where to get Response Assessment module information” on page 54.

**Where to get Symantec Enterprise Security Manager information**

You can access the Symantec Enterprise Security Manager (ESM) information from the product disc and the Symantec Web site.

The Documentation directory includes the following ESM documentation:

- **Symantec Enterprise Security Manager User's Guide**
  - The guide has post-installation information and procedures to help you learn how to use the product.

- **Symantec Enterprise Security Manager Installation Guide**
  - The guide assists users in installing the product and its components.

- **Symantec Enterprise Security Manager Online Help**
  - The Help file has post-installation information and procedures to help you learn how to use the product.
  - The Help file is accessible from within the Symantec Enterprise Security Manager console.

- **Symantec Enterprise Security Manager Release Notes**
  - The release notes contain any installation or other issues that users should know before they install the ESM.
Where to get Response Assessment module information

You can access the Response Assessment module (RAM) information from the product disc and the Symantec Web site.

The Docs directory on the product disc contains the following documents:

- **Response Assessment module User Guide**: The guide has post-installation information and procedures to help you learn how to use the product.
- **Response Assessment module Online Help**: The Help file has post-installation information and procedures to help you learn how to use the product. The Help file is accessible from within the Control Compliance Suite Console.
- **Response Assessment module Release Notes**: The release notes contain any installation or other issues that users should know before they install the RAM.

Note: To view the online documentation, you must have Acrobat Reader 5.0 or later.

You can also check the Symantec Web site and the knowledge base for answers to frequently asked questions, troubleshooting tips, and the latest product information.

On the Internet, go to: [www.symantec.com/support/](http://www.symantec.com/support/)
See “About the Control Compliance Suite” on page 29.
See “Where to get Symantec Enterprise Security Manager information” on page 53.
See “Where to get more information” on page 52.
Introducing Control Compliance Suite

Where to get more information
This chapter includes the following topics:

- About the console features
- About the console views
- Working in the console

About the console features

The Control Compliance Suite console provides several control features to help you work with ease and efficiency.

The console provides the following control features:

Menu bar

The menu bar appears across the top of the console window. You can access the Control Compliance Suite features using the menu options.

Navigation bar

The navigation bar appears under the menu bar across the top of the console window. The navigation bar groups the common tasks that you can perform.
### About the menu bar

You can access the Control Compliance Suite (CCS) features by using the menu bar that appears across the top of the Console window. The menu bar offers a traditional approach to using the application’s features. Some options are available only after an item is selected.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree pane</td>
<td>The tree pane appears on the left side of the console window under the navigation bar. The tree pane does not appear in all views. The tree pane displays a hierarchical, a folder-based navigation structure that lists the objects that are stored in the Directory. When you select an asset group from the tree pane, the list of assets is displayed in the table pane.</td>
<td>“About the tree pane” on page 60.</td>
</tr>
<tr>
<td>Filter by pane</td>
<td>The Filter by pane appears in the lower-left side of the console window under the tree pane. You can narrow the list of objects that are displayed in the table pane by selecting the filter options. The filter options vary based on the view selected.</td>
<td>“About the Filter by pane” on page 61.</td>
</tr>
<tr>
<td>Taskbar</td>
<td>The taskbar appears across the top of the tree pane and the table pane in the console window. The taskbar displays a list of tasks that are relevant to the current object that is selected in the table pane.</td>
<td>“Using filters in the Filter by pane” on page 67.</td>
</tr>
<tr>
<td>Table pane</td>
<td>The table pane appears in the right side of the console window under the taskbar. The table pane lists all the objects for the selected folder in the tree pane.</td>
<td>“Customizing the filter options” on page 67.</td>
</tr>
<tr>
<td>Details pane</td>
<td>The details pane appears in the lower-right side of the console window under the table pane. The details pane displays information about the object that is selected in the table pane.</td>
<td>“Viewing and editing the object details” on page 69.</td>
</tr>
</tbody>
</table>
## Table 2-1  Menu options

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Print Preview</td>
<td>Opens the <strong>Print Preview</strong> dialog box.</td>
</tr>
<tr>
<td></td>
<td>Print</td>
<td>Invokes the <strong>Print</strong> dialog box and lets you print the information in the view area to a selected printer.</td>
</tr>
<tr>
<td></td>
<td>Export to</td>
<td>Opens the <strong>Export to</strong> dialog box. The <strong>Export to</strong> dialog box lets you export the information in the view area. The Export to menu item is not available in all views.</td>
</tr>
<tr>
<td></td>
<td>Export options</td>
<td>Opens the <strong>Export Options</strong> dialog box. The Export options dialog box is not available in all views.</td>
</tr>
</tbody>
</table>
|         | Send            | **Link by E-mail** invokes your email application and lets you send a mail recipient a link to the view.  
**Shortcut to Desktop** lets you save the state of a particular view to your desktop for quick access at a later time. |
|         | Exit            | Closes the CCS application.                                                 |
| Edit    | Cut             | Cuts the currently selected item to the clipboard.                          |
|         | Copy            | Copies the currently selected item to the clipboard.                        |
|         | Paste           | Pastes the current contents of the clipboard.                               |
| View    | Back            | Returns to the previous view.                                               |
|         | Forward         | Returns to the view you were in when you selected Back.                     |
|         | Refresh         | Displays the most current information in the view you are in.               |
|         | Show/Hide       | Acts as a toggle to show or hide the following:  
- Tree pane  
- Filter by pane  
- Table pane  
- Details pane |
| Go      | Home            | Opens the CCS Home view.                                                   |
Table 2-1 Menu options (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor</td>
<td>Monitor</td>
<td>Opens the CCS Monitor view.</td>
</tr>
<tr>
<td>Manage</td>
<td>Manage</td>
<td>Opens the CCS Manage view.</td>
</tr>
<tr>
<td>Settings</td>
<td>Settings</td>
<td>Opens the CCS Settings view.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Reporting</td>
<td>Opens the CCS Reporting view.</td>
</tr>
<tr>
<td>Tasks</td>
<td>Tasks</td>
<td>Display the list of available tasks that are relevant to the item that is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>selected in the view. The tasks in the list are the same tasks available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>from the taskbar.</td>
</tr>
<tr>
<td>Help</td>
<td>Help Topic</td>
<td>Opens the Control Compliance Suite Online Help.</td>
</tr>
<tr>
<td>Index</td>
<td>Index</td>
<td>Opens the help file Index tab.</td>
</tr>
<tr>
<td>Search</td>
<td>Search</td>
<td>Opens the help file Search tab.</td>
</tr>
<tr>
<td>About</td>
<td>About</td>
<td>Opens the CCS About box. The About box provides information such as version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>number, copyright information, product information, and system information.</td>
</tr>
</tbody>
</table>

See “About the console features” on page 57.

About the tree pane

The tree pane displays a hierarchical, folder-based structure of the objects as stored in the Directory. The tree pane displays the objects that are relevant to the view in the console. For example, if you are in the Assets view, the tree pane displays only assets and the asset groups.

The tree pane appears on the left side of the console window under the navigation bar.

The tree pane contains the predefined folder and user-defined folders:

<table>
<thead>
<tr>
<th>Predefined</th>
<th>Displays the built-in business objects that are installed along with the product. All users can access the Predefined folder. When you select a folder, the list of objects within the folder is displayed in the table pane.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The objects in the Predefined folder cannot be modified.</td>
</tr>
</tbody>
</table>
User-defined Displays the hierarchical structure of folders as defined in the Directory. You can also create a folder structure from here. The hierarchy can be based on requirements such as platform and geographical locations. When you select a folder in the tree pane, the list of objects within that folder is displayed in the table pane.

See “About working in the tree pane” on page 70.
See “About the console features” on page 57.

About the Filter by pane

The Filter by pane displays the predefined filter options that correspond to each view in the console. You can select different options from the filter pane and click the Update icon to view the updated results in the table pane.

When filtering assets, you can only filter on the assets that are displayed in the table pane. You cannot filter on the assets that are in the asset store.

See “Asset folder hierarchy” on page 234.

The Filter by pane appears in the lower left side of the console window under the tree pane.

The filter pane has the following icons:

- **Customize** You can choose which filter options appear in the filter pane and the order in which the options appear. To choose the options that appear in the filter pane, you click the Customize icon.

- **Reset to last** You can reset the values of the filter options to the last saved values. When you make changes to the filter options and then decide to revert back to the previously selected filter options you click Reset to last icon. Once you navigate away from the view you cannot reset the options to the previous selection.

- **Update** When you modify the filter options and their values, you must click the Update icon to update the results in the table pane.

See “Customizing the filter options” on page 67.
See “Using filters in the Filter by pane” on page 67.

About the table pane

The table pane lists all the objects for the selected folder in the tree pane.
The table pane appears in the right side of the console window under the taskbar. You can select the object that you want to work with from the table pane. After the object is selected, all associated tasks are enabled on the taskbar. You can also use the context menu to do the tasks. Right-click the object in the table menu and the context menu appears.

You can also select multiple objects to work within the table pane. Select the check box next to the objects that you want to work with. Only the tasks that are associated with multiple selections are enabled.

When you edit multiple objects, the previous values of all the selected objects are replaced with the new values.

Use the Filter by pane and the other features of the console to manage and refine the results in the table pane.

See “Managing the table pane” on page 68.

See “Viewing and editing the object details” on page 69.

See “Selecting the columns headings” on page 69.

See “About the console features” on page 57.

About the details pane

The details pane displays the various properties of the object that is selected in the table pane. The object details are grouped in various tabs. The details pane appears in the lower-right side of the console window under the table pane. In the details pane, the object details are shown grouped in various tabs.

The details pane has the following icons:

- **Save**: You can make changes to certain values in the details pane. To save any changes that are made in the tabs, you click **Save**.

- **Revert**: You can reset the values of any changes that are made in the details pane. Revert only resets those values that have not been saved.

- **Refresh**: You can refresh the details pane to display any properties that has changed since the view was selected.

See “About the console features” on page 57.

About the taskbar

The taskbar displays the tasks that are relevant to the object that are selected in the current view. The taskbar appears across on top of the tree pane and the table pane in the console window.
In some views, where there are larger number of tasks, the taskbar contains a drop-down menu. You can click on the drop-down menu to view the additional tasks.

See “About the console features” on page 57.

About the console views

The console consists of several main views where you do your work. The views and tasks available to you are based on the roles and permissions that your administrator assigns to you.

The following are the main views of the console:

- Home view
- Monitor view
- Manage view
- Reports view
- Settings view

See “About the console features” on page 57.

About the Home view

The Home view is the default view that appears when you log on to the Control Compliance Suite (CCS) Console. The Home view contains the Home page and the User Preferences page.

The Home page is a static page that displays a brief introduction of the product and contains links that helps you to quickly get started with the product. The Home page also displays the link to launch CCS Web Console.

The User Preferences page allows users with the role to schedule jobs to store their password. The credentials are used to run the scheduled jobs at a later time.

See “About the User preferences page” on page 66.

See “Adding credentials for scheduled jobs” on page 164.

See “About the console views” on page 63.

About the Monitor view

The Monitor view displays the information that is related to Jobs and Evaluation Results.

The Monitor view consists of the following views:
About the console views

- Jobs
- Evaluation Results

See “About the Jobs view” on page 715.

See “About the Evaluation Results view” on page 727.

About the Manage view

The Manage view lets you perform all the tasks that are related to assets, entitlement, exceptions, standards, tags, and policies in the Control Compliance Suite.

The Manage view consists of the following views:

- Assets
- Entitlements
- Exceptions
- Standards
- Baselines
- Tags
- Content
- Policies

About the Settings view

The Settings view contains the tools that help the administrator to easily and efficiently configure and manage the Control Compliance Suite infrastructure.

The Settings view is displayed only to users with the Administrator role.

You can do the following from the Settings view:

- Configure and manage the infrastructure components.
- Deploy infrastructure updates, content updates, and patches.
- Report on the configuration and the health status of the infrastructure components.
- Configure and manage users, roles, and credentials.
- View component certificates
- Collect evidence
- Manage asset and entity schema
Settings contains the following views:

- General
- Roles
  See “About the Roles view” on page 105.
- Permissions Management
  See “About the Permission Management view” on page 106.
- Licenses
  See “About the Licenses view” on page 181.
- LiveUpdate
  See “About the LiveUpdate view” on page 194.
- System Topology
  See “About the Map view” on page 123.
  See “About the Grid view” on page 126.
- Certificates
  See “About the Certificates view” on page 82.
- User Management
  See “About the User Management view” on page 183.
- Schema Manager
  See “About the Schema Manager view” on page 444.
- Extended Evidence Source
  See “About the Extended Evidence Sources view” on page 810.

About the Reporting view

Control Compliance Suite provides a rich set of presentation-level reports. A report is a business document that contains a predefined, organized collection of data. A report can be viewed, printed, or analyzed. Reports are viewed in the Reporting view. You schedule reports in the Job Management view. The reporting features let you distill the data and publish the results.

To view dashboards, you are required to install a Flash player with the CCS console.

You can do the following in the Reporting view:

- Manage reports
- Export reports to a different format
- Manage historical data in My Reports view
Generate reports on compliance-relevant areas in the Control Compliance Suite

The Reporting view comprises the following:

- Reports Templates view
- My Reports view

See “About the Reports Templates view” on page 732.
See “About the My Reports view” on page 733.

About the User preferences page

Users with the role to schedule jobs can store their passwords. The password is required for asset resolution on the jobs that are scheduled to run at a later time. Only users with the role to schedule jobs can store their passwords.

This feature is available only if the administrator has selected the option to store password in Control Compliance Suite.

See “About the security settings for scheduled jobs” on page 164.
See “About the Home view” on page 63.

Working in the console

You can perform various tasks in the console views based on the roles and permissions that are assigned to you.

See “Using filters in the Filter by pane” on page 67.
See “Customizing the filter options” on page 67.

Accessing tasks

You can access tasks in the console from the following console features:

- Menu bar
- Navigation bar
- Taskbar
- Context menu

See “About the console features” on page 57.
Using filters in the Filter by pane

When configuring your console, you can set filters in each view to limit the number of objects that display in the table pane. Each view has a set of predefined filters that correspond to the type of information in the view. The Filter by pane also provides a customize feature where you can choose the filter options that appear in the Filter by pane.

See “Customizing the filter options” on page 67.

To use filters

1. In the Filter by pane, select the check box that corresponds to the required filter.
2. If applicable, select the filter value from the associated list box.
3. For certain filters, you must provide the upper and lower limit values to obtain the results that exist within the range.
4. Click the Update icon to view the results in the table pane.

See “About the Filter by pane” on page 61.

Customizing the filter options

You can choose which filter options and the order the options appear in the Filter by pane.

To customize the filter options

1. In the Filter by pane, click the Customize icon.
2. In the Customize Filters dialog box, from the list box select the filter type to edit.
3. For the selected filter type, you can do any of the following:
   - Select or deselect the Display filter type check box. If you deselect the filter type, the filter type and its options are not displayed in the Filter by pane.
   - Use the arrow icons to move the options between Display and Do not display boxes.
   - Use the Move up and Move Down icons to change the order of the options that is displayed in the Filter by pane.
4. Click Save Changes.

See “About the Filter by pane” on page 61.

See “Using filters in the Filter by pane” on page 67.
Managing the table pane

Use the Filter by pane and other areas of the console to manage and refine the results that are displayed in the table pane.

To manage the table pane

1. In the tree pane, navigate to the required folder.
2. Use any of the following to manage the objects that are shown in the table pane:

   - **Filter by pane**: Select the filter options in the Filter by pane to refine the results in the table pane.

   - **Display list box**: The Display list box lists the different types of content that can be displayed in the table. For example, in the Assets view, some of the Display selections are: Assets and Asset Groups, Asset Groups Only, and Assets Only.

     The Display list box is displayed on the top-left side of the table pane. The Display selection remains when you navigate away from the view and return.

   - **Column chooser**: Select the column headings that you want to see or hide in the table pane. To select the column headings, you click the column chooser icon. The options available in the Column Chooser dialog box depend on what is selected in the Display list box. The column chooser icon is displayed in the top-right side of the table pane.

   - **Column sort**: The content of table can be arranged based on the content of the columns that compose the table. Contents can be arranged in ascending or in descending order. The up or down arrow in the column heading indicates the order in which the table is sorted.

   - **Column order**: The columns can be rearranged in any order. To move a column, you drag the heading of the column to move to the new location in the column header.

   - **Column groups**: Some tables have the capability to group the table results by any column heading. This feature is available when the blue text “Drag a column heading here to group by that column” appears above the column headings. To group the results by column heading, you drag the heading of the column to group on to the Drag a column heading here area.

See “About the table pane” on page 61.

See “Viewing and editing the object details” on page 69.
Viewing and editing the object details

You can view and edit some of the object details from the details pane or from the details dialog box. The object details are grouped and displayed in tabs. Not all object details can be edited.

You can also select multiple objects to edit. Select the check box next to the objects that you want to edit. When you edit multiple objects, the previous values of all the selected objects are replaced with the new values.

To view and edit the object details in the details pane

1. In the table pane, select the object.
2. In the details pane, the object details are shown grouped in various tabs.
3. Select the required tab and edit the details.
4. Click the Save icon.

To view and edit the object details using the details dialog box

1. In the table pane, select the check box next to the object.
2. Do one of the following:
   - Click Edit Details in the taskbar.
   - Double-click the object.
   - Right-click the object, and click Details.
3. In the details dialog box, edit the details if required.
4. Click Save.

See “About the table pane” on page 61.
See “Managing the table pane” on page 68.

Selecting the columns headings

You can select the column headings that you want to see or hide in the table pane.

To select the column headings

1. In the view, click the column chooser icon.
2. In the Column Chooser dialog box, check the column headings.

See “About the table pane” on page 61.
Refreshing the view

You can refresh the view to update the currently displayed information with new information.

To refresh the view
◆ Do one of the following:
  ■ On the keyboard, press F5.
  ■ In the Menu bar, click View > Refresh.

See “About the console features” on page 57.

Searching for objects

You can perform a quick search or an advanced search to search for an object in the table pane. The search is performed on the contents of the selected folder in the tree pane. The type of objects you can look for depends on the current view. For example, if you are in the Standards view, you can search for standards, sections, checks, or all three.

When searching for assets in the Assets view, you can only search for the assets that are displayed in the table pane. You cannot search for the assets that are in the asset store.

See “Asset folder hierarchy” on page 234.

To perform a quick search
1 In the table pane, in the Search text box, type a text string.
2 To narrow the search to a certain type, select the type from the Search drop-down box.
3 Click the Search icon.

To perform an advanced search
1 In the table pane, click the Expand icon that is on the top-right of the table pane.
2 In the Advanced Search pane, select the details and click Search.

See “About the console features” on page 57.

About working in the tree pane

The tree pane provides a context menu for doing the common tasks on the folders. The menu options that are displayed are different in each view. Right-click the folder in the tree pane and the context menu appears.
The following common tasks are available in most views:

- **Move folder**
  See “Moving folders in the tree pane” on page 72.

- **Create new folder**
  See “Creating folders in the tree pane” on page 71.

- **Delete folder**
  See “Deleting folders in the tree pane” on page 72.

- **Rename folder**
  See “Renaming folders in the tree pane” on page 73.

- **Refresh folder**
  See “Refreshing folders in the tree pane” on page 73.

See “About the tree pane” on page 60.

---

### Creating folders in the tree pane

You create folders to organize the business objects in a hierarchical manner.

**To create a folder in the tree pane**

1. In the tree pane, right-click the root folder or an existing folder.
2. Select **New Folder**.
3. In the **Create New Folder** dialog box, type the name of the folder.
4. Click **OK**.

See “About using special characters in folder and job names” on page 71.

See “Creating the asset folders” on page 375.

See “About the tree pane” on page 60.

---

### About using special characters in folder and job names

When you create folders in the tree pane from any view, you need to ensure that you do not use certain special characters. The usage of special characters is not allowed in cases where a folder is created dynamically by the name of some value.

Consider the following example:

You create a Post Rule. Add an action to move the assets to the folder. You choose to create the folder dynamically based on the name of the value of the selected field. In this case, if the value of the field contains a special character that is not supported the folder is created with a different name.
Note: If a folder name contains a special character that is not supported by Control Compliance Suite, the character is replaced with - (hyphen).

Control Compliance Suite does not support the following special characters in the folder name and the job name:

- *
- ( 
- )
- \ 
- /
- ,
- +
- "
- <
- >
- ;
- =
- #
- \r

See “Creating folders in the tree pane” on page 71.

Moving folders in the tree pane

The move feature lets you easily change the location of a folder in the tree pane. When you move a folder, all the child folders are also moved.

To move a folder in the tree pane

1. In the tree pane, right-click the folder to move and select the Move task.
2. In the Move dialog box, select the new location in the tree pane.
3. Click OK.

See “About working in the tree pane” on page 70.

Deleting folders in the tree pane

When you delete a folder, all the child folders and objects are deleted.
To delete a folder in the tree pane
1 In the tree pane, right-click the folder to delete.
2 Select the Delete task.
3 In the message dialog box, click OK.
See “About the tree pane” on page 60.

Renaming folders in the tree pane
You can rename a folder in the tree pane.
To rename a folder in the tree pane
1 In the tree pane, right-click the folder to rename.
2 Select the Rename task.
3 In the Rename dialog box, type the new name of the folder.
4 Click OK.
See “About the tree pane” on page 60.

Refreshing folders in the tree pane
You must refresh the folder to display any changes in the directory objects.
To refresh a folder in the tree pane
1 In the tree pane, right-click the folder to refresh.
2 Select the Refresh task.
See “About the tree pane” on page 60.

Optimizing the console layout
When working in a view you can choose to show or hide the tree pane, filter pane, table pane, and details pane. By optimizing the layout of the view you can create more work area and focus on your current area of interest. For example, once you've set your filter options, you can hide the filter pane to increase the display area of tree pane, table pane, and the details pane.
The show or hide option is available only for certain views of the console.
To optimize the console layout

1. Go to the view you want to work in.
2. On the menu bar, click **View > Show/Hide**.
3. Select the pane you want to hide.

   You click the same option again to show the pane. This action acts like a toggle.

   The name of the pane varies depending on the view.
This chapter includes the following topics:

- Quick start with minimum configuration
- Configuration tasks
- Managing certificates
- Configuring roles and permissions
- Registering and configuring the Data Processing Service
- Working in the System Topology view
- Configuring sites
- Configuring the data collectors
- Configuring the application server settings
- About the security settings for scheduled jobs
- Adding credentials for scheduled jobs
- Configuring the general settings
- About audits
- Managing licenses
- Managing users
- Configuring the SQL Server settings
Quick start with minimum configuration

The quick start helps you to get started with the minimum initial configuration that is required to collect and evaluate data, and to view the reports with compliance information.

The quick start applies to single setup mode installation.

The Configuration tasks topic provides more information and links to procedures that help you configure the system to suit your organization's infrastructure.

See “Configuration tasks” on page 77.

Table 3-1  Tasks to get you started with Control Compliance Suite (CCS)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register installed Data Processing Service</td>
<td>You must register the Data Processing Service (DPS) with the application server. When you register the DPS, you also assign the DPS to the default site or create your own site and specify the DPS roles. Where appropriate, specify data types to collect.</td>
</tr>
<tr>
<td></td>
<td>See “Registering the DPS with minimum custom configuration” on page 117.</td>
</tr>
<tr>
<td>Create asset folders (optional)</td>
<td>You can store the objects in the default Asset System folder that is created when you install CCS or create user-defined folders. If you store objects in the default Asset System folder, you can later use the reconciliation rules to move the objects to a user-defined folder structure. The user-defined folders help to store business objects in a hierarchical manner that reflects your organizational structure. The user-defined folders let you effectively assign permissions.</td>
</tr>
<tr>
<td></td>
<td>See “Creating the asset folders” on page 375.</td>
</tr>
</tbody>
</table>
Table 3-1  Tasks to get you started with Control Compliance Suite (CCS)  
(continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create asset import reconciliation rules</td>
<td>Reconciliation rules let you filter the potential assets before they enter the asset system. The reconciliation rules also help to update the field values of the existing assets. You can use the predefined reconciliation rules or create your own reconciliation rules to filter the assets. See “Reconciliation rules and rule types” on page 276. See “Working with reconciliation rules scenarios” on page 308. See “Creating reconciliation rules without manual review” on page 306.</td>
</tr>
<tr>
<td>Create an asset import job</td>
<td>You must import assets from the network before you can collect data from the assets and evaluate the assets against specific standards and checks. See “Importing the assets for the first time” on page 319.</td>
</tr>
<tr>
<td>Create a common data collection, data</td>
<td>After you have imported the assets, you create a job to collect, evaluate, and report data from the imported assets. See “Running a collection-evaluation-reporting job from the Asset System view” on page 385.</td>
</tr>
<tr>
<td>evaluation, and a reporting job</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Run Scheduled Reporting</td>
<td>In order to see data, you must run the Scheduled Reporting Synchronization Job from the Monitor &gt; Jobs view before you open a report, dashboard or panel for the first time. See “Running a job now” on page 719.</td>
</tr>
<tr>
<td>Synchronization Job</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View a report</td>
<td>You can now view the report.</td>
</tr>
</tbody>
</table>

Configuration tasks

The administrator must perform certain tasks before the system users can use Control Compliance Suite (CCS) to collect and report on the compliance data from across the organization.

You can access the Configuration tasks topic from the Help > Configuration menu item.

You do the following tasks to configure CCS. Click on the links to learn more about how to perform each task.
See Table 3-2 on page 78.

See Table 3-3 on page 79.

See Table 3-4 on page 80.

See Table 3-5 on page 80.

**Table 3-2**  
Initial configuration tasks

<table>
<thead>
<tr>
<th>Tasks and links</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create asset folders in the Manage &gt; Asset System view.</td>
<td>The user-defined folders store business objects in a hierarchical manner that reflects your organizational structure. The user-defined folders let you effectively assign permissions. When you install CCS, a default hierarchy structure is created to store objects. Users should organize the tree to follow the flow of control in the organization. See “Creating the asset folders” on page 375.</td>
</tr>
<tr>
<td>Assign users to roles.</td>
<td>The role determines what you can see and perform in the CCS Console. In addition to the role, you must have permission on the required folders and objects to successfully perform a task. See “Adding users and groups to a role” on page 107.</td>
</tr>
<tr>
<td>Assign permissions to trustees.</td>
<td>You must manually assign permissions to the user-defined folders. When a role is assigned to a user, permissions are automatically granted to the objects in the predefined folders. See “Assigning permissions from the Permission Management view” on page 113.</td>
</tr>
<tr>
<td>Create sites to match the structure in the deployment plan.</td>
<td>You create sites to manage logical groups of assets. Grouping of assets facilitate data collection and other CCS operations. See “Creating a site” on page 136.</td>
</tr>
<tr>
<td>Register installed Data Processing Service instances.</td>
<td>Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register the DPS, you also assign the DPS to a site and specify the DPS roles. Where appropriate, specify data types to collect. See “Registering the Data Processing Service” on page 115.</td>
</tr>
</tbody>
</table>

You do the following tasks to discover assets, and then collect and evaluate data from the imported assets.
## Table 3-3  
### Assets, data collection, and evaluation tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description and task links</th>
</tr>
</thead>
</table>
| Create asset import reconciliation rules as specified in the deployment plan. | The reconciliation rules let you filter the potential assets before they enter the asset system. The reconciliation rules also help to update the field values of the existing assets.  
  See “Creating reconciliation rules using the manual review” on page 307.  
  See “Creating reconciliation rules without manual review” on page 306. |
| Create asset import jobs.                 | You must import assets from the network before you can collect data from the assets and evaluate the assets against specific standards and checks.  
  You can import the assets in one of the following ways:  
  See "Importing the assets for the first time" on page 319.  
  See "Importing asset-specific fields from the default data collector" on page 329.  
  See "Importing asset-specific and common fields using the default data collector" on page 332.  
  See "Importing asset-specific and common fields using the CSV data collector" on page 335.  
  See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338.  
  See “Working with asset import scenarios” on page 321. |
| Set up data collection jobs.              | After you have imported the assets you create jobs to collect data from the imported assets.  
  See “Setting up a data collection job from the Assets view” on page 380. |
| Create evaluation jobs.                  | After you have collected the data from the imported assets you create jobs to evaluate the assets.  
  See “Running an evaluation job from the Asset System view” on page 383. |

You do the following tasks to discover control points and create reports and dashboards.
### Table 3-4  Entitlements, reports, and dashboards tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description and task links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark and configure entitlement control points.</td>
<td>You mark an asset as a control point to monitor the entitlements of the asset through the approval workflow.</td>
</tr>
<tr>
<td></td>
<td>See “Marking an asset as a control point” on page 378.</td>
</tr>
<tr>
<td></td>
<td>You configure a control point to assign a data owner, an approver, the tags, and the review cycle to the control point</td>
</tr>
<tr>
<td></td>
<td>See “Configuring control points” on page 501.</td>
</tr>
<tr>
<td>Create report jobs.</td>
<td>The report job generates a report with the data from the reporting database.</td>
</tr>
<tr>
<td></td>
<td>You must synchronize the reporting database to view the latest data before you run a report job.</td>
</tr>
<tr>
<td></td>
<td>The Reporting Database Synchronization job is an existing job in the Monitor &gt; Jobs view.</td>
</tr>
<tr>
<td></td>
<td>See “Running a job now” on page 719.</td>
</tr>
<tr>
<td></td>
<td>See “Scheduling a report” on page 746.</td>
</tr>
<tr>
<td>Create dashboard jobs.</td>
<td>The dashboard job generates the dashboard with the data from the reporting database.</td>
</tr>
<tr>
<td></td>
<td>In order to see data, you must run the Scheduled Reporting Synchronization Job from the Monitor &gt; Jobs view before you open a dashboard or panel for the first time.</td>
</tr>
<tr>
<td></td>
<td>The Reporting Database Synchronization Job is an existing job in the Monitor &gt; Jobs view.</td>
</tr>
<tr>
<td></td>
<td>See “Running a job now” on page 719.</td>
</tr>
</tbody>
</table>

You do the following tasks to create and publish policies across the organization.

### Table 3-5  Policies and RAM tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description and task links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create policies.</td>
<td>Policies are rules established by an organization. Policies are designed to guide their employees. You can create a policy from scratch or import a Microsoft Word document as a policy.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a new policy” on page 693.</td>
</tr>
<tr>
<td></td>
<td>See “Importing a Word policy” on page 695.</td>
</tr>
</tbody>
</table>
### Table 3-5  Policies and RAM tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description and task links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish policies.</td>
<td>After a policy is created and approved, the policy is published to the selected audience members in the organization. The audience members can access the policy from the CCS Web Console. See “Publishing a policy” on page 704.</td>
</tr>
</tbody>
</table>

## Managing certificates

In Control Compliance Suite (CCS), a unique certificate is created for each installable component on each host. Certificates secure the environment by using a unique identifier for communications between CCS core components. The Certificate Management Console manages the certificates. In a distributed system, you create the application server certificate or the Data Processing Service (DPS) certificate manually using the console. The application server certificate is unbound until the component is installed. The DPS certificate is unbound until registered in the System Topology in the CCS console.

If any host or certificate becomes compromised, the compromised single certificate can be unbound using the Certificate Management Console. When the certificate is unbound, the compromised component can communicate with other CCS components. The `Symcert untrust` command places the certificate in an untrusted store and revokes communications with that certificate. The certificate of the single component must be regenerated and bound with the Control Compliance Suite system, and the component is fully functional again.

You can review the certificates in the following locations:
- **Certificates** view in the CCS Console
- **Certificate Management Console**

See “About Encryption Management Service” on page 82.
See “About the Certificates view” on page 82.
See “About the Certificate Management Console” on page 86.
See “Registering the Data Processing Service” on page 115.
About Encryption Management Service

Encryption Management Service is responsible for securely encrypting sensitive data.

The Certificate Management Console is installed on the same system as Encryption Management Service to manage certificates. Using the console, users can create, renew, bind, unbind, or remove certificates.

Symcert is a command-line utility for installing and removing certificates on CCS component systems. The utility is installed and automatically executed when a certified component is installed. Symcert functions add or remove component certificates in the computer’s certificate store. Symcert adds necessary certificate data to the component’s configuration file. The certificate data in the configuration file is read on service start and defines which CCS systems trust the component. Symcert can also be used to review certificate data for all of the CCS components that are installed on a local system. Symcert may be used in disaster recovery or migration scenarios without the expense of complete deployment of the DPS systems. Using Symcert CCS components can be updated with new certificates issued by the Certificate Management Console or from a different CCS root authority. The syntax for Symcert is available at the command line.

The Certificate MMC Snap-in component should not be used to install or remove CCS component certificates.

See “About the Certificates view” on page 82.

See “Using the Certificate Management Console” on page 85.

About the Certificates view

The Certificates view lists the certificates that have not been removed from the system. You can review the specific properties for each certificate.

You can do the following:

■ Search for a specific certificate by any of the certificate properties
■ Clear the results of the search
■ Use Column Chooser to select if specific columns are visible
■ Quickly view the number of certificates that are available in the view and for each of the categories

You can rearrange the columns for the view. If you rearrange the columns, the rearranged layout does not persist. The columns return to their default locations when you open or refresh the view.
If you want to modify a certificate, you must use the **Certificate Management Console**.

You can view the following categories:

<table>
<thead>
<tr>
<th>Table 3-6 Categories and descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>Bound</td>
</tr>
<tr>
<td>Root Certificate</td>
</tr>
<tr>
<td>Unbound</td>
</tr>
<tr>
<td>Disabled/Unbound</td>
</tr>
</tbody>
</table>

The **Disabled/Unbound** status is used for the certificates that should no longer be bound due to the uninstallation of a component. A certificate with this status can safely be removed. You can rebind a certificate in the **Disabled/Unbound** state in the **Certificate Management Console**. **Disabled/Unbound** DPS certificates may only be bound if the component has been registered in the CCS Console.

You can review the following properties for each certificate:

<table>
<thead>
<tr>
<th>Table 3-7 Certificate properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Component Name</td>
</tr>
<tr>
<td>Expiration Date</td>
</tr>
<tr>
<td>Host Name</td>
</tr>
<tr>
<td>Serial Number</td>
</tr>
</tbody>
</table>

See “**About the Certificate Management Console**” on page 86.

**About managing certificates using the command line**

**Symcert** is a command-line utility for installing and removing certificates on CCS component systems. The utility is installed and automatically executed when a certified component is installed. **Symcert** functions add or remove component certificates in the computer’s certificate store. Certificate data is also added or removed from the services configuration file. The certificate data in the configuration file is read on service start and defines which CCS systems are
trusted by the component. Symcert can also be used to read certificate data for all of the CCS components that are installed on a local system. Symcert may be used in disaster recovery or migration scenarios without the expense of complete deployment of the DPS systems. Using Symcert the systems can be updated with certificates from a different root authority. The syntax for Symcert is available at the command line.

See “About Encryption Management Service” on page 82.
See “About the Certificates view” on page 82.
See “Using the Certificate Management Console” on page 85.

About creating certificates

You create certificates in the Certificate Management Console. You create the certificate based on the service type and you can create several certificates sequentially. Certain information is reused as the default selections from the previous certificate, but all of the information can be edited. Every item in the Create Certificates dialog box is required. The information is not validated. You can be an ADAM administrator or have the "Manage Configuration Settings" task in your role to create certificates. You should be a local administrator and be a member of the Control Compliance Suite (CCS) administrator role.

**Note:** Computer names should not use any characters that are invalid for a DNS name. The list of characters that are not allowed is available at the following location:

http://support.microsoft.com/kb/909264

Each CCS component has a host registration in ADAM. In a single system installation, the certificates are created but you must manually bind the Data Processing Service (DPS) certificate. In a distributed system installation, you create the application server and DPS certificates manually. The application server certificate is unbound until the component is installed. The DPS certificate is unbound until registered in System Topology in the CCS console.

When you open the Certificate Management Console, you may be prompted to provide the root certificate password. The password is created during the installation of Control Compliance Suite. The password is not required if you have previously opened the console. The password is also not required if you are logged on in the context of the user who installed CCS.

You can find a list of the two-character codes at:
About certificate encryption

You create a certificate that uses the Secure Hash Algorithm (SHA) set of cryptographic hash functions. The National Security Agency (NSA) designed the set of functions. The National Institute of Standards and Technology (NIST) publish the set of functions as a Federal Information Processing Standard.

Windows XP and Server 2003 cannot obtain certificates using SHA-2 algorithms unless the operating systems have been updated with the appropriate Windows hotfix. You should review the Microsoft solution to be sure that it is appropriate for your organization.

When you create a certificate for use on a Windows Server 2003 system the password length is limited to a maximum of 31 characters. Certificates that are created for Windows Server 2008 systems may have passwords up to 255 characters.

### Table 3-8 Available signature algorithms and key size selections

<table>
<thead>
<tr>
<th>SHA hash functions</th>
<th>key size</th>
<th>key size</th>
<th>key size</th>
</tr>
</thead>
<tbody>
<tr>
<td>sha1RSA</td>
<td>2048</td>
<td>3072</td>
<td>4096</td>
</tr>
<tr>
<td>sha256RSA</td>
<td>2048</td>
<td>3072</td>
<td>4096</td>
</tr>
<tr>
<td>sha384RSA</td>
<td>2048</td>
<td>3072</td>
<td>4096</td>
</tr>
<tr>
<td>sha512RSA</td>
<td>2048</td>
<td>3072</td>
<td>4096</td>
</tr>
</tbody>
</table>

If you create a certificate with stronger hash function or larger key size, the creation process may take more time on certain computers.

See “About creating certificates” on page 84.

See “Creating a certificate” on page 89.
Console cannot be accessed remotely. You must be logged on to the system that hosts the Encryption Management Services to access the Certificate Management Console. Any user can open the Certificate Management Console to review the certificates.

A user can be a local administrator and an ADAM administrator and know the root certificate password to manage certificates. If the user is not an ADAM administrator, the user must have the "Manage Configuration Settings" task in the role.

Table 3-9 describes the typical certificate lifecycle.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation</td>
<td>You create the certificate based on the service type.</td>
<td>See “Creating a certificate” on page 89.</td>
</tr>
<tr>
<td>Renewal</td>
<td>You can renew the certificate, which extends the life of the certificate.</td>
<td>See “Renewing certificates” on page 91.</td>
</tr>
<tr>
<td>Bind</td>
<td>In certain circumstances, you can bind a certificate. The system trusts a component with a bound certificate.</td>
<td>See “Binding a certificate” on page 92.</td>
</tr>
<tr>
<td>Unbind</td>
<td>A certificate can become invalid before the expiration date. Under such circumstances, you should unbind the certificate.</td>
<td>See “Unbinding certificates” on page 93.</td>
</tr>
<tr>
<td>Removal</td>
<td>You should remove the disabled/unbound certificates or expired certificates when you perform a periodic system cleanup.</td>
<td>See “Removing a certificate” on page 94.</td>
</tr>
</tbody>
</table>

See “Managing certificates” on page 81.

About the Certificate Management Console

The Certificate Management Console (CMC) is used to manage certificates for Control Compliance Suite. The console is installed on the same system as the Encryption Management Services. The console cannot be accessed remotely. You must be logged on to the system that hosts the Encryption Management Services to access the CMC. Any user can open the CMC to review the certificates.

You can Search on any of the properties. You can Clear the results of the search.
Table 3-10  Certificate properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Name</td>
<td>The component that is used during the certificate creation.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Date and time when the certificate is no longer valid</td>
</tr>
<tr>
<td>Host Name</td>
<td>The fully qualified domain address for the component</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number is a unique identifier for a certificate. The number lets you identify a certificate if multiple certificates exist for the same component.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the certificate. The types of status are described in Table 3-11</td>
</tr>
</tbody>
</table>

Table 3-11  Status types and descriptions

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bound</td>
<td>The certificate is connected to a certain component</td>
</tr>
<tr>
<td>Root Certificate</td>
<td>The top level of the certificate hierarchy</td>
</tr>
<tr>
<td>Unbound</td>
<td>The certificate is not connected to a component</td>
</tr>
<tr>
<td>Disabled/Unbound</td>
<td>The certificate is no longer needed but not removed</td>
</tr>
</tbody>
</table>

The **Disabled/Unbound** status is used for the certificates that should no longer be bound due to the uninstall of a component. A certificate with this status can safely be removed. You can rebind a certificate in the **Disabled/Unbound** state in the Certificate Management Console. **Disabled/Unbound** DPS certificates may only be bound if the component has been registered in the CCS Console.

A certificate that is removed no longer is available to the system and is not visible in the CMC.

You can do a search on the certificates on any of the columns. You can drag a column header to group the certificates by that column.

A user can be a local administrator but must be an ADAM administrator and know the root certificate password to do the following:

- Create certificates
- Renew certificates
- Bind certificates
- Unbind certificates
### Remove certificates

In the CMC, the user activates a certificate by selecting the appropriate check box. After the check box has been selected, the user can renew, unbound, or remove a certificate. A certificate that is unbound but not removed has a status of disabled/unbound.

The type of installation determines the number of certificates that are created automatically. A directory service (DSS) installation always creates the root certificate. The DSS install also creates and binds the Management Service certificate. The DSS installation does not create the certificates that are needed to install the application server or the DPS servers. You must create the service type certificate for each installed component. For example, if your system has 50 DPS components, you must create 50 certificates. Each CCS component has a host registration in ADAM. In a single system installation, the certificates are created and bound for each component during installation. The DPS certificate is not bound during the single system installation. The certificate is created but its host record is not created during installation so the certificate cannot be bound until the DPS registration occurs. The registration process both creates the host record and binds the certificate to the host record. In a distributed installation, you create the application server and DPS certificates manually using the **Certificate Management Console**. The application server certificate is unbound until the component is installed. The DPS Certificate is unbound until registered in **System Topology** in the **CCS Console**.

In a single system installation, the following certificates are created automatically:

<table>
<thead>
<tr>
<th>CA</th>
<th>Root certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ManagementServices-&lt;computer name&gt;</td>
<td>Bound</td>
</tr>
<tr>
<td>AppServer-&lt;computer name&gt;</td>
<td>Bound</td>
</tr>
<tr>
<td>AppServerSSL-&lt;computer name&gt;</td>
<td>Bound</td>
</tr>
<tr>
<td>DPS-&lt;computer name&gt;</td>
<td>Unbound</td>
</tr>
</tbody>
</table>

In a distributed installation, the following certificates are created:

<table>
<thead>
<tr>
<th>CA</th>
<th>Root certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ManagementServices-&lt;computer name&gt;</td>
<td>Bound</td>
</tr>
</tbody>
</table>

See “Using the Certificate Management Console” on page 85.
Creating a certificate

You create the certificate based on the service type. You can create multiple certificates. Certain information is reused from the previous certificate, but all of the information can be edited. Every item in the Create Certificates dialog box is required. The information is not validated. You must be an ADAM administrator to create certificates. We recommended that you are also a local administrator and a Control Compliance Suite (CCS) administrator.

Table 3-12 Certificate options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>The available Service Type names are the following:</td>
<td>DPS</td>
</tr>
<tr>
<td></td>
<td>■ DPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Application Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Application Server (SSL Only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Encryption Management Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can only create the Encryption Management Service certificate on the computer that hosts the Directory Support Service.</td>
<td></td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>A mathematical scheme that demonstrates the authenticity of a digital message.</td>
<td>The signature algorithm that is selected at installation time for the Root certificate.</td>
</tr>
<tr>
<td></td>
<td>You can find a list of the available signature algorithms and the key sizes in See “About certificate encryption” on page 85.</td>
<td></td>
</tr>
<tr>
<td>Key Size</td>
<td>The length that is used in the cryptographic algorithm.</td>
<td>The key size that is selected at installation time for the Root certificate.</td>
</tr>
<tr>
<td></td>
<td>You can find a list of the available signature algorithms and the key sizes in See “About certificate encryption” on page 85.</td>
<td></td>
</tr>
<tr>
<td>Expires In</td>
<td>The number of years before the certificate expires</td>
<td>25</td>
</tr>
</tbody>
</table>
### Table 3-12 Certificate options (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization</strong></td>
<td>You can accept the value from a previous certificate or you can provide your own.</td>
<td>The information from the previous certificate.</td>
</tr>
<tr>
<td><strong>Division</strong></td>
<td>You can accept the value from a previous certificate or you can provide your own.</td>
<td>The information from the previous certificate.</td>
</tr>
<tr>
<td><strong>City</strong></td>
<td>You can accept the value from a previous certificate or you can provide your own.</td>
<td>The information from the previous certificate.</td>
</tr>
<tr>
<td><strong>State/Province</strong></td>
<td>You can accept the value from a previous certificate or you can provide your own.</td>
<td>The information from the previous certificate.</td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>You can accept the value from a previous certificate or you can provide your own.</td>
<td>The information from the previous certificate.</td>
</tr>
<tr>
<td><strong>NetBIOS Name</strong></td>
<td>You can use <strong>Browse</strong> to add a name. The NetBIOS Name must be less than 16 bytes in length.</td>
<td>None</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Populated from the NetBIOS Name selection.</td>
<td>None</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Populated from the NetBIOS Name selection.</td>
<td>None</td>
</tr>
<tr>
<td><strong>(*) plus icon</strong></td>
<td>Add multiple TCP/IP address</td>
<td>None</td>
</tr>
<tr>
<td><strong>Destination folder</strong></td>
<td>You can accept the value from a previous certificate or you can provide your own.</td>
<td><code>&lt;InstallDir&gt;\ManagementServices\DefaultCerts</code></td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password for the certificate. You must use this password to modify the certificate.</td>
<td>None</td>
</tr>
<tr>
<td><strong>Retype Password</strong></td>
<td>Confirm the password</td>
<td>None</td>
</tr>
</tbody>
</table>
To create a certificate

1. Click Start > All Programs > Symantec Corporation > Symantec Control Compliance Suite > Certificate Management Console.

2. Provide the Root Certificate Password and click OK, if needed. The password is used during installation.

3. In the Certificate Management Console taskbar, click Create Certificates.

4. In the Create Certificates dialog box, complete the form. All of the information is required. You can view the option name and descriptions in Table 3-12.

5. If the certificate has the same name as an existing file, you are asked if you want to overwrite the file, click Yes.

6. In the Success message box, click OK.

7. In the Create Certificate message box, click Yes to create another certificate, if needed.

See “About certificate encryption” on page 85.

See “About creating certificates” on page 84.

Renewing certificates

If a particular certificate is about to expire, you can renew the certificate. A renewal extends the date of the certificate. You must know the location and password for the current version to renew the certificate. You cannot change the password. The default value for the renewal is 25 years. When the certificate is renewed, its new expiration date must be less than January 1, 2038. The Expires In selection adds the number of years to the number of years that remain for that certificate.

When you open the console, you may be prompted to provide the root certificate password. The password is created during the installation of Control Compliance Suite (CCS).

The root certificate password is not required if either of the following conditions have occurred:

- You have previously opened the console
- You are logged on in the context of the user who installed CCS

All information in the Renew Certificate dialog box is required.
Table 3-13  Renew Certificate options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Certificate</td>
<td>Location of the current certificate. You can use <strong>Browse</strong> to navigate to the location.</td>
<td>None</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is assigned to the certificate during the certificate creation.</td>
<td>None</td>
</tr>
<tr>
<td>Destination folder</td>
<td>The folder to store the certificate. You can accept the current location or provide another location You can use <strong>Browse</strong> to navigate to a location.</td>
<td><code>&lt;InstallDir&gt;\ManagementServices\DefaultCerts</code></td>
</tr>
<tr>
<td>Expires In</td>
<td>The number of years for the certificate's lifetime</td>
<td>25</td>
</tr>
</tbody>
</table>

See “Managing certificates” on page 81.
See “Using the Certificate Management Console” on page 85.
See “Unbinding certificates” on page 93.
See “Removing a certificate” on page 94.

To renew a certificate

1 Click **Start > All Programs > Symantec Control Compliance > Certificate Management Console**.
2 Provide the **Root Certificate Password** and click **OK**, if needed.
   The password is used during installation.
3 In the **Certificate Management Console**, select the check box for the appropriate certificate and then click **Renew Certificates**.
4 In the **Renew Certificate** dialog box, complete the form. The description for the options is available in Table 3-13
5 Click **Renew Certificate**.
6 In the **Success** message box, click **OK**.

**Binding a certificate**

If you have registered a component in the CCS Console, and you have unbound the certificate for that component, you can bind the certificate. The certificate status changes to **Bound**.
The DPS certificate cannot be bound if the DPS has not been registered in the console. The certificate is bound when you register the DPS. The application server certificate cannot be bound if the application server has not been installed. The certificate is bound during the installation. A new DPS certificate can be bound in the Certificate Management Console if that DPS is registered. An application server certificate can be bound in the Certificate Management Console if the application server is installed.

When you open the Certificate Management Console, you may be prompted to provide the root certificate password. The password is created during the installation of Control Compliance Suite (CCS).

The root certificate password is not required if either of the following conditions have occurred:

- You have previously opened the console
- You are logged on in the context of the user who installed CCS

**Note:** You must use Symcert on the component’s computer to remove the old certificate and add the new certificate to the component.

**To bind a certificate**

1. Click **Start > All Programs > Symantec Control Compliance > Certificate Management Console**.
   
   The password is used during installation.
3. In the **Certificate Management Console**, select the check box for the appropriate certificate and then click **Bind Certificates**.

See “About managing certificates using the command line” on page 83.

**Unbinding certificates**

Certificates are issued with a planned lifetime. That lifetime is defined when the certificate is created and the certificate is valid until its expiration date. Under a variety of circumstances, you can unbind the certificate, if needed. The certificate status is changed to **Disabled/Unbound**. If the certificate is unbound, the component can communicate. The user should log on to the component's computer and use the **Symcert untrust** command. The command places the certificate in an untrusted store and revokes communications. The certificate status is changed to disabled/unbound.
When you open the Certificate Management Console, you may be prompted to provide the root certificate password. The password is created during the installation of Control Compliance Suite (CCS).

The root certificate password is not required if either of the following conditions have occurred:

- You have previously opened the console
- You are logged on in the context of the user who installed CCS

**To unbind a certificate**

1. Click **Start > All Programs > Symantec Control Compliance > Certificate Management Console**.
   - The password is used during installation.
3. In the **Certificate Management Console**, select the certificate.
4. Click **Unbind Certificates**.
5. In the **Warning** message box, click **Yes**.

See “Using the Certificate Management Console” on page 85.

See “Removing a certificate” on page 94.

**Removing a certificate**

You should remove the unbound or expired certificates when you perform a periodic system cleanup. A removed certificate is not visible in the **Certificates** view or **Certificate Management Console**. The file may exist in the assigned directory. If you have the **Certificates** view open, and remove a certificate in the **Certificate Management Console**, you must refresh the view before you see the change.

When you open the console, you may be prompted to provide the root certificate password. The password is created during the installation of Control Compliance Suite (CCS).

The root certificate password is not required if either of the following conditions have occurred:

- You have previously opened the console
- You are logged on in the context of the user who installed CCS

See “Managing certificates” on page 81.

See “Using the Certificate Management Console” on page 85.
To remove a certificate

1. Click Start > All Programs > Symantec Control Compliance > Certificate Management Console.
2. Provide the Root Certificate Password and click OK, if needed. The password is used during installation.
3. In the Certificate Management Console, select the check box for the appropriate certificate.
4. Click Remove Certificates.
5. In the Warning message box, click Yes.

Configuring roles and permissions

Control Compliance Suite (CCS) supports a combination of roles and permissions-based access control. When the users log on, they see only a filtered application that is based on their role. The role defines the access privileges for the views and tasks. The permissions that the user has on the objects in the CCS directory determine the tasks that the user can perform on an object.

Access control in CCS works in the following order:

- Related and relevant tasks are collected to define a role. Role and task association is predefined and cannot be modified.
- Roles are assigned to users or groups who access the application.
- Users are then assigned the permissions to objects to perform certain tasks. Only users with permissions can perform certain tasks on the objects.

CCS provides the interface to assign the predefined roles and permissions to the CCS users. If a user’s role assignment is modified, the user must quit and then restart the CCS console. When the console restarts, the user can see the new views and tasks that are associated with the role.

CCS also provides the facility to create custom roles if the predefined roles do not fit the needs of your organization.

See “About custom roles” on page 104.

See “About roles” on page 96.

See “About tasks” on page 97.
About roles

In Control Compliance Suite (CCS) a role is a collection of predefined tasks or functions. The user may perform each task that is a specific action, such as Create a policy or Run an evaluation. The role determines what a user can see and perform in the CCS console.

To have a role does not automatically grant the user the rights that are required to perform the task on the directory objects. In addition to the role, the user must have access rights on the required directory objects to successfully perform a task.

For example, if the user is in the Evaluators role, the user is allowed to set up and run evaluation jobs. But when the evaluation job is run, the results are based only on the assets for which the user has been granted the Evaluate permission.

CCS provides a number of predefined roles to suit your organizational needs. The predefined role and task association cannot be modified. However, CCS lets you create custom roles.

See “About custom roles” on page 104.
See “Predefined roles” on page 97.
See “About permissions” on page 96.
See “About tasks” on page 97.
See “Configuring roles and permissions” on page 95.

About permissions

Control Compliance Suite (CCS) lets you control which users have what access to which directory objects. When a user account is authenticated, the type of access granted to the objects is determined by the permissions that are attached to the objects.

When a role is assigned to a user, permissions are automatically granted to the directory objects in the predefined folders. The administrator must manually assign permissions to the user-defined folders at a later time.

Every directory object has a set of effective rights that is either assigned directly to or is inherited from the parent folder. The effective rights determine what kind of directory operations a specific user can perform on that object.
Objects are stored in the CCS directory. The directory is hierarchical in nature. You can create folders and objects in an inverted tree-like structure. The directory gives the user the flexibility to create a hierarchy that allows them to model the tree that is based on their organizational needs.

See “About roles” on page 96.

See “About tasks” on page 97.

See “Configuring roles and permissions” on page 95.

See “Predefined roles” on page 97.

About tasks

A task is an action that a user performs. CCS provides numerous tasks at a detailed level of granularity. For example, Create a policy or Run an evaluation are tasks provided by CCS. A collection of predefined tasks define a role. When a user is assigned to a role, the user can perform the tasks that are associated with the role.

See “About roles” on page 96.

See “Predefined roles” on page 97.

See “About permissions” on page 96.

See “Configuring roles and permissions” on page 95.

Predefined roles

Control Compliance Suite (CCS) includes several predefined roles that you can assign to users. These roles specify the level of interaction that the users have when they log on to the console.

An administrator can allow or block user access to features and functionality in the product by assigning different roles to the console users. Predefined roles cannot be edited.

Various CCS roles are based on the features and functionality of the product.
### Table 3-14  Administrative roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS Administrator</td>
<td>The CCS Administrator can perform most of the tasks in CCS.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In CCS v 10.0 the administrator can no longer review or approve policies. To review and approve policies, you must assign at least one user to the Policy Reviewer role and the Policy Approver role.</td>
</tr>
<tr>
<td>Power User</td>
<td>The Power User role lets the user do everything the CCS Administrator can do except the following tasks:</td>
</tr>
<tr>
<td></td>
<td>- Configure application.</td>
</tr>
<tr>
<td></td>
<td>- Manage audits.</td>
</tr>
<tr>
<td></td>
<td>- Manage licenses.</td>
</tr>
<tr>
<td></td>
<td>- Assign policy audience.</td>
</tr>
<tr>
<td></td>
<td>You can view the list of available tasks from the Settings &gt; Roles view.</td>
</tr>
<tr>
<td>Auditor</td>
<td>The Auditor role lets the user view the following:</td>
</tr>
<tr>
<td></td>
<td>- View all jobs.</td>
</tr>
<tr>
<td></td>
<td>- View assets and asset reconciliation rules.</td>
</tr>
<tr>
<td></td>
<td>- View baselines and baseline comparison results.</td>
</tr>
<tr>
<td></td>
<td>- View control points.</td>
</tr>
<tr>
<td></td>
<td>- View evaluation results.</td>
</tr>
<tr>
<td></td>
<td>- View notification templates.</td>
</tr>
<tr>
<td></td>
<td>- View roles and permissions.</td>
</tr>
<tr>
<td></td>
<td>- View policies, policy comments, and policy content.</td>
</tr>
<tr>
<td></td>
<td>- View reports and report templates</td>
</tr>
<tr>
<td></td>
<td>- View dashboards and tiered dashboards.</td>
</tr>
<tr>
<td></td>
<td>- View review cycles</td>
</tr>
<tr>
<td></td>
<td>- View standards</td>
</tr>
</tbody>
</table>

### Table 3-15  CCS user role and Policy Audience role

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS User</td>
<td>The CCS User role lets the user create dashboards in the Web console.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To view the assets in the dashboards, the CCS User must be assigned the Asset Viewer role and have permissions to the assets.</td>
</tr>
</tbody>
</table>
Table 3-15  CCS user role and Policy Audience role (continued)

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Policy Audience       | By default, all the authenticated CCS users have the Policy Audience role.  
                        | **Note:** When you upgrade from version 9.0.1 to 10.0, the Guest User role is removed in version 10.0. The user accounts of the Guest User role are now placed in the Policy Audience role.  
                        | The Policy Audience role lets the user do the following:  
                        |  ■ Accept or decline policies.  
                        |  ■ Request exceptions.  
                        |  ■ View policies and policy comments. |

Table 3-16  Assets roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Assets Viewer| The Assets Viewer role lets the user do the following:  
                        |  ■ View asset details.  
                        |  ■ View asset group details. |
### Table 3-17 Standards roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Standards Administrator | The Standards Administrator role lets the user do the following:  
  - Manage configuration settings.  
  - Manage standards, sections, and checks.  
  - Manage jobs.  
  - Collect data.  
  - Evaluate standards.  
  - Manage tags.  
  - Request exceptions.  
  - Generate reports.  
  - Manage tiered dashboards.  
  - View assets.  
  - View standards.  
  - View evaluation results.  
  - View roles and permissions.  
  - View reports and report templates.  
  - Customize report templates.  
  - View roles and permissions. |
| Standards Evaluator   | The Standards Evaluator role lets the user do the following:  
  - Manage jobs.  
  - Collect data.  
  - Evaluate standards.  
  - Manage jobs.  
  - Manage tags.  
  - Manage tiered dashboard.  
  - Request exceptions.  
  - Generate reports and dashboards.  
  - View evaluation results.  
  - View dashboards and reports.  
  - View assets.  
  - View standards.  
  - View and customize report templates. |
### Table 3-17  Standards roles (continued)

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation Administrator</td>
<td>The Remediator role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>- Collect data.</td>
</tr>
<tr>
<td></td>
<td>- Manage jobs.</td>
</tr>
<tr>
<td></td>
<td>- Execute remediation action.</td>
</tr>
<tr>
<td></td>
<td>- Evaluate standards.</td>
</tr>
<tr>
<td></td>
<td>- Evaluate assets.</td>
</tr>
<tr>
<td></td>
<td>- Manage jobs.</td>
</tr>
<tr>
<td></td>
<td>- Manage tags.</td>
</tr>
<tr>
<td></td>
<td>- Manage configuration settings</td>
</tr>
<tr>
<td></td>
<td>- Manage tiered dashboards</td>
</tr>
<tr>
<td></td>
<td>- Request exceptions.</td>
</tr>
<tr>
<td></td>
<td>- Generate reports.</td>
</tr>
<tr>
<td></td>
<td>- View configuration settings</td>
</tr>
<tr>
<td></td>
<td>- View tiered dashboards</td>
</tr>
<tr>
<td></td>
<td>- View reports and report templates.</td>
</tr>
<tr>
<td></td>
<td>- Customize report templates</td>
</tr>
<tr>
<td></td>
<td>- View evaluation results</td>
</tr>
<tr>
<td></td>
<td>- View assets.</td>
</tr>
<tr>
<td></td>
<td>- View standards.</td>
</tr>
</tbody>
</table>

### Table 3-18  Exception roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception Approver</td>
<td>The Exception Approver role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>- Approve exceptions.</td>
</tr>
<tr>
<td></td>
<td>- Manage tags.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The exception approver must have the required tasks and permissions to view assets.</td>
</tr>
<tr>
<td>Exception Requestor</td>
<td>The Exception Requestor role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>- Request exceptions on behalf of a user without an assigned CCS role.</td>
</tr>
<tr>
<td></td>
<td>- Manage tags.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The exception requestor must have the required tasks and permissions to add assets, standards, and entitlements.</td>
</tr>
</tbody>
</table>
### Table 3-19  Entitlements roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entitlements Administrator</strong></td>
<td>The Entitlements Administrator role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Manage the control points.</td>
</tr>
<tr>
<td></td>
<td>■ Assign the data owners and the alternate data owners to the control points.</td>
</tr>
<tr>
<td></td>
<td>■ Import entitlements.</td>
</tr>
<tr>
<td></td>
<td>■ Manage control points.</td>
</tr>
<tr>
<td></td>
<td>■ Manage users.</td>
</tr>
<tr>
<td></td>
<td>■ Manage review cycles.</td>
</tr>
<tr>
<td></td>
<td>■ Manage jobs.</td>
</tr>
<tr>
<td></td>
<td>■ Manage tags.</td>
</tr>
<tr>
<td></td>
<td>■ Manage tiered dashboards.</td>
</tr>
<tr>
<td></td>
<td>■ Manage users.</td>
</tr>
<tr>
<td></td>
<td>■ Request entitlements approval.</td>
</tr>
<tr>
<td></td>
<td>■ Request exceptions.</td>
</tr>
<tr>
<td></td>
<td>■ Customize report templates.</td>
</tr>
<tr>
<td></td>
<td>■ Manage configuration settings.</td>
</tr>
<tr>
<td></td>
<td>■ Update and view notification templates.</td>
</tr>
<tr>
<td></td>
<td>■ View assets and asset reconciliation rules.</td>
</tr>
<tr>
<td></td>
<td>■ View review cycles.</td>
</tr>
<tr>
<td></td>
<td>■ View control points.</td>
</tr>
<tr>
<td></td>
<td>■ View dashboards.</td>
</tr>
<tr>
<td></td>
<td>■ View reports and report templates.</td>
</tr>
<tr>
<td></td>
<td>■ View evaluation results.</td>
</tr>
<tr>
<td></td>
<td>■ View roles and permissions.</td>
</tr>
<tr>
<td></td>
<td>■ View tiered dashboards.</td>
</tr>
<tr>
<td><strong>Entitlements Data Owner</strong></td>
<td>The Entitlements Data Owner role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Request exceptions.</td>
</tr>
<tr>
<td></td>
<td>■ Manage entitlements.</td>
</tr>
<tr>
<td></td>
<td>■ Assign the alternate data owner to the control points.</td>
</tr>
<tr>
<td></td>
<td>■ View roles.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy Administrator</td>
<td>The Policy Administrator role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Manage policies.</td>
</tr>
<tr>
<td></td>
<td>■ Manage jobs.</td>
</tr>
<tr>
<td></td>
<td>■ Manage tags.</td>
</tr>
<tr>
<td></td>
<td>■ Manage policy comments.</td>
</tr>
<tr>
<td></td>
<td>■ Manage policy clarifications.</td>
</tr>
<tr>
<td></td>
<td>■ Manage policy content.</td>
</tr>
<tr>
<td></td>
<td>■ Manage tiered dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Request exceptions.</td>
</tr>
<tr>
<td></td>
<td>■ Publish policies.</td>
</tr>
<tr>
<td></td>
<td>■ Manage configuration settings.</td>
</tr>
<tr>
<td></td>
<td>■ Customize report templates.</td>
</tr>
<tr>
<td></td>
<td>■ Generate reports.</td>
</tr>
<tr>
<td></td>
<td>■ View assets.</td>
</tr>
<tr>
<td></td>
<td>■ View standards.</td>
</tr>
<tr>
<td></td>
<td>■ View policies, policy comments, and policy content.</td>
</tr>
<tr>
<td></td>
<td>■ View dashboards.</td>
</tr>
<tr>
<td></td>
<td>■ View reports and report templates.</td>
</tr>
<tr>
<td></td>
<td>■ View roles and permissions.</td>
</tr>
<tr>
<td></td>
<td>■ View tiered dashboard</td>
</tr>
<tr>
<td>Policy Approver</td>
<td>The Policy Approver role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Approve policies.</td>
</tr>
<tr>
<td></td>
<td>■ Manage policy comments.</td>
</tr>
<tr>
<td></td>
<td>■ View asset and asset group details.</td>
</tr>
<tr>
<td></td>
<td>■ View policy and policy content details.</td>
</tr>
<tr>
<td></td>
<td>■ View roles.</td>
</tr>
<tr>
<td>Policy Reviewer</td>
<td>The Policy Reviewer role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Manage policy comments.</td>
</tr>
<tr>
<td></td>
<td>■ Review policies.</td>
</tr>
<tr>
<td></td>
<td>■ View asset and asset group details.</td>
</tr>
<tr>
<td></td>
<td>■ View policy, policy comments, and policy content details.</td>
</tr>
<tr>
<td></td>
<td>■ View roles.</td>
</tr>
</tbody>
</table>
Table 3-21  Reports and dashboards roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting Administrator</td>
<td>The Reporting Administrator role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Generate reports.</td>
</tr>
<tr>
<td></td>
<td>■ Customize report templates.</td>
</tr>
<tr>
<td></td>
<td>■ View dashboards.</td>
</tr>
<tr>
<td></td>
<td>■ View reports and report templates.</td>
</tr>
<tr>
<td></td>
<td>■ Manage tiered dashboards</td>
</tr>
<tr>
<td></td>
<td>■ Manage jobs.</td>
</tr>
<tr>
<td></td>
<td>■ Assign permissions to folders.</td>
</tr>
<tr>
<td></td>
<td>■ Manage tags.</td>
</tr>
<tr>
<td></td>
<td>■ Request exceptions.</td>
</tr>
<tr>
<td></td>
<td>■ Manage configuration settings.</td>
</tr>
<tr>
<td></td>
<td>■ View assets and asset reconciliation rules.</td>
</tr>
<tr>
<td></td>
<td>■ View standards.</td>
</tr>
<tr>
<td></td>
<td>■ View review cycles.</td>
</tr>
<tr>
<td></td>
<td>■ View baselines.</td>
</tr>
<tr>
<td></td>
<td>■ View evaluation results.</td>
</tr>
<tr>
<td></td>
<td>■ View roles and permissions.</td>
</tr>
<tr>
<td></td>
<td>■ View tiered dashboards</td>
</tr>
<tr>
<td>Report Result Viewer</td>
<td>The Report Result Viewer role lets the user do the following:</td>
</tr>
<tr>
<td></td>
<td>■ View all jobs.</td>
</tr>
<tr>
<td></td>
<td>■ View the reports and report templates.</td>
</tr>
<tr>
<td></td>
<td>■ View tiered dashboards</td>
</tr>
</tbody>
</table>

See “About roles” on page 96.

About custom roles

Control Compliance Suite (CCS) comes with a number of predefined roles that typically suit most organizations. CCS also provides the ability to create custom roles if the predefined roles do not fit the needs of your organization. However, the custom roles can only be created using a combination of tasks that come built-in with CCS.

You can create new roles or base them on existing roles. Some caution is called for when you create custom roles, because of the dependency between tasks.
For example, you create a custom role to manage the roles. If you add only the Manage Roles task to the custom role, the user is not able to view the roles. To view the roles, you must also add the View Roles task.

**Note:** The Manage Roles task must be assigned only to users with the administrative privileges as this task implicitly gives permissions to all folders in the directory.

See “Creating a custom role” on page 110.
See “Copying a role” on page 111.
See “Editing a custom role” on page 111.
See “Deleting a role” on page 112.

**About the Roles view**

The Roles view lets you assign roles to users and create custom roles.

The Roles view contains the following panes:

- **Table pane**: The table pane lists the predefined roles and the custom roles.
- **Details pane**: The details pane lists the tasks that are associated to a role and the users who are assigned to a role.

You can do the following from the Roles view:

- Add user to a role.
  See “Adding users and groups to a role” on page 107.
- Remove user from a role.
  See “Removing a user or a group from a role” on page 107.
- Assign permissions to the directory folders.
  See “Assigning permissions from the Roles view” on page 109.
- View the tasks that are associated to a role.
  See “Viewing tasks associated to a role” on page 108.
- View the users assigned to a role.
  See “Viewing users assigned to a role” on page 108.
- Create a custom role.
  See “Creating a custom role” on page 110.
- Edit a custom role.
  See “Editing a custom role” on page 111.
- Delete a custom role.
  See “Deleting a role” on page 112.
- Copy a custom role.
  See “Copying a role” on page 111.

About the Permission Management view

The **Permission Management** view lets you assign permissions to the directory folders and items. Once you assign a role to a user, the permissions must be assigned to the folders before the user can perform any tasks on the folder.

The **Permission Management** view contains the following panes:

- **Tree pane**
  The tree pane displays a hierarchical, folder-based structure of the folders that are stored in the CCS directory.
- **Table pane**
  The table pane lists any subfolders of the folder that is selected in the tree pane.
- **Details pane**
  The details pane lists the users who have permissions over the selected folder in the table pane.

You can do the following from the Permission Management view:

- Assign permissions.
  See “Assigning permissions from the Permission Management view” on page 113.
- Remove permissions.
  See “Removing permissions” on page 113.
- View users who have permissions on a folder.

Working with roles

Control Compliance Suite (CCS) provides a number of predefined roles that can be assigned to the CCS users.

A role is a collection of predefined tasks. The user may perform each task that is a specific action, such as Create a policy or Run an evaluation. The role determines what a user can see and perform in the Control Compliance Suite console.

See “Adding users and groups to a role” on page 107.
See “Removing a user or a group from a role” on page 107.
See “Viewing users assigned to a role” on page 108.
Adding users and groups to a role

You must add user and groups to roles in Control Compliance Suite. After you add a user to a role you must grant the user permissions to the folders or the objects in the folders. You must grant the permissions for the user to perform the tasks.

Permissions to the predefined folders are automatically granted when the user is added a role.

You can assign permissions from the Roles view or the Permissions view.

To add a user or a group to a role

1. Go to Settings > Roles.
2. In the Roles view, select the check box next to the role to which you want to add the users or groups.
3. Click Add Users and Groups.
4. In the Select Users or Groups dialog box, type the name of the user or group to add and click OK.

The new user is listed in the Users and Groups list for the role.

Removing a user or a group from a role

After a user is removed from a role, the user can no longer perform the tasks that are associated with the role. All the assigned permissions over the directory folders are also removed.
To remove a user or a group from a role

1. Go to Settings > Roles.
2. In the Roles view, select the check box next to the role that you want to remove.
3. Click Remove Users and Groups.
4. In the Remove Trustees dialog box, select the user that you want to remove.
5. Click Remove.
6. Click OK.

See “Adding users and groups to a role” on page 107.
See “Configuring roles and permissions ” on page 95.

Viewing users assigned to a role

User with the Administrator role can assign users and groups to a role. Each role can have any number of users assigned to it.

To view users and groups assigned to a role

1. Go to Settings > Roles.
2. In the Roles view, do one of the following:
   - Select the role. The Users and Groups tab lists all the users who are assigned to the role.
   - Right-click the role and select View Details.
     The View Details - Settings dialog box lists the users who are assigned to the role and the tasks that are associated with the role.

See “Adding users and groups to a role” on page 107.
See “Configuring roles and permissions ” on page 95.
See “Viewing tasks associated to a role” on page 108.

Viewing tasks associated to a role

Each role has a list of tasks that are associated to it. The tasks are predefined and cannot be modified.

To view tasks associated to a role

1. Go to Settings > Roles.
2. In the Roles view, do one of the following:
   - Select the role, the Tasks tab lists tasks that are associated to the role.
Right-click the role and select **View Details**.

The **View Details - Settings** dialog box lists the tasks that are associated with the role and the users who are assigned to the role.

See “Adding users and groups to a role” on page 107.

See “Configuring roles and permissions” on page 95.

See “Viewing users assigned to a role” on page 108.

### Assigning permissions from the Roles view

After you add a user or a group to a role you must grant permissions to folders and its objects. You cannot grant a user the permissions to a folder unless the user has been added to the appropriate role.

See “Adding users and groups to a role” on page 107.

When you assign permissions to a parent folder, the subfolders automatically inherit the parent folder permissions.

When you add a user to a role, the system automatically assigns permissions to any predefined folders.

---

**Note:** There may be time delay for permissions to propagate through the directory.

### To assign permissions

1. Go to **Settings > Roles**.
2. In the **Roles** view, select the role.
3. In the **Users and Groups** tab, select the user or group.
4. Click **Assign Permissions**.
5. In the **Assign Permissions** panel, in the left pane, navigate to the required folder.

   All the subfolders are listed in the right pane.

6. Do one of the following:
   - To add a folder that is listed in the right pane, select the folder and click **Add**.
   - To add all folders that are listed in the right pane, click **Add All**.

   You can use the search feature to quickly find the required folder.

7. The newly added folders are listed in the **Selected Items** list.
8. Click **Next**.
In the Review Assigned Permissions panel, confirm if the folder selection is accurate.

Click Finish.

See “Assigning permissions from the Permission Management view” on page 113.

See “Configuring roles and permissions” on page 95.

Creating a custom role

You can create new roles or copy an existing role and make changes to suit your needs.

See “Copying a role” on page 111.

Note: The Manage Roles task must be assigned only to users with the administrative privileges as this task implicitly gives permissions to all folders in the directory.

To create a custom role

1. Go to Settings > Roles view.
2. In the Roles view, on the taskbar, click Create Role.
3. In the Create or Edit Custom role wizard > Specify Custom Role details panel, type the name of the role.
4. Type a brief description of the new role and then click Next.
5. In the Specify tasks for custom role panel, select the tasks for the new role. To select the tasks do the following:
   - From the roles list, select a role. The tasks for the selected role are listed in the tasks list.
   - From the tasks list, select the tasks. Click Add for each task you select or you can click Add all to select all tasks from the tasks list.
   The Selected Items section lists all the tasks that you added from the tasks list.
6. Repeat step 5 to select tasks from a different role.
7. Click Next.
8. In the Summary panel, review the tasks that you have selected for the custom role and click Back to make changes.
9. Click Finish to close the wizard.

See “Configuring roles and permissions” on page 95.
Copying a role

You can copy a predefined role or a custom role to create a new role. You can make the required changes to the name and description.

To modify the tasks that are associated with a custom role, you must select Edit Role on the taskbar.

To copy a role

1. Go to Settings > Roles.
2. In the Roles view, select the role that you want to copy.
3. On the taskbar, click Copy Role.
4. In the Copy Role View dialog box, type a unique name for the new role.
5. Change the description of the role.
6. Click OK to save.

See “Configuring roles and permissions” on page 95.
See “Creating a custom role” on page 110.

Editing a custom role

You can edit the name, the description, and the tasks that are associated with the role.

When you modify the tasks in a role, the system automatically updates the permissions on the directory folders and objects for the user with the role.

Note: The Manage Roles task must be assigned only to users with the administrative privileges as this task implicitly gives permissions to all folders in the directory.

To edit a custom role

1. Go to Settings > Roles.
2. In the Roles view, select the role that you want to edit.
3. On the taskbar, click Edit Role.
4. In the Create or Edit Custom Role wizard > Specify Custom Role details panel, change the name and description of the role if required.
5. Click Next.
6. In the Specify Tasks for Custom Role panel, add or remove the tasks for the role.
To add tasks, do the following:

- From the roles list, select a role. The tasks for selected role are listed in the tasks list.
- From the tasks list, select the tasks. Click Add for each task that you select or you can click Add all to select all tasks from the tasks list.

Repeat step 6 to select tasks from a different role.

To remove tasks, in the Selected Tasks list, select the task to remove, click Remove or you can click Remove All to remove all tasks.

Click Next.

In the Summary panel, review the tasks that you have selected for the role.

Click Back to make changes or click Finish to close the wizard.

See “Creating a custom role” on page 110.

Deleting a role

You can only delete custom roles.

When you delete a role, the system automatically updates the permissions on the directory folders and objects for the users with the role.

To delete roles

1. Go to Settings > Roles.
2. In the Roles view, select the check boxes next to the roles you want to delete.
3. On the taskbar, click Delete Roles.

See “Creating a custom role” on page 110.

Working with permissions

Control Compliance Suite lets you control which users have what access to which directory objects. When a user account is authenticated, the type of access that is granted to the objects is determined by the permissions that are attached to the object.

When a role is assigned to a user, permissions are automatically granted to the directory objects in the predefined folders. The administrator must manually assign permissions to the user-defined folders.

See “Assigning permissions from the Permission Management view” on page 113.

See “Removing permissions” on page 113.
Assigning permissions from the Permission Management view

After you add a user or group to a role in the Roles view, you must grant permissions to folders to perform tasks. You cannot grant a user the permissions to a folder unless the user has been added to the appropriate role.

See “Adding users and groups to a role” on page 107.

When you add a user to a role, the system automatically assigns permissions to any predefined folders.

When you assign permissions to a parent folder, the subfolders automatically inherit the parent folder permissions.

Note: There may be time delay for permissions to propagate through the directory.

To assign permission

1. Go to Settings > Permission Management.

2. In the Permission Management view, in the tree pane, navigate to the required folder.

3. In the table pane, select the folder to assign the permissions.

4. In the User and Groups tab, click Assign Permissions.

5. In the Assign Permissions dialog box, click Add.

6. In the Select Users/Groups dialog box, select the role name and click OK.

   The newly added user is listed in the Assign Permissions dialog box.

7. To add more users or groups, go to step 5.

8. Click OK.

9. Click the refresh icon on the details pane to list all the newly assigned users.

See “Assigning permissions from the Roles view” on page 109.

See “Configuring roles and permissions ” on page 95.

Removing permissions

You can remove permissions that are assigned to a user over a directory folder.

To remove permission

1. Go to Settings > Permission Management.

2. In the Permission Management view, in the tree pane, navigate to the required folder.
3 In the table pane, select the folder.
4 In the Users and Group tab, select the user or group.
5 Click Remove Permissions.
6 In the Remove Permission View dialog box, select the role name and click Remove.
7 Click Update to confirm the removal of permission.

See “Assigning permissions from the Permission Management view” on page 113.
See “Assigning permissions from the Roles view” on page 109.
See “Configuring roles and permissions” on page 95.

Registering and configuring the Data Processing Service

After you install a Data Processing Service (DPS) instance, you must register it. Until you register it, the Application Server cannot contact the DPS. When you register the DPS, you import a copy of the certificate that is associated with the DPS and store it. You can also configure the DPS to fit your environment when you register the DPS.

Changes to the DPS Settings can help to optimize the performance of the Control Compliance Suite (CCS). Changes to the settings that you make in error can make it impossible to collect data from the data collectors on your network. Changes to the settings can also harm the performance of CCS.

The settings lets you change how the DPS Collector interacts with the following:
- RMS data collector Information Server
- ESM data collector managers
- Data that another tool collects and stores in a file (CSV files)
- Data that another tool collects that is accessible using ODBC.

For each DPS, you can configure the following:
- DPS roles
- Site assignment

You can also change the data collector settings for any DPS assigned to the DPS Collector role.

See “Configuring the data collectors” on page 138.
See “Configuring the Windows data collector” on page 140.
See “Configuring the Oracle data collector” on page 141.
See “Configuring the SQL data collector” on page 142.
See “Configuring the UNIX data collector” on page 142.
See “Configuring the Exchange data collector” on page 143.
See “Configuring the NetWare data collector” on page 144.
See “Configuring the NDS data collector” on page 144.
See “Configuring the ESM data collector” on page 145.
See “Configuring the CSV data collector” on page 156.
See “Configuring the ODBC data collector” on page 158.
See “Configuring the assets batch size” on page 121.
See “About the Control Compliance Suite Data Processing Service” on page 37.

About Data Processing Service roles

The Data Processing Service (DPS) must be assigned one or more roles within the Control Compliance Suite (CCS). The assigned role or roles control what tasks the DPS performs in your CCS deployment. Any DPS can be assigned to multiple roles, but more often a DPS plays a single role.

A DPS can be assigned to one or more of the following roles:

- DPS Load Balancer
  See “About the Data Processing Service Load Balancer” on page 38.

- DPS Collector
  See “About the Data Processing Service Collector” on page 40.

- DPS Evaluator
  See “About the Data Processing Service Evaluator” on page 41.

- DPS Reporter
  See “About the Data Processing Service Reporter” on page 39.

For information on how to choose which DPS computers to assign to which roles, see the Symantec Control Compliance Suite Planning and Deployment Guide.

Registering the Data Processing Service

Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register a DPS, the Directory Server verifies a copy of the certificate that is assigned to
the DPS host. The certificate is then used to secure communications with the DPS. When you register the DPS, you can also configure the DPS settings.

The DPS icon in the Map View and Grid View does not reflect the updated DPS status until you refresh the view.

---

**Note:** Assign the first DPS that you register to the Load Balancer role.

---

**To register the Data Processing Service**

1. In the System Topology > Map View or System Topology > Grid View, click Register DPS.
2. In the Data Processing Service Selection panel, select one or more DPS hosts to register and click Next.
3. In the Site Selection panel, select the site to which the DPS hosts should be assigned. You can use an existing site or create a new site. To create a new site, click Create Site and enter a site name and click Next.
4. In the Role Selection panel, select the roles to which the DPS should be assigned. You must assign the DPS to at least one role.
   
   You can also change the port the DPS uses to communicate with the Application Server. The default port is 3993. Click Next.
5. In the Confirm or change the DPS to Use for Synchronizing the Reporting Database panel, select the DPS that should perform synchronization of the reporting database, then click Next.
6. If you selected the DPS Collector role, in the Data Collector Selection panel, select the data collectors that the DPS should use, then click Next.
7. In the Summary panel, click Next.
8. Do one of the following:
   
   - If you assigned a DPS to the DPS Collector role, in the Finished panel, click Advanced Settings for registered components.
   
   - If you did not assign a DPS to the DPS Collector role and need to register another DPS, in the Finished panel, click Register another DPS.
   
   - If you did not assign a DPS to the DPS Collector role, in the Finished panel, click Close.
9 Click the name of the setting to configure.
   Enter any information that is required on the panel.
   See “Configuring the Windows data collector” on page 140.
   See “Configuring the Oracle data collector” on page 141.
   See “Configuring the SQL data collector” on page 142.
   See “Configuring the UNIX data collector” on page 142.
   See “Configuring the Exchange data collector” on page 143.
   See “Configuring the NetWare data collector” on page 144.
   See “Configuring the NDS data collector” on page 144.
   See “Configuring the ESM data collector” on page 145.
   See “Configuring the CSV data collector” on page 156.
   See “Configuring the ODBC data collector” on page 158.
   See “Configuring basic Data Processing Service settings” on page 119.
   See “Configuring advanced Data Processing Service settings” on page 119.

10 In the Edit Settings dialog box, click Save to close the dialog box and save the changes.

11 In the Finished panel, click Close.

Registering the DPS with minimum custom configuration

Before the application server can use a newly installed Data Processing Service (DPS), you must register the DPS with the application server. When you register a DPS, the Directory Server verifies a copy of the certificate that is assigned to the DPS host. The certificate is then used to secure communications with the DPS. When you register the DPS, you can also configure the DPS settings.

See “About the Control Compliance Suite Data Processing Service” on page 37.

To register the Data Processing Service

1 In the System Topology > Map View click Register DPS.

2 In the Data Processing Service Selection panel, select the DPS host to register and click Next.

3 In the Site Selection panel, select the Default Site option. You can also create a new site. To create a new site, click Create Site and enter a site name and click Next.
4 In the Role Selection panel, click Select ALL Items link and click Next.
   The DPS is assigned to all the roles.
   See “About Data Processing Service roles” on page 115.
5 In the Confirm or change the DPS to Use for Synchronizing the Reporting Database panel, select the DPS that should perform synchronization of the reporting database, then click Next.
6 In the Data Collector Selection panel, select the data collectors that the DPS should use, then click Next.
7 In the Summary panel, click Next.
8 In the Finished panel, click Change advanced settings for registered components to change the settings of the DPS Collectors to collect data.
9 In the Edit Settings dialog box, select the data collector and configure the settings.
10 Click Save to close the dialog box and save the changes.
   See “Quick start with minimum configuration” on page 76.
   See “Registering the Data Processing Service” on page 115.

Unregistering a Data Processing Service

If needed, you can unregister a Data Processing Service (DPS) instance. When you do so, you remove the DPS from the list of Data Processing Services that the Application Server contacts. Before you unregister a DPS, make sure that another DPS is assigned to take over the duties of the unregistered DPS.

To unregister a Data Processing Service

1 In the System Topology > Map View or System Topology > Grid View, click Unregister DPS.
2 In the Data Processing Service Selection panel, select one or more DPS hosts to unregister, then click Next.
3 In the Summary panel, click I understand the above DPS and associated data collector configurations will be removed permanently and I understand this action is irrevocable, and then click Next.
4 In the Finish panel, do one of the following:
   - Click Unregister another DPS.
   - Click Close
Configuring basic Data Processing Service settings

You can configure the Data Processing Service (DPS) settings when you register the DPS. You can also configure the DPS settings at a later time. You use one of the system topology views to select the DPS to configure.

When you configure the DPS settings, the panels that appear vary depending on the components that are deployed on the host system. In addition, the DPS settings determine what information appears. For example, options to enable data sources only appear if the DPS is assigned to the DPS Collector role.

If you modify more than one DPS at a time, only the common setting tabs and fields appear. Select each DPS individually to view all settings that apply to the DPS.

**Note:** If you make a change to the basic Data Processing Service settings, the changes do not appear immediately. You must close and reopen the *Edit Settings* dialog box before the new options appear.

See “Configuring advanced Data Processing Service settings” on page 119. See “Configuring the data collectors” on page 138. See “About the Control Compliance Suite Data Processing Service” on page 37.

To configure the basic Data Processing Service settings

1. Go to the *System Topology > Grid View* or *System Topology > Map View*.
2. In the *System Topology > Grid View* or the *System Topology > Map View*, right-click the Data Processing Service component and click *Edit Settings*.
3. In the *Data Processing Service* area of the *Edit Settings* dialog box, click *Basic*.
4. On the *DPS - Basic* panel, click the roles to assign the DPS to.
5. If the DPS is assigned to the DPS Collector role, select the data collectors to enable on the DPS.
6. Click *Save* to save the changes and close the dialog box.

Configuring advanced Data Processing Service settings

You can change the advanced Data Processing Service (DPS) settings.

You can configure the Data Processing Service settings when you register the DPS. You can also make changes to the settings of an existing DPS from the *System Topology > Map View* or *System Topology > Grid View* views.
If you modify more than one DPS at a time, only the common setting tabs and fields appear. Select each DPS individually to view all settings that apply to the DPS.

See “Registering the Data Processing Service” on page 115.

See “Configuring basic Data Processing Service settings” on page 119.

See “Configuring the data collectors” on page 138.

See “About the Control Compliance Suite Data Processing Service” on page 37.

---

**Warning:** When you change the advanced settings, you can render the Data Processing Service invisible to other components. You can also harm the speed of data collection and job processing on the DPS. Only change these settings when asked to do so by Symantec Technical Support.

The Advanced settings include the following:

- TCP/IP port settings
- Session Manager settings
- Scheduler settings

You can change the following TCP/IP port setting:

- **Port**
  - The TCP/IP Port other components use to communicate with the DPS.

You can change the following settings that the Data Processing Service uses internally to define how the Session Manager behaves:

- **Command Threads**
  - The minimum number and maximum number of processor threads available for the Session Manager. This thread pool is used to collect job results and perform other maintenance tasks. These settings are appropriate for most installations. If a very high performance computer hosts the Data Processing Service, more available threads may improve performance.

- **Job Poll Interval**
  - The time, in seconds, the Data Processing Service waits between attempts to collect job results.

You can change the following settings the Data Processing Service uses internally to define how the Scheduler behaves:
Command Threads
The minimum number and maximum number of processor threads available for the Data Processing Service Scheduler. If a very high performance computer hosts the Data Processing Service, more available threads may improve performance.

Submit Threads
The minimum number and maximum number of processor threads available for the scheduler Job Submission thread pool. This thread handles newly submitted jobs.

Resume Threads
The minimum number and maximum number of processor threads available for the scheduler Job Resumption thread pool. This thread handles any jobs that were submitted, transferred to the scheduler, and later resumed.

To configure the advanced Data Processing Service settings
1. Go to the System Topology > Grid View or System Topology > Map View.
2. In the System Topology > Grid View or the System Topology > Map View, right-click the Data Processing Service component and click Edit Settings.
3. In the Data Processing Service area of the Edit Settings dialog box, click Advanced.
4. On the DPS - Advanced panel, make any required changes to the advanced settings.
5. Click Save to save the changes and close the dialog box.

Configuring the assets batch size
You can control the number of assets that are imported from data collectors in a single batch. Each data collector size is set separately. These settings let you optimize the collection of data from your network.

Symantec recommends that you use the default batch size to ensure better performance.

See “Configuring the data collectors” on page 138.

To configure the assets batch size
1. Go to Settings > System Topology.
2. Do one of the following:
   - In the System Topology > Grid View, right-click the Data Processing Service component and click Edit Settings.
   - In the System Topology > Map View, right-click the Data Processing Service component and click Edit Settings.
In the Edit Settings dialog box, click Assets Batch Size.

On the Assets Batch Size panel, provide the number of assets that are imported in a batch from each data collector.

Click Save.

Assigning a role to a Data Processing Service

Each instance of the Data Processing Service (DPS) is assigned to one or more roles. A role controls what tasks the DPS performs.

You can assign a DPS to one or more of the following roles:

- DPS Load Balancer
- DPS Collector
- DPS Evaluator
- DPS Reporter

DPS Collectors list the enabled data collectors. Only enabled data collectors have configuration tabs available. If you make changes to the selected data collectors, you must close and reopen the dialog for the changes to take effect.

For information on how to choose which DPS computers to assign to which roles, see the Symantec Control Compliance Suite Planning and Deployment Guide.

See “Configuring basic Data Processing Service settings” on page 119.

See “Configuring advanced Data Processing Service settings ” on page 119.

See “About the Control Compliance Suite Data Processing Service” on page 37.

To assign a role to a Data Processing Service

1. Go to the System Topology > Grid View or System Topology > Map View.
2. In the System Topology > Grid View or the System Topology > Map View, right-click the Data Processing Service component and click Edit Settings.
3. In the Data Processing Service area of the Edit Settings dialog box, click Basic.
4. On the DPS - Basic panel, click the roles the DPS should be assigned to.
5. Click Save.

Synchronizing Data Processing Service settings

The Application Server periodically synchronizes settings on all registered Data Processing Service hosts. You can also synchronize settings manually if needed.
To manually synchronize settings

- Do one of the following:
  - In the System Topology > Map View, click Infrastructure Tasks > Sync Configuration.
  - In the System Topology > Grid View, click Sync Configuration.

Working in the System Topology view

The System Topology view contains the Map view and the Grid view. Both views read data from the Control Compliance Suite Directory. The Map view displays a graphical representation of all the deployed infrastructure components. The Grid view displays the same information in a tabular format. Using both the views you can inspect and query the various deployed components.

See “About the Map view” on page 123.

See “About the Grid view” on page 126.

See “About navigating in the Map view” on page 124.

See “About the Map view icons” on page 125.

About the Map view

The Map view reads data from the Control Compliance Suite (CCS) Directory and displays a graphical representation of all deployed components. When you navigate to the view, a map is drawn with a balanced spacing between all the components. You can use the mouse to move the components around the view to draw a different layout.

The Map view displays the association between the application server and all the load balancers. The load balancers show their association with the other data processing servers that are assigned to various sites.

When you exit from the Map view, the configuration layout is automatically saved. The next time you navigate to the Map view, the saved configuration layout is displayed. If a component is deleted or added, the Map view reconciles any differences with the CCS Directory and dynamically displays the updated configuration.

You can do the following from the Map view:

- Register and unregister DPS.
  See “Registering the Data Processing Service” on page 115.
  See “Unregistering a Data Processing Service” on page 118.
Sync configuration.
See “Synchronizing Data Processing Service settings” on page 122.

- Modify or view the settings of each component.
  See “Modifying the settings of a component” on page 127.

- Create sites.
  See “Creating a site” on page 136.

- View health and status information.
  See “Viewing the health and the status details” on page 131.

- Monitor system jobs.
  See “Monitoring infrastructure jobs” on page 133.

- Create and delete annotations.
  See “Adding annotations to the components” on page 128.

- Save an image of the components layout.
  See “Saving an image of the configuration layout” on page 128.

- Zoom in and zoom out of the layout.

- Display a balanced view of the components layout.

- Modify the layout of the components.
  See “About navigating in the Map view” on page 124.

  See “About the Map view icons” on page 125.

  See “About the Grid view” on page 126.

About navigating in the Map view

The Map view provides the following features to adjust the layout and view of the components:

- **Zoom in and zoom out**
  You can use the zoom icons to zoom in or zoom out of the component layout.

- **Fit in Window**
  The **Fit in Window** feature redraws the map with a balanced spacing between all the components and zooms out so that the whole map is visible.
Move

You can manually move a specific component or multiple components in the view area. To move a specific component, you click the component and drag and drop it to the new location. To move multiple components, you click in an empty area on the view. Hold down the left mouse key and drag the mouse until the frame is around the objects to be moved. All the component icons are highlighted inside the frame. You click on any of the highlighted icons and drag the icon to the new location.

Reset

If the layout of all the components is not well balanced, clicking Auto Layout redraws the map.

Refresh

You can refresh the Map view to display any changes to the component configurations since the view was selected.

After a Data Processing Service is registered, the DPS status in the Map view and the Grid view does not reflect the updated status until you refresh the view.

You can also view the status of the current configuration jobs that are running from the *Infrastructure Job Monitor* dialog box.

See “Monitoring infrastructure jobs” on page 133.

See “About the Map view” on page 123.

**About the Map view icons**

The Map view icons help visually to identify the different roles of the Data Processing Service (DPS) and the health status of the components.

The following table displays the DPS role icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="DPS Load Balancer" /></td>
<td>The DPS with a blue icon depicts a DPS Load Balancer. When the DPS acts as a load balancer, the DPS routes data collection jobs from the application server to a DPS Collector. In addition, a load balancer routes the evaluation jobs to the DPS Evaluator and the reporting jobs to the DPS Reporter.</td>
</tr>
<tr>
<td><img src="icon" alt="DPS Collector" /></td>
<td>The DPS with a green icon depicts a DPS Collector. The DPS Collector is the interface to the programs that do the actual work of collecting data from the network.</td>
</tr>
</tbody>
</table>
The DPS with a red icon depicts a DPS Evaluator.

Evaluation jobs are sent from the application server to one of the Data Processing Service (DPS) Load Balancers. The DPS Load Balancer then sends the evaluation job to the DPS Evaluator. The evaluator compares the data to the specifications in the Standards that you select and then stores the evaluation results in the production database.

The DPS with a yellow icon depicts a DPS Reporter.

The Data Processing Service (DPS) Reporter generates reports and dashboards for display by the Control Compliance Suite Console. In addition, a single DPS Reporter is assigned to perform database synchronization between the production database and the reporting database test.

The following table displays the health status icons of the components:

- ![Icon] Indicates a healthy status.
- ![Icon] Indicates that the component needs attention. For example: There can be a version mismatch of the application server and the DPS server.
- ![Icon] Indicates that the component has failed the health status check.
- ![Icon] Indicates that system cannot get a status on the component.

After a Data Processing Service is registered, the DPS status in the Map view and the Grid view does not reflect the updated status until you refresh the view.

You can also view the status of the current configuration jobs that are running from the **Infrastructure Job Monitor** dialog box.

See “Monitoring infrastructure jobs” on page 133.

See “About the Control Compliance Suite Data Processing Service” on page 37.

See “Viewing the health and the status details” on page 131.

**About the Grid view**

The **Grid** view reads data from the Control Compliance Suite Directory and displays a tabular representation of all deployed components. The information that is
displayed in the **Map** view and the grid view is the same except for the format that displays the information.

You can do the following from the **Grid** view:

- **Register and unregister DPS.**
  - See “Registering the Data Processing Service” on page 115.
  - See “Unregistering a Data Processing Service” on page 118.

- **Sync configuration.**
  - See “Synchronizing Data Processing Service settings” on page 122.

- **Modify or view the settings of each component.**
  - See “Modifying the settings of a component” on page 127.

- **Create site.**
  - See “Creating a site” on page 136.

- **Monitor system jobs**
  - See “Monitoring infrastructure jobs” on page 133.

- **Select the columns to be displayed in the grid.**

- **Sort the grid.**

  See “About the Map view” on page 123.

### Modifying the settings of a component

You can modify the component settings from the Map view or from the Grid view.

**To modify the settings of a component from the Map view**

1. Go to **Settings > System Topology**.
2. In the **Map** view, right-click the component to modify the settings.
3. Click **Edit Settings**.
4. In the **Edit Settings** dialog box, modify the required properties.
5. Click **Save**.

**To modify the settings of a component from the Grid view**

1. Go to **Settings > System Topology**.
2. In the **Grid** view, right-click the component in the grid.
3. Click **Edit Settings**.
4. In the **Edit Settings** dialog box, modify the required properties.
5. Click **Save**.
See “About the Map view” on page 123.
See “About the Grid view” on page 126.

Viewing additional component information
You can view additional information about a component from the Map view. The additional information window displays the details of the component and the health and status of the component.

To view additional information of a component
1  Go to Settings > System Topology > Map view.
2  In the Map view, do one of the following:
   •  Right-click the component.
   •  Pause the mouse over the component. You can view information of the selected component in the balloon window that appears.

See “Modifying the settings of a component” on page 127.

Saving an image of the configuration layout
You can save the image of the Map view layout and print it for later use.

To save an image of the configuration layout
1  Go to Settings > System Topology.
2  In the Map view, click Save Image.
3  In the Save as dialog box, navigate to the location to save the image file.
4  Modify the name of the file, and click Save.

See “About the Map view” on page 123.

Adding annotations to the components
You can add an annotation to the link that connects two components in the Map view. You can add comments, notes, or any text that is relevant to the linked components.

To add an annotation
1  Go to Settings > System Topology.
2  In the Map view, right-click the blue link between the two components and select Annotate.
3 In the text box, type the notes.
4 Click outside the text box to save.
   If required, you can move the text box to a location in the view.
See “Deleting annotations” on page 129.
See “Associating components” on page 129.
See “Deleting the association between components” on page 130.

Deleting annotations
You can delete the annotations that are added to the components.

To delete an annotation
1 Go to Settings > System Topology.
2 In the Map view, right-click the annotation text and select Delete Label.
See “Adding annotations to the components” on page 128.
See “Associating components” on page 129.
See “Deleting the association between components” on page 130.

Associating components
You can create associations between the infrastructure components. By default, the association between components are drawn in the Map view. The links between components help to add annotations.

The Map view lets you draw association that you may have deleted.

To add a link between components
1 Go to Settings > System Topology.
2 In the Map view, roll the mouse over the arrow icon that is displayed on the component image that you want to associate.
   When the cursor changes from an arrow to a hand, drag the mouse to the other component that you want to associate with. A blue link is created, associating the two components.
   You can now add annotation to the link.
See “Deleting the association between components” on page 130.
See “Deleting annotations” on page 129.
Deleting the association between components

You can delete the link between two components in the Map view.

To delete the link between components

1. Go to Settings > System Topology.
2. In the Map view, right-click the link between the two components select **Delete Link**.

See “Associating components” on page 129.

See “Deleting annotations” on page 129.

See “Adding annotations to the components” on page 128.

About the health and status of a component

You can view the configuration information of all the Control Compliance Suite (CCS) services that are installed. The health and the status jobs are run only on Data Processing Service (DPS) and the application server components.

The following health and status information is available:

- Communication settings
- Application server settings
- CCS directory Settings
- Data Processing Service settings
- Infrastructure logs

The health information that is displayed is not live and is based on the scheduled jobs and the manual job runs. The health and the status jobs are run at the following time intervals:

Full status  The information is posted every 24 hours at midnight.
You can manually refresh the information at anytime from the **Settings > Map** view and the **Settings > Grid** view.
See “Refreshing the health and the status information” on page 133.
The information is purged after 90 days.

Quick status  The information is posted every hour and is purged after seven days.
The quick status is not displayed for the report server and the application configuration files.

You can export the data format.
You can view the health status of multiple Data Processing Service at the same time.

In the **Health and Status Details** dialog box, the component name is color coded to indicate the health status of the component. You can also export the data.

- **Green** Indicates a healthy status.
- **Yellow** Indicates that the component needs attention.
- **Red** Indicates that the component has failed the health status check.
- **Pink** Indicates that system cannot get a status on the component.

See “Viewing the health and the status details” on page 131.
See “Refreshing the health and the status information” on page 133.
See “About the Map view” on page 123.
See “About the Grid view” on page 126.

**Viewing the health and the status details**

The health information and status information lets users view the configuration details of the infrastructure components. The information can be used to detect and diagnose any issues. You can also the export the data to an XML format.

See “About the health and status of a component” on page 130.

If an error appears, manually run the **Refresh Health Status** task from the **Settings > Map view** or the **Settings > Grid view**.

See “Refreshing the health and the status information” on page 133.
To view health and status of a component

1. Go to Settings > System Topology.
2. In the Map view or the Grid view, right-click a component and then select Health and Status Details.
3. In the Health and Status Details dialog box, you can view the following information:

- **LiveUpdate**: Displays the updates that are downloaded and are ready to be installed.
- **Host Machine Details**: Displays the details of the host machine on which the selected Control Compliance Suite component is installed.
- **Service Details**: Displays the details about the selected component.
- **Production Database Details**: Displays the details of the SQL Server host and the list of the databases that are installed on the SQL Server host.
- **Evidence Management Details**: Displays the schema version of the evidence management database.
- **Report Server Details**: Displays the details of the SQL Server host, the reporting database, and the schema versions of the various modules.
- **Logging Details**: Displays the logging settings and statistics.
  
  If the default log location is modified, then the log file information is not displayed here. Only the log files that are stored in the default location appear here.
- **App. Config Details**: Displays the details of the application configuration files.
- **Integration Bridge Details**: Displays all the integration bridge interfaces and the available endpoints.
- **Data Collector Configuration Details**: Displays the data collectors that are configured on the Data Processing Service.

See “About the health and status of a component” on page 130.

See “About the Map view” on page 123.

See “About the Grid view” on page 126.
Refreshing the health and the status information

The scheduled health and status information is posted every 24 hrs at midnight. You can manually refresh the Map view at anytime to see the latest health information of a component.

To refresh the health and status information

- Do one of the following:
  - In the Settings > System Topology > Map view, on the taskbar, click Infrastructure Tasks > Refresh Health Status.
  - In the Settings > System Topology > Grid view, on the taskbar, click Refresh Health Status.

See “About the health and status of a component” on page 130.

See “Refreshing the health and the status information” on page 133.

See “About the Map view” on page 123.

See “About the Grid view” on page 126.

Monitoring infrastructure jobs

You can monitor the status of any system configuration jobs that are currently running.

To monitor the infrastructure jobs

1. Do one of the following:
   - In the Settings > System Topology > Map view, on the taskbar, click Infrastructure Tasks > Monitor System Jobs.
   - In the Settings > System Topology > Grid view, on the taskbar, click Monitor System Jobs.

   The InfrastructureJobMonitor dialog box displays any jobs that are running.

2. You can choose to refresh the Map view when the job completes. You can also modify the time interval to refresh the Map view when the job completes.

See “About the Map view” on page 123.

See “About the Grid view” on page 126.
Configuring sites

A site is a logical grouping of assets and servers. Sites are organizational tools. Sites help you configure how data is collected and which DPS Collector performs the collection.

Each asset is assigned to a single site.

All instances of the Data Processing Service (DPS) are assigned to one or more sites. Every site must have at least one DPS Collector assigned.

Data is collected from the assets that are assigned to a site by the DPS Collectors that are also assigned to the site. Any DPS Collector can be assigned to more than one site.

Multiple, identically configured DPS Collectors can be assigned to a single site. When multiple DPS Collectors are assigned to a site, the DPS Load Balancers assign jobs in a round robin fashion. An asset is assigned to a single site.

A site can represent a physical location that is separated from the remainder of your Control Compliance Suite deployment by slow network links. A site can also represent a logical subdivision of a single location such as a single department, a single building, or a single floor.

See “What sites can do for you” on page 134.

See “About using sites” on page 135.

See “About planning sites” on page 136.

See “Creating a site” on page 136.

See “Deleting a site” on page 137.

See “Assigning a Data Processing Service to a site” on page 137.

See “Removing a Data Processing Service from a site” on page 138.

What sites can do for you

Sites let you group assets together with the Data Processing Services that handle the assets. Sites let you adapt Control Compliance Suite (CCS) data collection to your needs. You can use sites to represent physical groups of your assets.

Sites can represent a physical grouping of assets. When the deployment spans multiple locations and the locations have slow network links, sites help to optimize data collection. In this model, the site groups all assets at a single physical location with the DPS Collectors that retrieve data from the assets. The DPS Collectors collect data from the assets over local, high-speed network connections. Only communications with other CCS components cross the slow link to the remainder of the network. Further, communications between the collector and other
components are designed to accommodate these slow links. Data is compressed before transmission and broken into chunks to facilitate the transmission.

As a variation, you can group the assets that share a single type of network access into a group. A site that groups assets by network speed can help to optimize data collection performance. For example, any assets that are accessible over a low-speed virtual private network (VPN) access can be grouped in a single site. This model isolates assets with slower data collection. In this model, the DPS Collector that collects data from the remote access site is hosted in the same location as the VPN router.

You can also subdivide assets at a single location into multiple sites that are based on their physical location. At a campus with multiple buildings, you can group all assets from a single building into a site. You can also group all assets from a portion of a building into a single site.

Sites can also represent a logical grouping of assets. For example, you can assign all assets in a single department or a small group of departments to a site.

Finally, sites can be used to group DPS Load Balancers, Evaluators, and Reporters. A site without a DPS Collector cannot include any assets. This type of phantom site can be useful when you plan and document the CCS deployment.

See “About using sites” on page 135.

See “About planning sites” on page 136.

About using sites

All assets and all Data Processing Service (DPS) instances are assigned to a site. Assets are always assigned to a single site. A DPS must be assigned to a site and can be assigned to more than one site. If a site has assets assigned, the site must have at least one DPS Collector assigned to collect data from the assets. You use the Control Compliance Suite (CCS) console to create, assign, and manage sites. Only users with appropriate privileges can make changes to sites.

All CCS deployments must include at least a single site. A default site is created when you install CCS. You can create as many additional sites as you need. You can also rename or delete any site except the default site.

**Note:** If a DPS is removed from a site, it cannot collect data from the assets you assigned to that site.

See “What sites can do for you” on page 134.

See “About planning sites” on page 136.
About planning sites

Sites benefit from careful plans. Before you begin your Control Compliance Suite (CCS) deployment, you should evaluate your network and consider the best way to divide it into sites.

You begin with a diagram of your network. Your diagram should include a note of the speed of the links that connect parts of your network. This analysis suggests how your assets should be divided into sites.

Site planning is integrated into the deployment planning process. You must consider your site plans in light of your comprehensive deployment plans.

See “What sites can do for you” on page 134.
See “About using sites” on page 135.

Creating a site

You create a site to organize a group of assets.

By default, all the Data Processing Services are assigned to the Default site.

See “About the Control Compliance Suite Data Processing Service” on page 37.

To create a site from the Map view

1. Go to Settings > System Topology.
2. In the Map view, right-click on an empty area of the map.
3. Click Create Site.
4. In the Create Site dialog box, type the name of the site.
5. Click OK.

To create a site from the Grid view

1. Go to Settings > System Topology.
2. In the Grid view, on the taskbar, click Create Site.
3. In the Create Site dialog box, type the name of the site.
4. Click OK.

See “What sites can do for you” on page 134.
See “About using sites” on page 135.
See “Deleting a site” on page 137.
See “Modifying the site name” on page 138.
Deleting a site

You must first remove any Data Processing Service that is assigned to the site before you delete the site.

See “Removing a Data Processing Service from a site” on page 138.

You must also reassign the assets that are assigned to the site. You can manually assign the assets one at a time or you can use the reconciliation rule.

Do the following to reassign the assets:

- Create an Update reconciliation rule.
  See “Creating reconciliation rules” on page 306.

- Reimport the assets.
  See “Importing assets” on page 313.

To delete a site from the Map view

1. Go to Settings > System Topology.
2. In the Map view, right-click on the site name.
3. Click Delete site.

See “Creating a site” on page 136.
See “Modifying the site name” on page 138.
See “About using sites” on page 135.

Assigning a Data Processing Service to a site

You assign a Data Processing Service (DPS) that is responsible for load balancing, data collection, evaluation, and reporting from the assets in the site. A DPS can be assigned to multiple sites. By default all DPS are assigned to the Default Site.

If a DPS is removed from a site, the DPS cannot collect data from the assets that are assigned to that site.

To assign a DPS to a site from the Map view

1. Go to Settings > System Topology.
2. In the Map view, right-click the DPS to assign.
3. Click Assign to site, and then select the name of the site.

See “About the Control Compliance Suite Data Processing Service” on page 37.
See “Creating a site” on page 136.
See “About using sites” on page 135.
Removing a Data Processing Service from a site

Whenever a Data Processing Service (DPS) is removed from a site the DPS is automatically added to its last default site.

If a DPS is removed from a site, the DPS cannot collect data from the assets that are assigned to that site.

To remove a DPS from a site in the Map view

1. Go to Settings > System Topology.
2. In the Map view, right-click the DPS in the site from which you want it removed.
3. Click Remove from site, and then select the name of the site.

See “Assigning a Data Processing Service to a site” on page 137.
See “About the Control Compliance Suite Data Processing Service” on page 37.
See “About using sites” on page 135.

Modifying the site name

You can modify the site name at anytime.

The site name can contain a maximum of 256 characters.

To modify the name of a site

1. Go to Settings > System Topology.
2. In the Map view, click on the site name to modify the name.
3. In the text box, modify the name of the site.
4. Click anywhere outside the text box to save.

See “Creating a site” on page 136.
See “Deleting a site” on page 137.
See “About using sites” on page 135.

Configuring the data collectors

In Control Compliance Suite, the Data Processing Service (DPS) component is configured as a data collector. The DPS in the role of a data collector collects data from the data collection components such as RMS, ESM, and CSV files.

The RMS data collection component comprises the RMS Console and Information Server into which snap-in modules of predefined platforms are registered. The
snap-in modules are equipped to collect data from the computers that are installed with any of the predefined platforms. RMS Console and Information Server supports data collection from the computers that are installed with the predefined platforms such as Windows, UNIX, SQL, and Oracle. In Control Compliance Suite, for every predefined platform a predefined data collector is defined. The data collector routes the Control Compliance Suite data collection query through the Information Server and collects the data that is queried and gathered by the snap-in module. The collected data is routed through the data collector to the Control Compliance Suite infrastructure.

The ESM data collection component comprises the ESM Manager and the agent. The ESM Manager does the following:

- Controls and stores policy data and passes the data to the agents or to the console.
- Gathers and stores security data from the agents and passes the data to the console.

The manager uses the control information files (CIF) server to communicate with the agents and the ESM Console. The control information files (CIF) server is the primary component of the manager and is an important part of the ESM information exchange process. Control Compliance Suite defines an ESM data collector that routes the query through the ESM Manager to collect data from the agents. The collected data is routed through the ESM data collector to the Control Compliance Suite infrastructure.

A CSV file or an ODBC compliant database are defined as data collection components that facilitate import of any custom application data. In Control Compliance Suite, a CSV data collector is defined and configured to collect data of the application from the CSV files. An ODBC data collector is defined and configured to collect data from the ODBC compliant databases.

### Table 3-22 Predefined platforms and the corresponding data collectors

<table>
<thead>
<tr>
<th>Platform</th>
<th>Data collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM</td>
<td>ESM data collector</td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle data collector</td>
</tr>
<tr>
<td>SQL</td>
<td>SQL data collector</td>
</tr>
<tr>
<td>UNIX</td>
<td>UNIX data collector</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows data collector</td>
</tr>
<tr>
<td>Exchange</td>
<td>Exchange data collector</td>
</tr>
<tr>
<td>Platform</td>
<td>Data collector</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>NDS</td>
<td>NDS data collector</td>
</tr>
<tr>
<td>NetWare</td>
<td>NetWare data collector</td>
</tr>
<tr>
<td>CSV</td>
<td>CSV data collector</td>
</tr>
<tr>
<td>ODBC</td>
<td>ODBC data collector</td>
</tr>
</tbody>
</table>

See “Configuring the ESM data collector” on page 145.
See “Configuring the Oracle data collector” on page 141.
See “Configuring the SQL data collector” on page 142.
See “Configuring the UNIX data collector” on page 142.
See “Configuring the Windows data collector” on page 140.
See “Configuring the Exchange data collector” on page 143.
See “Configuring the NDS data collector” on page 144.
See “Configuring the NetWare data collector” on page 144.
See “Configuring the CSV data collector” on page 156.
See “Configuring the ODBC data collector” on page 158.

### Configuring the Windows data collector

The Control Compliance Suite can use Symantec Information Server to retrieve data from your enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for Windows snap-in module to collect data from the Windows computers.

The Control Compliance Suite uses the Windows data collector to collect data from RMS. Before you use the Windows data collector on the DPS computer, you must configure this data collector. The Windows data collector must be associated with an Information Server.

You can configure the Windows Data Collector components either from the Grid View or from the Map View.

See “Configuring the data collectors” on page 138.
To configure the Windows data collector

1. Go to Settings > System Topology.

2. Do one of the following:
   - In the System Topology > Grid View, right-click **Data Collection Service** and click **Edit Settings**.
   - In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.

3. In the **Edit Settings** dialog box, under Data Collector, click **Windows - Information Server**.

4. In the Windows - Information Server panel, enter the required information.

5. Click **Save**.

Configuring the Oracle data collector

The Control Compliance Suite uses the Information Server to retrieve data from the enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for Oracle snap-in module to collect data from the Oracle databases.

The Control Compliance Suite uses the Oracle data collector to collect data from the Information Server. Before you use the Oracle data collector on the DPS computer, you must configure this data collector. The Oracle data collector must be associated with an Information Server.

You can configure the Oracle Data Collector components either from the Grid View or from the Map View.

See “Configuring the data collectors” on page 138.

To configure the Oracle data collector

1. Go to Settings > System Topology.

2. Do one of the following:
   - In the System Topology > Grid View, right-click **Data Collection Service** and click **Edit Settings**.
   - In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.

3. In the **Edit Settings** dialog box, click **Oracle - Information Server**.
On the Oracle - Information Server panel, enter the required information.

Click Save.

Configuring the SQL data collector

The Control Compliance Suite uses the Information Server to retrieve data from your enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for Microsoft SQL Server snap-in module to collect data from the SQL Server databases.

The uses the SQL data collector to collect data from the Information Server. Before you use the SQL data collector on the DPS computer, you must configure this data collector. The SQL data collector must be associated with an Information Server.

You can configure the SQL Data Collector components either from the Grid View or from the Map View.

See “Configuring the data collectors” on page 138.

To configure the SQL data collector

1 Go to Settings > System Topology.
2 Do one of the following:
   ■ In the System Topology > Grid View, right-click Data Collection Service and click Edit Settings.
   ■ In the System Topology > Map View, right-click a registered DPS component and click Edit Settings.
3 In the Edit Settings dialog box, click SQL - Information Server.
4 On the SQL - Information Server panel, enter the required information.
5 Click Save.

Configuring the UNIX data collector

The Control Compliance Suite can use the Information Server to retrieve data from the enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for UNIX snap-in module to collect data from the UNIX target computers.
The Control Compliance Suite uses the UNIX data collector to collect data from the Information Server. Before you use the UNIX data collector on the DPS computer, you must configure this data collector for an Information Server.

See “Configuring the data collectors” on page 138.

**To configure the UNIX data collector**

1. Go to Settings > System Topology.
2. Do one of the following:
   - In the System Topology > Grid View, right-click **Data Collection Service** and click **Edit Settings**.
   - In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, click **UNIX - Information Server**.
4. On the UNIX - Information Server panel, enter the required information.
5. Click **Save**.

**Configuring the Exchange data collector**

The Control Compliance Suite can use Symantec RMS to retrieve data from your enterprise network. RMS passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. RMS uses the bv-Control for Microsoft Exchange snap-in module to collect data from the Exchange server.

The Control Compliance Suite uses the Exchange data collector to collect data from RMS. Before you use the Exchange data collector on the DPS computer, you must configure this data collector. The Exchange data collector must be associated with an Information Server.

You can configure the Exchange Data Collector components either from the Grid View or from the Map View.

See “Configuring the data collectors” on page 138.

**To configure the Exchange data collector**

1. Go to Settings > System Topology.
2. Do one of the following:
   - In the System Topology > Grid View, right-click **Data Collection Service** and click **Edit Settings**.
In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.

3 In the **Edit settings** dialog box, click **Exchange - Information Server**.

4 On the Exchange - Information Server panel, enter the required information.

5 Click **Save**.

### Configuring the NDS data collector

The Control Compliance Suite can use Symantec RMS to retrieve data from your enterprise network. RMS passes the collected data to the Data Processing Service (DPS) collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. RMS uses the bv-Control for NDS eDirectory snap-in module to collect data from the server.

You can configure a DPS as an NDS data collector to collect data from the NDS eDirectory snap-in module.

See “Configuring the data collectors” on page 138.

To **configure the NDS data collector**

1 Go to Settings > System Topology.

2 Do one of the following:
   - In the **System Topology > Grid View**, right-click **Data Collection Service** and click **Edit Settings**.
   - In the **System Topology > Map View**, right-click a registered DPS component and click **Edit Settings**.

3 In the **Edit Settings** dialog box, click **NDS - Information Server**.

4 On the NDS - Information Server panel, enter the required information.

5 Click **Save**.

### Configuring the NetWare data collector

The Control Compliance Suite can use Symantec RMS to retrieve data from your enterprise network. RMS passes the collected data to the Data Processing Service (DPS) collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. RMS uses the bv-Control for NetWare snap-in module to collect data from the server.

You can configure a DPS as a NetWare data collector to collect data from the NetWare snap-in module.
See “Configuring the data collectors” on page 138.

To configure the NetWare data collector

1. Go to Settings > System Topology.
2. Do one of the following:
   - In the System Topology > Grid View, right-click Data Collection Service and click Edit Settings.
   - In the System Topology > Map View, right-click a registered DPS component and click Edit Settings.
3. In the Edit Settings dialog box, click NetWare - Information Server.
4. On the NetWare - Information Server panel, enter the required information.
5. Click Save.

Configuring the ESM data collector

You must configure the ESM data collector before you use the ESM data collector on a computer where Data Processing Service (DPS) is installed. The ESM data collector must be associated with one or more ESM managers.

Before you configure the ESM data collector, you must provide the details about the ESM components that the data collector is configured to communicate with. At any point of time after you configure the ESM data collector, you can re-configure the settings to make changes to the data collector.

See “Configuring the data collectors” on page 138.

To configure the ESM data collector

1. Go to Settings > System Topology.
2. Do one of the following:
   - In the System Topology > Grid View, right-click Data Collection Service and click Edit Settings.
   - In the System Topology > Map View, right-click a registered DPS component and click Edit Settings.
3. In the Edit Settings dialog box, click Data Collector Sites > ESM.
4. On the ESM panel, configure the ESM Manager by providing the required information.
5 In the **Edit Settings** dialog box, navigate to **Data Collector > ESM**.

Provide the required information to configure the thread settings and poll settings of the ESM data collector.

6 Click **Save**.

See “**Modifying the settings of a component**” on page 127.

See “**Configuring basic Data Processing Service settings**” on page 119.

See “**Configuring the ESM manager settings**” on page 147.

See “**Configuring the ESM general settings**” on page 152.

**About Symantec Enterprise Security Manager**

Corporations handle large amounts of information in complex computer environments with multiple platforms and integrated networks. The client or the server system solves the challenge of accessing this information quickly and easily. However, client or the server computers can leave sensitive data vulnerable to unauthorized access or modification.

Organizations need to secure their data against unauthorized use while still providing easy access to authorized users on multiple platforms. They need a way to apply security policies, then monitor and enforce compliance throughout the enterprise network. Symantec provides the solution to security policy management with the Symantec Enterprise Security Manager (ESM).

Symantec ESM manages sensitive data and enforces security policies across the following client or server platforms:

- Windows
- UNIX

Symantec ESM administers and enforces the policies and procedures that your organization establishes to control access to secured areas. Symantec ESM identifies the potential security risks and recommends actions to resolve the potential breaches in security. When the potential breaches are resolved, Symantec ESM delivers frequent updates to ensure protection against new threats. Symantec ESM has a broad reporting capability to keep you informed of the security status of the network.

Symantec ESM achieves the goals of confidentiality, integrity, and availability of secured information for your organization.

The primary functions of Symantec ESM are as follows:

- Manage security policies.
Detect changes to security settings or files.

Evaluate and report computer conformance with security policies.

To effectively evaluate the security of your enterprise, you can customize the Symantec ESM environment to match the needs of your organization. You can then continue to adapt Symantec ESM to the changing conditions in the network.

## Configuring the ESM components

You must configure the ESM data collector before you use the ESM data collector on the Data Processing Service computer. The ESM data collector must be associated with one or more ESM managers.

The ESM manager settings are specific to a site. The configurations that you do for the ESM manager is specific to the site where you have configured the ESM data collector. You can view or update the ESM data collector configuration for a site by selecting the site from the Site drop-down list. The drop-down list displays the list of sites that have at least one DPS that is configured as the ESM data collector.

### To configure the ESM components

1. In the CCS console, go to Settings > System Topology.
2. Do one of the following:
   - In the System Topology > Grid View, right-click Data Collection Service and then click Edit Settings.
   - In the System Topology > Map View, right-click the site where DPS is installed and then click Edit Settings.
3. In the Edit Settings dialog box, do one of the following:
   - Click Data Collector > ESM
   - Click Data Collector Sites > ESM

See “Configuring the ESM manager settings” on page 147.

See “Configuring the ESM general settings” on page 152.

See “Configuring an ESM manager for custom messages” on page 148.

See “Collecting suppressed ESM messages” on page 149.

## Configuring the ESM manager settings

The ESM managers that are configured for the data collector of a site are displayed in the List of configured ESM Managers list box.
To configure the ESM manager settings

- On the right pane, provide the required information to configure an ESM manager.

Adding, modifying, or removing an ESM manager

You must configure a data collector as the ESM Manager before you start ESM data collection from the ESM infrastructure. In the ESM infrastructure, the ESM manager collects data from the individual computers on which the ESM agents are installed. You can configure a data collector by adding an ESM manager through the **ESM Manager Credentials** dialog box. The ESM manager can also be modified or removed for the configured data collector.

**To add or modify an ESM manager**

1. On the **Data Collector > ESM** panel of the **Edit Settings** dialog box, click **Add** or **Modify**.
2. In the ESM Manager Credentials dialog box, in the Manager details section, provide the required information.

**To remove an ESM manager**

1. On the panel, select an ESM manager from the **List of configured ESM managers** pane.
2. Click **Remove**.

See “Configuring the ESM manager settings” on page 147.

Configuring an ESM manager for custom messages

You can configure the ESM data collector to use the custom messages during data collection, if you have customized ESM messages. You can select only one ESM manager per site as a source for custom messages.

The message schema includes the following:

- Message description
- Message title
- Message format

You can customize the message schema on the selected ESM manager. The ESM data collector uses the message schema during data collection for the specified site.
To specify an ESM manager for custom messages

1. Navigate to **Settings > Map View** or **Settings > Grid View** of the console and right-click on a DPS and click **Edit Settings**.

2. In the **Edit Settings** dialog box, select **Data Collector Sites - ESM**.

3. On the right pane of the dialog box, for the **Manager for custom messages** section, click the **Manager Name** drop-down list. You can select the ESM manager that maintains the custom messages, which you have configured. The schema of the custom messages, such as description, title, format and so on are also collected from the selected ESM manager.

4. Keep **Report error if custom messages manager not available** checked. If you check **Report error if custom messages manager not available**, then the data collection job fails with an error if the specified custom messages manager is unavailable. If you uncheck **Report error if custom messages manager not available**, then the ESM data collector collects data even if the specified custom messages manager is unavailable. If the custom messages manager is not available, a message prompt appears in the job failures tab, which states about the unavailability of the manager.

See “Configuring the ESM manager settings” on page 147.

Collecting suppressed ESM messages

You can configure the ESM data collector to do the following:

- Collect suppressed ESM messages
- Filter suppressed messages

The data collector configuration to collect suppressed messages applies to the ESM managers that are configured for the selected site.

---

**Note:** When you uncheck **Do not collect suppressed messages**, the checks which were successful in the previous data collection might fail in the subsequent data collection.
To collect suppressed messages

1. Navigate to Settings > Map View or Settings > Grid View of the console and right-click on a DPS and click Edit Settings.

2. In the Edit Settings dialog box, select Data Collector Sites - ESM.

3. On the right pane of the dialog box, for the Collection of suppressed messages section, uncheck Do not collect suppressed messages.

See “Configuring the ESM manager settings” on page 147.

About CCS ESM policy run configurations

Every check in a CCS ESM standard is mapped to an ESM policy. A CCS ESM Standard is mapped to one or more ESM policies. Policy run options let you specify the data that the ESM data collector must collect for a given policy.

The default setting for all policies is "Do not run policy, collect data from last successful policy run." However, you can add exceptions to the default setting by adding an entry in the policy run settings for each policy that you want to customize. The ESM data collector executes a policy run on the basis of the policy run configuration.

You can configure the number of messages that you want ESM data collector to fetch for each policy run. The Symantec.CSM.ESM.Integration.dll.config file contains the MaximumPolicyRunMessageCount parameter, where you can specify the value for the message count. The Symantec.CSM.ESM.Integration.dll.config file that is located in the following location:

<Install_Directory>\CCS\Reporting and Analytics\DPS\Data Collectors\ESM

The default value is 3000.

The ESM data collector collects policy run data on the basis of the policy run configuration. The ESM data collector does not verify the agents and the modules in the policy run when it fetches the latest policy run data. The data collections job completes successfully even if the selected policy run does not contain the modules or the agents that you have specified. However, the result for the data collection job displays the corresponding errors if the policy run data is not present on the ESM manager.

The available modes for data collection are:

- Collect data from the last policy run on the ESM manager.
- Run the ESM policy on the ESM manager and collect the policy run data.
- Run policy on the ESM manager only if the last policy run is older than the <number of> days.
For example, consider that the 'Security essentials W2K3MS v2.0' policy includes the 'Account Integrity' and 'Password Strength' modules. Consider the two agents, 'W2k3Server1-USA' and 'W2k3Server2-USA.' You have run all the modules of 'Security essentials W2K3MS v2.0' on both the agents on 28th September, 2008, at 11:00 a.m. Later, you fix certain violations and then run only the Password Strength module of 'Security essentials W2K3MS v2.0' policy on W2k3Server2-USA on the 29th September, 2008, at 01:00 p.m. You schedule a data collection job on the 30th September, 2008, at 11:00 a.m. to collect data for ESM agents W2k3Server1-USA and W2k3Server2-USA for the same policy and the modules. In CCS 9.0, you configure the ESM policy 'Security essentials W2K3MS v2.0' as 'Run policy if data is older than 1 days.'

During data collection, ESM data collector retrieves the timestamp of the last policy run of the selected agents for all the selected modules.

In the given scenario, the policy run timestamps for the 'Security essentials W2K3MS v2.0' policy on W2k3Server1-USA and W2k3Server2-USA agents are as follows:

<table>
<thead>
<tr>
<th>ESM agent</th>
<th>ESM policy</th>
<th>ESM module</th>
<th>Timestamp of the last policy run</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2k3Server1-USA</td>
<td>Security essentials W2K3MS v2.0</td>
<td>Account Integrity</td>
<td>28th September, 2008, 11:00 a.m.</td>
</tr>
<tr>
<td>W2k3Server1-USA</td>
<td>Security essentials W2K3MS v2.0</td>
<td>Password Strength</td>
<td>28th September, 2008, 11:00 a.m.</td>
</tr>
<tr>
<td>W2k3Server2-USA</td>
<td>Security essentials W2K3MS v2.0</td>
<td>Account Integrity</td>
<td>28th September, 2008, 11:00 a.m.</td>
</tr>
<tr>
<td>W2k3Server2-USA</td>
<td>Security essentials W2K3MS v2.0</td>
<td>Password Strength</td>
<td>29th September, 2008, 01:00 p.m.</td>
</tr>
</tbody>
</table>

The most recent timestamp of the values that the ESM data collector retrieves in this case is 29th September, 2008, 01:00 p.m. Assume that the data collection job is initiated as per its schedule. The ESM data collector compares the 29th September, 2008, 01:00 p.m. timestamp with the current timestamp on the DPS computer, which is 30th September, 2008, 11:00am. Since the data is not older than 1 day, the ESM data collector imports the messages from the last policy run from all the ESM agents.

See “Configuring CCS ESM policy run options” on page 152.
Configuring CCS ESM policy run options

The ESM data collector collects policy run data on the basis of the policy run configuration. You can configure the number of messages that you want ESM data collector to fetch for each policy run.

To configure policy run options

1. Navigate to Settings > Map View or Settings > Grid View of the console and right-click on a DPS and click Edit Settings.
2. In the Edit Settings dialog box, select Data Collector Sites - ESM.
3. On the right pane of the dialog box, click Configure policy run options.
4. In the ESM Policy Configuration dialog box, click Add to add a policy configuration.
5. In the Configure policy dialog box, type the ESM policy name in the Policy name text box and provide the required information.
   You can use the Configure Policy dialog box to add, modify, or remove an ESM policy.
6. In the ESM Policy Configuration dialog box, select the policy that you want to modify and then click Modify.
7. In the ESM Policy Configuration dialog box, select the policy that you want to delete and then click Remove.
   You cannot delete a predefined policy.
8. Click Yes on the message prompt that appears to confirm the deletion of the ESM policy.

See “Configuring the ESM manager settings” on page 147.

Configuring the ESM general settings

The Edit Settings dialog box lets you configure the functional settings of the ESM data collector component.

To configure the ESM general settings

1. In the Edit Settings dialog box, click Data Collector - ESM.
2. In the panel, provide the following information:
Thread settings

- In the Thread count text box, type the number of ESM managers that the ESM data collector can communicate in parallel.
  The default value is 5.
- In the Thread timeout seconds text box, type the time in seconds after which the ESM data collector should terminate an idle thread.
  The default value is 600.

See “About the thread settings for ESM data collector” on page 153.

Poll settings

- In the ESM manager polling seconds text box, type the manager polling time in seconds.
  The default value is 30 seconds.
- In the ESM policy run submit retry seconds text box, type the policy run retry submit time in seconds.
  The default value is 300 seconds.

See “About the poll settings for ESM data collector” on page 154.

See “Configuring the ESM manager settings” on page 147.

About the thread settings for ESM data collector

A thread is a connection that an ESM data collector creates to communicate with an ESM manager to collect data. The ESM data collector can communicate with multiple ESM managers in parallel. The thread settings let you define the number of ESM managers the ESM data collector can contact in parallel.

You can configure the following parameters for the ESM thread settings:

Thread count

- Specify the number of ESM managers that the ESM data collector can communicate in parallel.
  The default value is 5.
The ESM data collector terminates a thread that continues to be idle for longer than the specified time. Specify the time in seconds after which the ESM data collector must terminate an idle thread. The default value is 600 seconds.

**Note:** The **Thread Timeout Seconds** setting impacts data collection only when the ESM data collector queries more than one manager in a data collection request.

See “Configuring the ESM manager settings” on page 147.

See “Configuring the ESM general settings” on page 152.

**About the poll settings for ESM data collector**

Sometimes, the ESM data collector initiates policy runs before the ESM manager starts data collection from the agents. You can configure the polling frequency of the ESM data collector to initiate the policy runs through the general settings configuration of the data collector.

The scenarios for which the ESM data collector uses the poll setting configurations are as follows:

- Establish contact with the ESM manager when the ESM data collector starts a new policy run.
- Determine the policy completion status.

The ESM manager lets only four concurrent policy runs in the starting state on the ESM manager. If you initiate the fifth policy run, the ESM manager displays the following error:

*Could not start job: server too busy. Reschedule job for a later time.*

You can configure the following parameters for the ESM poll settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM manager polling seconds</td>
<td>Specify the interval period after which the ESM data collector must query the ESM manager to find the policy completion status. The default value is 30 seconds.</td>
</tr>
</tbody>
</table>
ESM policy run submit retry seconds

The ESM data collector re-submits a policy run if the data collector encounters an error when it starts the policy run. Specify the interval period after which the ESM data collector must try to re-submit a policy run on the ESM manager.

The default value is 300 seconds.

See “Configuring the ESM manager settings” on page 147.

See “Configuring the ESM general settings” on page 152.

Changing the Data Processing Service settings

Symantec recommends that you change the settings of the DPS that is configured for ESM data collection. You can configure the DPS settings from the computer where the Data Processing Server service is installed.

To change the Data Processing Service settings

1 Open the DPS configuration file from the following location:

   <Install Directory>\Symantec\CCS\Reporting and Analytics\DPS\Symantec.CSM.DPS.exe.config

2 Add the keys in the <appSettings> section of the configuration file.

   You can restrict the maximum number of concurrent jobs that the DPS handles to four when you specify the values that are mentioned in the table.

   The following table lists the keys that you need to add in <appSettings> and the key descriptions.

<table>
<thead>
<tr>
<th>Key Description</th>
<th>Key Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the DPS to have at least one worker process at any given point of time.</td>
<td>WPM_MinimumWorkerProcesses</td>
</tr>
<tr>
<td>Configures the DPS to create maximum of two concurrent worker processes for processing the data collection job.</td>
<td>WPM_MaximumWorkerProcesses</td>
</tr>
<tr>
<td>Configures the DPS to assign maximum of one job to a single worker process.</td>
<td>WPM_MaximumJobsPerWorkerProcess</td>
</tr>
</tbody>
</table>

3 Restart the DPS Service.

The configuration of the DPS for the ESM data collector with other roles such as evaluation or reporting may affect the data collection performance. Symantec
recommends that you install a DPS only with the DPS Collection role for the ESM data collector.

Configuring the CSV data collector

In the Control Compliance Suite, you can store assets in a CSV file and import them using a CSV data collector. The assets and their relevant data must be arranged in a specific format in the CSV file for importing them into the infrastructure using the CSV data collector.

See “About format of the CSV file headers” on page 353.

In the Control Compliance Suite, a DPS that is registered to a site can be configured as a CSV data collector. The DPS can be configured as a CSV data collector either from the Grid View or from the Map View of the console. Before configuring the DPS, ensure that the CSV file containing the assets is placed in a network share path of the computer that hosts the DPS.

---

**Note:** If a CSV file is shared on a DPS collector computer, then ensure that the user has either log on locally or log on as a batch job permission. This permission is required for the CSV data collector of both the single setup and distributed setup modes. The user is the one whose credentials are required to access the network share path. The same user credentials are also specified for the selected platform of the CSV option in the **Edit Settings** dialog box.

The CSV data collector is used to collect data in the following scenarios:

- To collect data for the common fields of the predefined asset types.
  You must use the platform, Common in the Common settings dialog box for the CSV configuration.
  See “Configuring Common platform through CSV settings” on page 326.

- To collect data for assets that are stored in the CSV files for any predefined asset type or a custom application.

See “Configuring the data collectors” on page 138.

**To configure the CSV data collector**

1. Go to Settings > System Topology.
2. Do one of the following:
   - In the System Topology > Grid View, right-click the Data Collection Service and click **Edit Settings**.
   - In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, select **CSV** under the Data Collector Sites option on the left pane of the dialog box.

4. Select the site to which the DPS is registered from the Site Name drop-down box on the right side pane of the dialog box.

5. Enter values for the fields to configure the CSV data collector.

   The fields and the descriptions are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Enter the platform of the application whose data is to be queried. You can use the drop-down box to select the platform of the application.</td>
</tr>
<tr>
<td>CSV File(s) Path</td>
<td>Enter the path where the CSV file is placed. If you are importing assets from the Altiris CMDB, the file path should point to location of the CSV file on Altiris Notification Server. The CSV file is created by the CCS Asset Export Task solution on Altiris Notification Server. See “About importing assets from Altiris” on page 411. Click the browse button and in the Browse for folder dialog box, browse to the path where the CSV file is located. You must ensure that the CSV file path is specified in the UNC format, &lt;server name&gt;&lt;share name&gt;&lt;path&gt;&lt;filename&gt;.csv.</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>Enter the domain of the Windows computer, where the CSV file is located. You need to provide the credentials of the Windows domain user in the dialog box, Credentials for the Platform.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name of the specific domain.</td>
</tr>
</tbody>
</table>
Enter the search pattern of the CSV file. For example, in a given share path there can be several CSV files for the same platform. In such a case, if you want to have data from the CSV file that starts with the alphabet, m, then the search option can be, m*.csv.

Enter the encoding type of the file. For example, Unicode (UTF-8).

You can use the drop-down box to select the unicode of the CSV file.

6 Click Save.

See “Creating a CSV file for custom application” on page 357.

See “Creating a CSV file for predefined asset types” on page 356.

**Configuring the ODBC data collector**

You can configure a Data Processing Service (DPS) as an ODBC data collector to collect data from the ODBC compliant databases.

See “About the ODBC data collector” on page 159.

See “Configuring the data collectors” on page 138.

**To configure an ODBC data collector**

1 Go to Settings > System Topology.

2 Do one of the following:

   ■ In the System Topology > Grid View, right-click the Data Collection Service and click Edit Settings.

   ■ In the System Topology > Map View, right-click a registered DPS component and click Edit Settings.

3 In the Edit settings dialog box, under the Data Processing Service section, select Basic and check ODBC Data Collector.

4 In the Edit settings dialog box, select ODBC under the Data Collector Sites option on the left pane of the dialog box.

5 Select the site to which the DPS is registered from the Site Name drop-down box on the right side pane of the dialog box.

6 Enter values for the fields to configure the ODBC data collector.
Click Save.

See “Format to create ODBC compliant database tables” on page 363.

### About the ODBC data collector

The ODBC data collector is used to import assets and collect data from the Open Database Connectivity (ODBC) compliant databases. For example, you maintain an Oracle database that stores asset details of various Oracle computers, which you can import using an ODBC data collector. In Control Compliance Suite, you must configure a DPS as an ODBC data collector.

The ODBC data collector is equipped to import assets of predefined platforms or custom platforms and also collect data for the assets. The data collector interprets data only if the database table or view names and the column names are defined in a specific format.

See “Format to create ODBC compliant database tables” on page 363.

The end-to-end sequence to import assets and collect data using the ODBC data collector is as follows:

- Identify the assets for which data is to be collected using the ODBC data collector.
  
  Assets belonging to either the predefined platforms or custom platforms can be imported.
  
  See “Predefined platforms” on page 235.

- Create ODBC compliant database, which contain the assets that you want to import and their data. The ODBC compliant database tables or view names and the column names must be of the defined format for easy interpretation by the Control Compliance Suite for asset import or data collection.
  
  See “Format to create ODBC compliant database tables” on page 363.

---

**Note:** If the database table or column names are not as per the naming convention, then you can manually map them through a dialog box.

- Register a DPS as the ODBC data collector through the Edit Settings dialog box.
  
  You must navigate to the Edit Settings > Data Processing Service > Basic and check the option, ODBC Data Collector.

- Configure the DPS as the ODBC data collector.

- Import the assets through the Create or Edit Asset Import Job wizard.
  
  See “Importing the assets for the first time” on page 319.
See “Configuring the ODBC data collector” on page 158.

About the entity table mapping

Entity table mapping is about mapping the entities and their fields to the database table or view names and the database table column names, respectively. For a custom application, you create the entities and their fields using the Create New Entity Schema wizard.

See “Creating a new entity schema” on page 461.

The infrastructure performs data collection from the ODBC compliant databases using the ODBC data collector. For easy interpretation of data by the ODBC data collectors, define the database table or view names and column names as per the defined format. As per the defined format, the entities that you create for a platform are mapped with the database table or view names. Similarly, the fields are mapped with the table column names. After all these requirements are met, the ODBC data collector can successfully import assets or collect data.

See “Format to create ODBC compliant database tables” on page 363.

The entity table mapping option provides you the recommended table or view names for every entity and the recommended column names for every field. The option intuitively derives the entities from the entity schema and provides the recommended corresponding database table or view names. Similarly, the option also provides the mapping between the fields and the recommended table column names. These mappings can be viewed through the Entity Table Mapping dialog box. If you create table or view names or column names that are not as per the defined format, then you can edit them through this dialog box.

The mappings are primarily performed to map the entities and their fields with the unconfigured database table names, view names, or column names. The mappings can be performed through the SQL query too. For example, a SQL database has a table or view name as MyTable, which is to be mapped to the Windows Machine entity of the Windows platform. The fields of the Windows Machine entity are Domain Name and Machine Name and the column names of the MyTable view are FieldSample1 and FieldSample2. You must map the fields, Domain Name and Machine Name with the table column names, FieldSample1 and FieldSample2 respectively.

You do not need to use the entity table mapping option if you manually create the database table or view names or the column names as per the defined format.

The entity and field mappings for all the predefined platforms are displayed in the Entity Table Mapping dialog box.

See “Predefined asset types” on page 236.
Switching between CSV and ODBC data collectors

For custom platforms, even after you configured a default data collector, you can still switch over to another data collector to do asset import or data collection. This switching of data collector function is performed through the dialog box, **Switch CSV or ODBC Data Collector**. You can switch between a configured CSV data collector and an ODBC data collector to import assets and collect data for any custom platform.

After you switch, the data collector to which you switched the selected platform becomes the default data collector for importing assets. For example, you have configured a CSV data collector to collect data for a custom platform, DB2. Later, you want to switch to ODBC data collector to import assets and collect data for the same platform, DB2. You use the dialog box to switch between the CSV and the ODBC data collector.

You can also switch the common platform fields alone from one configured data collector to another. The common platform contains the common fields of an asset type.

See “**Common fields for all asset types**” on page 345.

**To switch between CSV and ODBC data collectors**

1. Go to **Settings > Schema Manager** in the console.
2. In the **Schema Manager** view, click **Switch CSV or ODBC data collector**.
3. In the **Switch CSV or ODBC Data Collector** dialog box, provide the details to switch a data collector.

See “**Importing the assets for the first time**” on page 319.

Configuring the application server settings

You can change the authentication type for storing the security settings.

**To configure the application server settings**

1. Go to **Settings > System Topology**.
2. Do one of the following:
   - In the **System Topology > Grid View**, right-click the application server component and click **Edit Settings**.
   - In the **System Topology > Map View**, right-click the application server component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, click **Application Server**.
4 On the **Application Server - Basic** panel, select one of the following authentication types:

- **Use controlled delegation of security rights**
  - Select this option if you want to use the Constrained Delegation feature of Windows 2003.

- **Use Control Compliance Suite to store the password**
  - Select this option if you want to use the built-in storage to store the encrypted password.
On the Application Server - Integration Services panel, provide the following information:

- **Enabled**: Select this option to enable the TCP/HTTPS/HTTP protocol.
  - The field is not editable for the TCP.

- **Metadata Enabled**: Select this option if you want to use the Integration Services APIs over TCP or HTTPS or HTTP binding.

- **Port Number**: Type the port number.

- **Transport Name**: This option is not editable.
  - The transport name is populated from the Directory Server.

- **Enabled**: Select this option to enable the Windows Security or the Username Security based on how you want to make APIs calls.
  - In case of TCP/IP and HTTP, you can only use the Windows Security. In case of HTTPS, you can use either the Windows Security or Username Security.

- **BindingFactory**: This option is not editable.
  - The transport name is populated from the Directory Server.

- **ClientBindingFactory**: This option is not editable.
  - The transport name is populated from the Directory Server.

- **UriSuffix**: This option is not editable.
  - The transport name is populated from the Directory Server.
Public Transport

Select from the Yes or No options.
If you select Yes, only the public APIs are exposed. If you select No, both the public and the internal APIs are exposed.

Exception Details In Faults

Select from the Yes or No options.
If you select Yes, the internal error details that occur on the Server side also are included in Faults.

6 Click Save.

See “About the security settings for scheduled jobs” on page 164.
See “Adding credentials for scheduled jobs” on page 164.

About the security settings for scheduled jobs

Control Compliance Suite (CCS) provides the option to store the user password that is required for asset resolution when running scheduled jobs.

During installation, the administrator can choose from one of the following security settings:

- Use controlled delegation of security rights
  CCS uses the Constrained Delegation feature of Windows 2003
- Use Control Compliance Suite to store the password
  CCS uses the built-in secured storage to the encrypted password

Administrator can later choose to change the security setting from the Settings > System Topology > Map view.

See “Configuring the application server settings” on page 161.

Only users with the role to schedule jobs can store their passwords from the Home > User Preferences view.

See “Adding credentials for scheduled jobs” on page 164.

Adding credentials for scheduled jobs

Users with the role to schedule jobs can store their passwords. The password is required for asset resolution on the jobs that are scheduled to run at a later time.
This feature is available only if the administrator has selected the option to store password in Control Compliance Suite.

See “About the security settings for scheduled jobs” on page 164.

Only users with the role to schedule jobs can store their passwords.

To add user preferences

1. Go to the Home > User Preferences.
2. In the User Preferences view, type the password.
3. Click Update password.

Configuring the general settings

The Control Compliance Suite Console comes configured with default values for the various system settings. You can change the values to meet your organization's requirements. Only users with the Administrator role can configure the settings.

You can configure the settings from the Settings > General view.

Configuring the data locations

Data location configuration is about configuring a network share path of a computer or to establish connection with an ODBC database. Such configuration facilitates import of files through the network share path of a computer or establish connection with an ODBC database table for data collection. You can place CSV or XML files in the network share path, which require credentials to access.

Note: If you change the data location configuration, then you must synchronize the DPS with the latest configuration. You can synchronize DPS using the Sync Configuration option from the Settings > General > Data Processing Service view.

To configure the data location

1. Go to Settings > General.
2. In the General view, on the left panel, click System Configuration > Data Locations.
3. On the right panel, click Add.
4 In the **Add Data Location** dialog box, provide the required information.
   To edit an existing data location, select the data location and click **Edit**.
   To delete an existing data location, select the data location and click **Delete**.
5 Click **OK** to save.

### Enabling and disabling audit setting

Configuring the audit settings is a system-wide setting that applies to all CCS users.

**To configure auditing**

1 Go to **Settings > General**.
2 In the **General** view, on the left panel, click **System Configuration > Auditing**.
3 On the right panel, do one of the following:
   ■ To enable auditing, check **Enable Auditing**.
   ■ To disable auditing, uncheck **Enable Auditing**.

See “About audits” on page 178.

### Configuring the email Notification Server

You must specify the server and the port number to send and receive notifications in Control Compliance Suite (CCS).

CCS can be configured to send notifications for the following events:

■ Completion of the asset import jobs.
■ Completion of the data collection and data evaluation jobs.
■ Expiration of an exception.
■ Change in the status of a policy.
■ Response to policy clarification requests.
■ Change in status of a dashboard or a dashboard update job.
■ State transitions of the control points.
■ Asset remediation.
To configure the email notification settings

1. Go to Settings > General.
2. In the General view, on the left panel, click System Configuration > Email Notifications.
3. On the right panel, provide the following information:

   - **Notification Server**: Type the name of the computer that hosts the SMTP server. The name is specified in any format: computer name, IP address, or host name.
   - **From Email Address**: Type the default email address that is used in the Job wizards to send notifications. If required, at the time of creating the job you can change the address in the wizard.
   - **Notification Port**: Type the port number of the computer that hosts the SMTP server.

See “About the job types” on page 712.

### Selecting the DPS to synchronize the reporting database

You can select the Data Processing Service (DPS) that is used for synchronizing the reporting database. The reporting database is periodically synchronized with the data that is stored in the production database. Data is synchronized when the Reporting Database Synchronization job is run.

**To select the DPS for data synchronization**

1. Go to Settings > General.
2. In the General view, on the left panel, click System Configuration > DPS for Reporting Synchronization.
3. On the right panel, select the DPS that can be used for synchronization of the reporting database.

See “About the Control Compliance Suite Data Processing Service” on page 37.

### Synchronizing the reporting database

Configuring the report server settings is a system-wide setting that applies to all Control Compliance Suite (CCS) users.

You can choose to synchronize the reporting database immediately after certain jobs are completed.
To perform data synchronization

1. Go to Settings > General.
2. In the General view, on the left panel, click System Configuration > Reporting Synchronization.
3. On the right panel, you can do the following:
   - **Check/uncheck jobs for synchronization**
     - Check or uncheck the jobs for the reporting database synchronization. By default, all the jobs are selected.
     - If you uncheck any of the jobs, the corresponding job data is synchronized when the scheduled reporting data synchronization job is run.
     - If you check any of the jobs, the corresponding job information is synchronized in the reporting database immediately after the jobs are completed.

See “About data synchronization” on page 737.

About the purge settings

When objects in the Directory are deleted, the corresponding information and results are stored in the database. The database must be purged regularly to maintain optimum performance. As the database grows, the results are longer queries, corrupt databases, and depleted disk space.

Control Compliance Suite (CCS) includes a default global purge setting. Some modules have their own purge settings. You can schedule the purge job to run periodically.

You can configure the purge settings from the System > General > Data Purge > Purge Settings panel.

The following are the different purge settings tabs in the Purge Settings panel:

- **Stale Data**
  - Settings for the global purge.
  - The number of days after which data is purged. The default value is 180 days.

- **Exceptions**
  - Settings for purging the exceptions data.
  - The exceptions data older than the number of days that is specified in the Exceptions tab is deleted. The default value is 180 days.
### Standards
Settings for purging the standards data.

The standards data older than the number that is specified in the **Stale Data** tab are deleted.

Data can also be deleted if it is younger than the number that is specified. The data collection results and the data evaluation results for runs greater than the number that is specified in the **Standards** tab are deleted.

**Note:** A purge of evaluations results does not re-compute summary statistics until another evaluation is executed.

### Entitlements
Settings for purging the historical entitlements data.

The entitlements historical data older than the number of days that is specified in the **Entitlements** tab is deleted. The default value is 180 days.

The minimum value is 100 days and the maximum value is 9999 days.

### System Audit Log
Settings for purging the historical audit log data.

The audit log historical data older than the number of days that is specified in the **System Audit log** tab is deleted. The default value is 365 days.

See “About audits” on page 178.

### Baselines
Settings for purging the comparison results.

The comparison results older than the number of days that is specified in the **Baselines** tab is deleted. The default is 60 days.

### Reports
Settings for purging the report results in the reporting database.

The report results older than the number that is specified in the **Reports** tab are deleted. Report results are also deleted for runs greater than the number that is specified in the **Reports** tab.

See “Configuring the purge settings” on page 169.

See “Configuring the purge job schedule” on page 170.

### Configuring the purge settings
Control Compliance Suite (CCS) comes configured with default purge settings. You can change the values if you prefer different settings.

See “About the purge settings” on page 168.
To configure the purge settings

1. Go to **Settings > General**.
2. In the **General** view, on the left panel, click **Data Purge > Purge Settings**.
3. On the right panel, do the following:

   - **Stale Data**
     Type the number of days after which the information in the production database is purged. The default value is 180 days.
     The stale data setting is used as the default global purge setting. Some modules have their own purge settings.
     Select the purge schedule options.

   - **Exceptions**
     Type the number of days after which the exceptions data is purged. The default value is 180 days.

   - **Standards**
     Type the number of data collection job runs, the results of which must be retained. The default value is 10
     Type the number of data evaluation job runs, the results of which must be retained. The default value is 10.

   - **Entitlements**
     Type the number of days after which the entitlements historical data is purged. The default value is 180 days.
     The minimum value is 100 days and the maximum value is 9999 days.

   - **System Audit Log**
     Type the number of days after which the historical audit log data is purged. The default value is 365 days.

   - **Baselines**
     Type the number of days after which the baselines comparison result is deleted. The default is 60 days.

   - **Reports**
     Type the number of report job runs, the results of which must be retained. The default value is 10.
     Type the number of days after which the information in the reporting database is deleted.

4. On the **Purge Settings > State Data** tab, click **Execute Job** to run the job according to the selected schedule options.

See “Configuring the purge job schedule” on page 170.

Configuring the purge job schedule

You can check the status of a purge job from the **Monitor > Job Management** view.
To configure the purge schedule

1. Go to Settings > General.
2. In the General view, on the left panel, click Data Purge > Purge Settings.
3. On the Stale Data tab, Select one of the following schedule options:
   - **Run now**
     Select this option to run the job immediately after you click Schedule Job.
   - **Run periodically**
     Select this option to run the job on a specified date and time.
     Provide the following information:
     - **Start on** Select the date and time to run the evaluation job.
     - **Run once** Select this option to run the job one time on the specified date and time.
     - **Run every** Select this option to specify how often (in days) the scheduled purge job runs.

4. Click **Execute Job** to save the settings and run the job that is based on the settings.

See “About the purge settings” on page 168.

See “Configuring the purge settings” on page 169.

Configuring the entitlements settings

Configuring the entitlements settings is a system-wide setting that applies to all Control Compliance Suite users.
To configure the entitlements settings

1. Go to Settings > General.

2. In the General view, on the left panel, click Application Configuration > Entitlements.

3. On the right panel, provide the following information:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi select approval tasks</td>
<td>Select the check box to allow data owners to change and approve multiple control points at the same time.</td>
</tr>
<tr>
<td>Daily Approval Job run time</td>
<td>Select the time to schedule the entitlements approval job. The approval job starts and ends the review cycles.</td>
</tr>
<tr>
<td>Automatically Import Entitlements</td>
<td>Select the check box if you want the system to automatically import the entitlements at a scheduled time.</td>
</tr>
<tr>
<td>Automatic Import Job Runtime</td>
<td>If you have selected to automatically import entitlements, select the time to schedule the job.</td>
</tr>
<tr>
<td>Connection timeout interval</td>
<td>Select the database timeout interval. The database terminates the session when it reaches the specified time.</td>
</tr>
<tr>
<td>Revert Import Pending Control Point Status</td>
<td>Due to system failure the status of some control points are left in the Entitlement Import Pending status. Select this option to change the status of the control points with status Entitlement Import Pending to Entitlement Import Required.</td>
</tr>
</tbody>
</table>

See “About entitlements” on page 483.

Configuring the exceptions settings

Configuring the exceptions settings is a system-wide setting that applies to all Control Compliance Suite users.
To configure the exceptions settings

1. Go to Settings > General.
2. In the General view, on the left panel, click Application Configuration > Exceptions.
3. On the right panel, provide the following information:

- **Expiration notification period**: Type the number of days before the expiration date when a notification must be sent.
- **Run the exceptions update job at**: Select the time to schedule the exception management job.
- **From address for exception details**: Type the email address from which the email notification is sent.

See “About exceptions” on page 530.

Customizing the report logo and name

You can select the company logo and the company name to replace the existing logo and the name that appear on the report.

The following is the recommended logo size:

- For the company logo: The maximum size is 44 x 42 pixels at 72 DPI resolution.
- For the company banners that contain both the logo and name: The maximum size is 570x42 pixels at 72 DPI resolution.

To customize the report logo and name

1. Go to Settings > General.
2. In the General view, on the left panel, click Application Configuration > Report Customization.
3. On the right panel, click Add to select the logo and the company name.
4. To set the default logo, select the logo and click Set Default.
5. To set the default company name, select the company name and click Set Default.

See “Working with reports ” on page 745.
Configuring the policy settings

Configuring the policy settings is a system-wide setting that applies to all Control Compliance Suite users.

To configure the policy settings

1. Go to Settings > General.
2. In the General view, on the left panel, click Application Configuration > Policies.
3. On the right panel, provide the following information:

- **Expire policies after**
  Type the default number of days of a policy’s life span. When a policy is created, this number is used to calculate the policy expiration date.

- **Policies must be reviewed within**
  Type the default number of days for reviewing a policy. When a policy is created, this number is used to calculate the date by when a policy must be reviewed.

- **Clarifications are due within**
  Type the default number of days for submitting a clarification.

- **Run the daily policies update job at**
  Select the daily scheduled time to run a policy job.

- **Notifications**
  You can configure the notifications that are sent to the assigned policy users at different stages of the policy life cycle. The notifications are meant to inform the user about the status of the policy. The notifications are sent as an email.

  - **Notification type**
    Select the type of policy notification.

  - **Subject**
    You can type the subject of the email notification.

  - **Message**
    You can customize the message of the policy.

  **Note**: Policy notifications are sent only if the From email address is specified in Settings > General > System Configuration > Email Notifications.

  See “Configuring the email Notification Server” on page 166.

See “Working with policies” on page 693.
Configuring the dashboard settings

Configuring the dashboards is a system-wide setting that applies to all the tiered dashboards. You can configure the security assessment status level settings to all the evaluation nodes and the dashboard job settings.

To configure the dashboard settings

1. Go to Settings > General.

2. In the General view, on the left panel, click Application Configuration > Tiered Dashboards.

3. On the right panel, provide the following information:

Global Threshold Settings tab

Define a threshold for each status level of Standards and bv-Control query.

The four possible security assessment status levels for the dashboard are:

- Critical
- Danger
- Warning
- Normal

The build-up of the security assessment of the evaluation nodes for both bv-Control and Standards evaluation results determine a dashboard’s security assessment status.

See “Example of status calculation for bv-Control Query Results node” on page 775.

See “Example of status calculation for Standards Evaluation Results node” on page 774.

Global Job Settings tab

Type the maximum number of update jobs that can be assigned to each Data Processing Service (DPS) in the Reporting role.

See “About the Control Compliance Suite Data Processing Service” on page 37.

See “About threshold settings in tiered dashboard” on page 772.

See “About status calculation” on page 774.

See “About the threshold types” on page 772.
Configuring the remediation settings

You must configure the remediation settings to create the ServiceDesk tickets and to send email notifications for asset remediation.

To configure the remediation settings

1. Go to **Settings > General**.
2. In the **General** view, on the left panel, click **Application Configuration > Remediation Settings**.
3. On the right panel, provide the following information:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Desk Incident Web Service URL</strong></td>
<td>Type the fully qualified URL of the Web Service. The URL is used to create ServiceDesk tickets for asset remediation.</td>
</tr>
<tr>
<td></td>
<td>http://&lt;serverName&gt;/SD.Remediation.RemediationService.asmx</td>
</tr>
<tr>
<td><strong>CCS Web Server</strong></td>
<td>Type the name of the computer that hosts the CCS Web server. The Web server is used to communicate with the ServiceDesk application to reevaluate the assets that required remediation. The Web server is also used to send email notifications for the assets that require remediation. The name is specified in any of the following formats: IP address, the fully qualified DNS, or the computer.</td>
</tr>
<tr>
<td></td>
<td>The Web server account must exist in the ServiceDesk application as the account is the primary contact for the ServiceDesk tickets that are submitted from CCS.</td>
</tr>
<tr>
<td><strong>Submitting contact email</strong></td>
<td>Type the contact email address. The email address is used as the From address in the email notifications that are sent for asset remediation. The email account must exist in the ServiceDesk application as the account is the primary contact for the ServiceDesk tickets that are submitted from CCS.</td>
</tr>
<tr>
<td><strong>Maximum assets per ticket</strong></td>
<td>Type the maximum number of assets that can be included in a remediation ticket for each asset type. The default value is 20. The minimum value is 1.</td>
</tr>
</tbody>
</table>

See “About remediation” on page 661.
Configuring the standards settings

You can configure the maximum number of job runs that are displayed for each asset. You can also set the number of data collection results that are displayed for each category of the standard.

By default, the 10 most recent job runs are displayed.

To configure the standards settings

1. Go to Settings > General.
2. In the General view, on the left panel, click Application Customization > Standards.
3. On the right panel, provide the following information:
   - Type the number of job runs to be displayed in Evaluation tab for each asset.
     The Evaluation tab is displayed in the Manage > Assets > Asset System view and in the Manage > Standards view.
   - Type the number of job runs to be displayed in Data Collection tab for each asset.
     The Data Collection tab is displayed in the Manage > Assets > Asset System view.
   - Type the number of data collection results to be displayed in the Data Collection Details dialog box for each category of the standard.
     The Data Collection Details dialog box is displayed when you click the view icon on the Data Collection tab in the details pane of Manage > Assets > Asset System view.
     The details pane displays the details of the assets that are evaluated against a standard.

See “Viewing asset information in the details pane” on page 394.
See “Viewing standard information in the details pane” on page 598.

Configuring the job count settings

You can configure the number of jobs and the job runs that are displayed in the Monitor > Jobs view.

By default, 20 jobs and 10 job runs are displayed. For each job, the most recent job runs are displayed. Entering the value zero displays all jobs and job runs.
To configure the job count settings
1. Go to Settings > General.
2. In the General view, on the left panel, click Application Customization > Job Count.
3. On the right panel, provide the following information:

   Number of Jobs  Type the number of jobs to be displayed in the Monitor > Jobs view.

   Number of Job Runs  Type the number of job runs to be displayed in the Monitor > Jobs view.

   For each job, the specified number of job runs are displayed.

See “About the Jobs view” on page 715.

Configuring the assets count settings

You can configure the number of assets that are displayed in the Manage > Assets > Assets System view.

By default, 2000 imported assets are displayed. Entering the value zero displays all the assets in the system.

To configure the assets count setting
1. Go to Settings > General.
2. In the General view, on the left panel, click Application Customization > Assets Count.
3. On the right panel, type the number of assets.

   The assets are displayed in the Manage > Assets > Assets System view.

See “Performing the tasks in the Asset System view” on page 375.

About audits

An audit of the Control Compliance Suite (CCS) involves tracking and logging the events that occur on the system. You can change the audit settings to comply with your organization's standards. You can either enable or disable auditing in the Settings > General view. Auditing is a system-wide setting. Auditing tracks the changes to standards, policies, and assets and captures the data to an audit log. The log captures the information on who changed what and when the change was made. The log can track the changes to permissions on the objects.
An audit usually includes the following tracking information:

- Insertions of new records
- Deletions of existing records
- Modifications of existing records

See “About audit event triggers” on page 179.

See “Enabling and disabling audit setting” on page 166.

See “About viewing the audit logs” on page 180.

### About audit event triggers

The following are the actions that trigger an audit event:

<table>
<thead>
<tr>
<th>Event type</th>
<th>Module</th>
<th>Triggering Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Change</td>
<td>C1 Core</td>
<td>An attribute of an asset is changed.</td>
</tr>
<tr>
<td>Job Execution</td>
<td>C1 Core</td>
<td>At the successful completion of every job that the application server launches.</td>
</tr>
<tr>
<td>Job Creation/Deletion</td>
<td>C1 Core</td>
<td>Log the creation or deletion of a job</td>
</tr>
<tr>
<td>Role Member Change</td>
<td>C1 Core</td>
<td>A person or group is added to and or removed from a role.</td>
</tr>
<tr>
<td>Role Create/Delete</td>
<td>C1 Core</td>
<td>A role is created or deleted.</td>
</tr>
<tr>
<td>Role Power Change</td>
<td>C1 Core</td>
<td>A power is added to or removed from a role.</td>
</tr>
<tr>
<td>Policy Change</td>
<td>Policy</td>
<td>Any component of a Policy is modified.</td>
</tr>
<tr>
<td>Standard Change</td>
<td>Standards</td>
<td>Any component of a Standard is modified. Each modification creates a separate log entry of this type.</td>
</tr>
<tr>
<td>Policy Module Control Statement Create/Change/Delete</td>
<td>Policy</td>
<td>A control statement is created, changed, or deleted.</td>
</tr>
<tr>
<td>Policy Module Control Statement Assignment/De-Assignment</td>
<td>Policy</td>
<td>A control point is linked to or delinked from a policy.</td>
</tr>
</tbody>
</table>
Table 3-23  Audit Event Triggers (continued)

<table>
<thead>
<tr>
<th>Event type</th>
<th>Module</th>
<th>Triggering Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Point Configuration Change</td>
<td>Entitlement</td>
<td>The configuration for a control point is changed. The configuration may include a change in published status, data owner, management classification, department, or review cycle.</td>
</tr>
<tr>
<td>Control Point Approval or Rejection/Request for Change</td>
<td>Entitlement</td>
<td>A control point entitlement approval or request for change occurred.</td>
</tr>
<tr>
<td>Control Point Approval Violation</td>
<td>Entitlement</td>
<td>A control point review cycle ended without the required approval event.</td>
</tr>
</tbody>
</table>

See “About audits” on page 178.

About viewing the audit logs

You can generate audit reports and view the reports in the My Reports view after they are scheduled.

You cannot open or view an audit log within the console. A SQL Server database maintains the audit logs. With the appropriate permissions and third-party tools, you can view the log data.

See “About audits” on page 178.

See “About audit event triggers” on page 179.

Managing licenses

You can add licenses at the time of Control Compliance Suite (CCS) installation or at a later time from the console's Licenses view. You must provide the core license during installation. The core license, CCS_Core.slf, is required for installing the Directory Support Service and the CCS Application Server components.

The CCS licenses are stored in the ELS (Enterprise License Store) store of the product (C:\Program Files\Common Files\Symantec Shared\Licenses).

In the CCS Console, users can view and add CCS license files from the Licenses view. Users can view only those features that have a valid license.

You cannot open the CCS Console if the core license expires. The core license can be renewed from the stand-alone utility Symantec.CSM.LicenseUtil.exe that is stored in the following location:
<install directory>\CCS\Reporting and Analytics\Directory Support Service\ 
See “Adding licenses on the Directory Server” on page 182.

The CCS Console does not display any expired component's features. The system displays a message to indicate that a license has expired.

See “About the Licenses view” on page 181.
See “Adding a license” on page 181.
See “Viewing the list of licenses” on page 182.

About the Licenses view

In the Settings > Licenses view, the user can view, and add licenses. You can check the status, the type, the product ID, and the expiration dates of licenses.

You can use the Licenses view for the following tasks:

- View registered licenses for the installed Control Compliance Suite components.
- Add a new license.

The Licenses view displays the following information for each license:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Component name and its version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Valid or Invalid license</td>
</tr>
<tr>
<td>Product ID</td>
<td>Component name</td>
</tr>
<tr>
<td>Expires</td>
<td>Expiration date of the license. Some licenses never expire.</td>
</tr>
</tbody>
</table>

See “Managing licenses” on page 180.
See “Adding a license” on page 181.
See “Adding licenses on the Directory Server” on page 182.
See “Viewing the list of licenses” on page 182.

Adding a license

When you add a license you enable an installed feature.

To add a license

1. Go to Settings > Licenses.
2. In the Licenses view, click Add License.
3 In the Add Licenses dialog box, click Import to add the license.

4 Locate and open the license file, then select the license or licenses to add and click Open, or double-click a license.

5 Click OK.

See “Managing licenses” on page 180.

See “About the Licenses view” on page 181.

See “Adding licenses on the Directory Server” on page 182.

See “Viewing the list of licenses” on page 182.

Adding licenses on the Directory Server

When you add a license you enable an installed feature. You can use the Symantec.CSM.LicenseUtil.exe utility on the Control Compliance Suite Directory Server to add license files. The tool imports a Symantec License File (.slf) and activates the software.

The tool is available on the Directory Server host at <install directory>\CCS\Reporting and Analytics\Directory Support Service\Symantec.CSM.LicenseUtil.exe.

See “Managing licenses” on page 180.

To add a license on the Directory Server

1 On the Directory Server host, open the Symantec.CSM.LicenseUtil.exe tool.

2 In the Add Licenses dialog, click Add Licenses.

3 Locate and open the license file, then select the license or licenses to add and click Open, or double-click a license.

4 In the Add Licenses dialog, click Done to close the utility.

Viewing the list of licenses

You can view the list of licenses and their status.

To view a list of licenses

1 Go to Settings > Licenses.

2 The Licenses view lists the Control Compliance Suite licenses and their status.

See “Managing licenses” on page 180.

See “About the Licenses view” on page 181.

See “Adding a license” on page 181.
Managing users

Control Compliance Suite (CCS) lets you store the CCS user and group accounts. The user accounts are automatically added when the users are assigned to roles. The user and the group accounts can also be imported from a CSV file. The accounts store the user and the group email addresses that are used to send any updates.

See “About the User Management view” on page 183.

About the User Management view

The User Management view lists all the Control Compliance Suite (CCS) users and groups.

You can do the following from the User Management view:

■ Import user and group accounts from a CSV file
   See “Importing user accounts” on page 183.

■ Update email addresses
   See “Updating a user email address” on page 184.

■ Delete user and group accounts
   See “Deleting user accounts” on page 184.

■ Update all users and groups from the domain
   See “Updating user accounts” on page 185.

See “Managing users” on page 183.

About adding a user account

When a user is assigned a role in the Settings > Roles view, an account for the user is automatically created in the system. All of the Control Compliance Suite users and groups are displayed in the Settings > User Management view.

See “About the User Management view” on page 183.

See “Managing users” on page 183.

Importing user accounts

Control Compliance Suite lets you import user and group accounts from a CSV file.
The CSV file should contain fields in the following format:
<DomainName\SAM Account name>,<Display name>,<Mail ID>

<table>
<thead>
<tr>
<th>CSV field</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM Account name</td>
<td>ABC\jsmith</td>
</tr>
<tr>
<td>Display name</td>
<td>John Smith</td>
</tr>
<tr>
<td>Mail ID</td>
<td><a href="mailto:jsmith@abc.com">jsmith@abc.com</a></td>
</tr>
</tbody>
</table>

To import user and group accounts
1. Go to Settings > User Management.
2. In the User Management view, on the taskbar, click Import from CSV.
3. In the Open dialog box, browse to the location of the CSV file.
4. Select the file and click Open.

See “About the User Management view” on page 183.
See “Managing users” on page 183.

Updating a user email address

You can update a user email address from the User Management view.

To update user information
1. Go to Settings > User Management.
2. In the User Management view, select the user or the group account to update the email ID.
3. Click on the Mail ID cell of the user account, and type the email address.
   The system displays a message if the ID is invalid.

See “About the User Management view” on page 183.
See “Managing users” on page 183.

Deleting user accounts

You can only delete the user or the group accounts that are not responsible for any critical functions of the system. A message appears when you try to delete a user or the group account that is responsible for executing certain functions of the system.
To delete user accounts

1. Go to Settings > User Management.
2. In the User Management view, right-click the user or the group account to be deleted, and select Delete.

See “About the User Management view” on page 183.

See “Managing users” on page 183.

Updating user accounts

You can update all the Control Compliance Suite user and group accounts with current information from Active Directory.

To update user accounts

1. Go to Settings > User Management.
2. In the User Management view, select the check boxes of the user and group accounts to be updated.
3. From the Common Tasks menu, select Update.

See “About the User Management view” on page 183.

See “Managing users” on page 183.

Configuring the SQL Server settings

The following are the minimum permissions required to run the synchronization and reporting jobs:

Table 3-25 Minimum permissions required to run synchronization and reporting jobs

<table>
<thead>
<tr>
<th>Type of authentication</th>
<th>Server role</th>
<th>Database user</th>
<th>Database role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Authentication</td>
<td>Public</td>
<td>dbo</td>
<td>db_owner</td>
</tr>
<tr>
<td>SQL Authentication</td>
<td>Public</td>
<td>dbo</td>
<td>db_owner</td>
</tr>
</tbody>
</table>

You can modify the SQL Server settings of the reporting database and the production database. The SQL Server settings are initially configured in the Installation Wizard.

You can modify the settings from the Settings > Secure Configuration view.
Configuring the production database connection settings

You can modify the SQL Server settings of the production database that is initially configured in the Installation Wizard.

**Note:** If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

See “Troubleshooting when the message “Login failed for user &lt;user name&gt;” appears in the Web console” on page 919.

Use the settings to set up a new server. The data is not automatically migrated to the new database.

**To configure the production database settings**

1. Go to **Settings > Secure Configuration > Production Database Connection**.
2. Provide the following information:

   - **SQL Server**
     Type the computer name that hosts the SQL Server.
   - **Database name**
     Type the name of the database.
     By default, the existing database name is displayed in the text box.
   - **Instance name**
     Type the SQL Server instance name if the SQL Server database is not the default instance.
   - **Port number**
     Type the port number of the computer that hosts the SQL Server. By default, Control Compliance Suite Application Server connects through the port, 1433 of the SQL Server computer.
   - **Use SSL**
     Check this option if your computer that hosts the SQL Server is SSL enabled for communication.
   - **Use Windows NT Integrated Security**
     Select this option if you have installed the SQL Server in the Windows NT user context.
Use a SQL user name and password

Select this option if you have installed the SQL Server in a different user context.

Specify the authentication details of the user in the respective text boxes.

If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

You cannot specify the following special characters for the User name and the Password fields:

- Semicolon (;)
- Double quotes ("")

Connection timeout interval

Type the number of minutes after which the server terminates the connection attempt.

The default timeout interval is 30 minutes.

3 Click Update to save.

See “About the Control Compliance Suite production database” on page 41.

Configuring the reporting database connection

You can modify the SQL Server settings of the reporting database that is initially configured in the Installation Wizard.

Note: If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

See “Troubleshooting when the message “Login failed for user <user name>” appears in the Web console” on page 919.

The application server uses the settings to communicate with the reporting database. The reporting database stores the evaluated data that is used for generating reports.

Use the settings to set up a new server. The data is not automatically migrated to the new database.

To configure the reporting database settings

1 Go to Settings > Secure Configuration > Report Database Connection.
2 Provide the following information:
## Configuring SQL Server settings

<table>
<thead>
<tr>
<th><strong>SQL Server</strong></th>
<th>Type the computer name that hosts the SQL Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database name</strong></td>
<td>Type the database name. The default database name appears in the text box.</td>
</tr>
<tr>
<td><strong>Instance name</strong></td>
<td>Type the SQL Server instance name. The default SQL Server instance name appears in the text box.</td>
</tr>
<tr>
<td><strong>Port number</strong></td>
<td>Type the port number of the SQL Server instance. If the port is enabled, the SQL Server default instance listens on TCP port 1433.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Check this option if you want SQL Server to use SSL to encrypt network transmissions independent of the network protocol.</td>
</tr>
<tr>
<td><strong>Use Windows NT Integrated Security</strong></td>
<td>Select this option if you connect to the SQL Server instance using Windows Authentication.</td>
</tr>
</tbody>
</table>
| **Use a SQL user name and password** | Select this option if you connect to the SQL Server instance using SQL Server Authentication. You must specify the authentication details of the user in the respective text boxes. If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer. You cannot specify the following special characters for the User name and the Password fields:  
- Semicolon (;)  
- Double quotes ("") |
| **Connection timeout interval** | Type the number of minutes after which the server terminates the connection attempt and the query execution. The default timeout interval is 120 minutes. |

### Step 3

Click **Update** to save.

See “About the Control Compliance Suite reporting database” on page 41.
Configuring the application server credentials

Provide the credentials of the user in whose context the application server is run on the computer. You must also set the Service Principal Name for the Application Server service account.

See “Configuring service accounts with unconstrained delegation” on page 189.

See “Configuring the S4U and constrained delegation” on page 190.

To modify application server credentials

1. Go to Settings > Secure Configuration > AppServer Credentials.
2. Type the password that authenticates the specified user account.
3. Click Update password to save.

Configuring service accounts with unconstrained delegation

You need to configure the service accounts for the Directory Support Service (DSS) and the Application Server to operate with unconstrained delegation in distributed and single setup modes.

Note: Setting up of Service Principal Names (SPNs) is important for a successful installation and configuration of a distributed setup. You must execute the procedure to configure the service accounts for unconstrained delegation before you install the CCS components.

To configure the service accounts with unconstrained delegation

1. Identify the user accounts that you want to use as the service accounts for DSS and Application Server.
   The user accounts must have the necessary privileges.
2. Create the Service Principal Name (SPN) for the Application Server and the DSS services.
   The SPN for both the short NetBIOS name and the fully-qualified host name (FQDN) is created. While delegation can work without SPN in Windows Server 2000 domains, it can also fail depending on the operating system that is in use.
   You must associate an SPN to a single user account.
   The service-name portion of the SPN must match the following:
   ■ SetSpn -A Symantec.CSM.AppServer/appserver_machine\domain\appserver_account
- SetSpn -A Symantec.CSM.AppServer/appserver_machine.fqn domain\appserver_account
- SetSpn -A Symantec.CSM.DSS/dss_machine domain\dss_account
- SetSpn -A Symantec.CSM.DSS/dss_machine.fqn domain\dss_account
- SetSpn.exe -a http/IIS_computer's_NetBIOS_name DomainName\UserName
  This is applicable only for Windows Server 2003.
- SetSpn.exe -a http/IIS_computer's_FQDN DomainName\UserName
  This is applicable only for Windows Server 2003.

3 Enable delegation for the Application Server's service account.

The following service accounts are to be enabled:

<table>
<thead>
<tr>
<th>Windows Server 2003 Domain</th>
<th>In the user properties, go to the Delegation tab and select the option, <strong>Trust this user for delegation to any service (Kerberos only)</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 Domain</td>
<td>In the user properties for the Application Server account, go to Accounts tab and check the option, <strong>Account is trusted for delegation</strong>.</td>
</tr>
</tbody>
</table>

4 When installing the Application Server, specify the FQDN when prompted by the setup for the computer that installed the DSS. It is not mandatory to specify the FQDN, but sometimes specifying a short NetBIOS name can cause problems.

### Configuring the S4U and constrained delegation

Before configuring the Service for User (S4U) and constrained delegation, ensure that you configure the service accounts with unconstrained delegation. The S4U configuration is a modification of the unconstrained delegation configuration and is therefore an optional task for you to perform.

See “Configuring service accounts with unconstrained delegation” on page 189.

**To configure S4U with constrained delegation**

1 Set up delegation on the Application Server account.

For AD users and computers, open the properties for the Application Server's service account and make the following changes on the Delegation tab:
Select Trust this user for delegation to specified services only
Select Use any authentication protocol
Under Services to which this account can provide delegated credentials

do the following:

■ Click Add and type in the name of the machine where DSS is installed.
  From the list of services, select the service, LDAP that has the same
  port number as the port where the ADAM instance is running and click
  OK.

■ Click Add and type the name of the service account for which the DSS
  service is running. You can view the custom SPN that was created for
  the DSS before installation.
  Select the service and click OK.

2 On the Application Server computer, open the Local Security Policy editor.
  Navigate to Under Local Policies > User Rights Assignment and grant the
  privilege, Act as part of the operating system to the Application Server.

3 Configure the Application Server in the following manner to use S4U
  authentication:

■ In the CCS Console, go to Settings > System Topology.

■ Select the Application Server component, and right-click on Edit Settings.

■ In the Edit Settings dialog box, select the Application Server > Basic
  option.

■ For the Authentication type option, select Use controlled delegation of
  security rights.

■ Click Save.

4 Reboot the Application Server computer so that the delegation settings can
  take effect.

About using special characters in credentials

Control Compliance Suite supports using specific special characters in the
credentials of the user accounts when you install the product components. Using
any unsupported special characters in the credential of the user account can cause
the component installation to fail.

The supported special characters are applicable to the Windows user accounts
for the following services:

■ Directory Support Service
Application server Service
Data Processing service (DPS) running in the reporter role

The supported special characters are applicable to the following databases:

- Production database
- Reporting database

The following special characters are supported in the user account user name:

- A-Z, a-z
- 0-9
- At sign (@)
- Hash (#)

The following special characters are supported in the user account password:

- A-Z, a-z
- 0-9
- At sign (@)
- Hash (#)
- Less-than (<)
- Greater-than (>)

See “Configuring the application server credentials” on page 189.

Updating Control Compliance Suite

Symantec releases system patches and updates for the Control Compliance Suite (CCS) components, which are downloaded using LiveUpdate. LiveUpdate is a core Symantec technology that is used to simplify maintenance and updates of Symantec software after deployment.

Symantec hosts an online database of all possible product updates. The LiveUpdate client contacts the Symantec LiveUpdate Server and submits a list of products that are currently installed on the LiveUpdate client. The LiveUpdate server returns a list of appropriate updates.

Various LiveUpdate client types are available, but Control Compliance Suite uses only the Windows LiveUpdate Client. In CCS, the LiveUpdate client is automatically installed on the computer on which the CCS Application Server component and the Data Processing Service are installed.
The LiveUpdate client also requires the LiveUpdate Administrator (LUA) for downloading the patches. You can install the LUA on any computer where Internet access is available, including a computer that runs the LiveUpdate client. The LUA is equipped with a distribution mechanism to distribute the updates to a distribution area. The LiveUpdate client is responsible for picking up the updates from the distribution area for the components that are installed on the LiveUpdate client computer. All computers that host a LiveUpdate client must be configured with a host file that points to the LUA distribution area.

See “About the host file for Windows LiveUpdate clients” on page 195.

The administrator needs to decide whether content or system updates are required for the installed components and to configure the LUA appropriately.

The following two types of updates are available for the CCS components:

- Content updates
- System patches and service pack updates

See “How LiveUpdate works in Control Compliance Suite” on page 193.

See “About the LiveUpdate view” on page 194.

How LiveUpdate works in Control Compliance Suite

Control Compliance Suite (CCS) uses Symantec LiveUpdate to get the latest product updates. Other distribution methods such as direct download from the Symantec Web site are available per Symantec policies.

Do the following to set up LiveUpdate:

- Configure a host file on the LUA.
  See “About the host file for Windows LiveUpdate clients” on page 195.

- Copy the host file to the LiveUpdate client computers.
  You must copy the client settings host file to the LiveUpdate installation folder on the client computer. By default, LiveUpdate is installed to C:\Program Files\Symantec\LiveUpdate.

- Enable and schedule LiveUpdate.
  See “Enabling and scheduling LiveUpdate” on page 194.

In CCS, LiveUpdate works in the following way:

- The LiveUpdate client detects new update and copies the package to the CCS LiveUpdate staging location on the LiveUpdate client.
  See “About the LiveUpdate staging location” on page 195.

- From the staging location, the CCS administrators must install the updates manually on each computer that hosts the LiveUpdate client.
Before you install updates, confirm that the staging progress is 100% complete in the System > LiveUpdate view.

Symantec recommends that you first install the updates on the Application Server. When the updates are installed, the Percent Deployed column in the System > LiveUpdate view shows 100%.

If the Directory Server is not installed on the same computer as the Application Server, the update status of the Directory Server is not calculated. A 100% does not include the Directory Server status.

See “About the LiveUpdate view” on page 194.

See “Updating Control Compliance Suite” on page 192.

About the LiveUpdate view

In the LiveUpdate view, you can view the status of the deployed version and the latest update of the component that is available for download. The view also displays the Readme file of the latest update.

The LiveUpdate view displays the following information for each update:

- Component name: The name of the installed component.
- Current Version: The version of the component that is currently deployed.
- Percent Deployed: The percentage of successful deployment of the target component in the Control Compliance Suite environment.
  
  A 100% would mean that the update is deployed successfully on all the computers that hosts the target component.
- Available Version: A newer version of the component that is available on the LiveUpdate client.
- Percent Staged: The percentage of successful downloads of the latest update package in all computers that host the target component.
- Detection Date: The date when the newer version is available for download.

See “How LiveUpdate works in Control Compliance Suite” on page 193.

See “Updating Control Compliance Suite” on page 192.

Enabling and scheduling LiveUpdate

You can enable LiveUpdate to run automatically at a scheduled time interval to ensure that Symantec CCS always has the most current updates. By default, when
LiveUpdate clients are installed on the CCS computers, the clients are not scheduled to run automatically. You must manually configure the schedule to run LiveUpdate on the CCS computers.

**To enable and configure LiveUpdate**

1. Run LuConfig.exe from `\Program Files\Symantec\LiveUpdate` folder.
2. In the LiveUpdate Configuration console, click **Automatic LiveUpdate** tab.
3. In the Automatic LiveUpdate box, check **Use Automatic LiveUpdate**.
4. In the Update Frequency box, type the number in hours or minutes to set the frequency that you want Automatic LiveUpdate to run.
   
   The default is every 240 minutes.

See “How LiveUpdate works in Control Compliance Suite” on page 193.

See “Updating Control Compliance Suite” on page 192.

See “Performing LiveUpdate on demand” on page 196.

### About the host file for Windows LiveUpdate clients

When a LiveUpdate client is installed, the client is configured to use a Symantec LiveUpdate server. You must generate a new client settings host file to redirect LiveUpdate clients to retrieve updates from a Distribution server. The host file must then be distributed to each client computer on the network. When the client computer runs LiveUpdate, LiveUpdate connects to the server that you designate in the host file and downloads the updates from that location.

In Control Compliance Suite (CCS), the LiveUpdate client is installed on the computer on which the Application Server and the Data Processing Service are installed.

You must copy the client settings host file to the LiveUpdate installation folder on the client computer. By default, LiveUpdate is installed to `C:\Program Files\Symantec\LiveUpdate`.

For information on how to generate a host file, refer to *Symantec LiveUpdate Administrator User’s Guide*.

See “How LiveUpdate works in Control Compliance Suite” on page 193.

See “Updating Control Compliance Suite” on page 192.

### About the LiveUpdate staging location

When LiveUpdate runs, it copies the latest update package to the staging location.
The staging location is user-definable. The location is specified by creating a text file with a single line of text that contains the fully qualified path to the staging location. The file is named LUStagingLocation.txt and should be located in the following directory: `<common_app_data>\Symantec\CCS`

If LUStagingLocation.txt does not exist, cannot be read, or is empty, LiveUpdate uses the default staging location, which is `<common_app_data>\Symantec\CCS\LiveUpdateStaging`.

See “How LiveUpdate works in Control Compliance Suite” on page 193.

See “Updating Control Compliance Suite” on page 192.

See “Performing LiveUpdate on demand” on page 196.

**Performing LiveUpdate on demand**

You can run LiveUpdate on demand to force an immediate update of a component or the content.

**To perform LiveUpdate on demand**

1. Run LuALL.exe from \Program Files\Symantec\LiveUpdate folder.
2. Follow the on-screen instructions to run LiveUpdate.

See “How LiveUpdate works in Control Compliance Suite” on page 193.

See “Updating Control Compliance Suite” on page 192.

**Configuring Response Assessment Module in Control Compliance Suite**

Control Compliance Suite (CCS) lets you connect to the Response Assessment Module (RAM) and assign the CCS assets to questionnaires to collect the evidence data.

Table 3-26 lists all the tasks that you must do to successfully view the evidence data from the questionnaires.

<table>
<thead>
<tr>
<th>Table 3-26</th>
<th>Collect data from RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Assign roles</td>
<td>Assign the Asset Viewer role to users answering the questionnaire about CCS assets. The role determines what you can see and perform in the CCS Console.</td>
</tr>
<tr>
<td></td>
<td>See “Adding users and groups to a role” on page 107.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Configure the evidence source for RAM</td>
<td>By default, RAM creates an evidence source, Symantec Response Assessment module provider in the <strong>Manage &gt; Extended Evidence Sources</strong> view of the console. You must create a data location for connecting to the RAM database. The RAM database can be connected using the ODBC connection details. You can edit the already added RAM evidence source to configure its data location. See “Editing an evidence source” on page 824.</td>
</tr>
<tr>
<td>Create asset groups</td>
<td>Create the asset groups to use in the questionnaires. Individual assets can be used but they must be part of an asset group for the Policy module to use. An asset group consists of assets of one or more types. The grouping is represented in a hierarchical fashion with nested subsets. You can create dynamic and static asset groups to organize the assets into logical groups. See “Creating a dynamic asset group” on page 370. See “Creating a static asset group” on page 372.</td>
</tr>
<tr>
<td>Enable the CCS connection</td>
<td>Enable the connection to the CCS application server to collect the evidence data. See “Adding a link to Control Compliance Suite” on page 201.</td>
</tr>
<tr>
<td>Create a questionnaire</td>
<td>Create a questionnaire or choose a questionnaire from the predefined content folders. Refer to the <em>Response Assessment module User Guide</em> for steps on how to create a questionnaire.</td>
</tr>
<tr>
<td>Add an asset group variable</td>
<td>Create a user-defined property and assign it to a CCS asset. See “Adding a Response Assessment Module user-defined property” on page 201.</td>
</tr>
<tr>
<td>Invite questionnaire users</td>
<td>Invite users to the new questionnaire and select the CCS asset to link to the questionnaire. See “Publishing a questionnaire with invitations in Response Assessment Module” on page 202.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create a policy</td>
<td>After the evidence data is in the database, create a policy for the questionnaire from the CCS console. Create a policy and link it to the same asset group that is linked to the questionnaire. The policy reports do not work if not linked to the same asset group. See “Creating a new policy” on page 693. See “Importing a Word policy” on page 695.</td>
</tr>
<tr>
<td>Map control statements</td>
<td>After the policy is created, map the control statements to the policy. The control statements are mapped to the frameworks and regulations that your enterprise must adhere to. The policy reports do not work if the policy and questions in the questionnaire are not linked to the same control statements. See “Mapping policies to control statements” on page 797.</td>
</tr>
<tr>
<td>Publish the policy</td>
<td>After the policy is mapped to the control statements, publish the policy for user acceptance. See “Publishing a policy” on page 704.</td>
</tr>
<tr>
<td>Run the evidence collection job</td>
<td>You can configure the existing evidence source for RAM as the evidence collection job. You can configure the evidence source as a job through the <strong>Create or Edit Evidence Source</strong> wizard. See “Running a job now” on page 719.</td>
</tr>
<tr>
<td>Synchronize the reporting database</td>
<td>After the policy is published, synchronize the reporting database to run reports. <strong>Note:</strong> Evidence from RAM is only imported if it exists in the Evidence table of the RAM database. See “Synchronizing the reporting database” on page 167. See “Running a job now” on page 719.</td>
</tr>
</tbody>
</table>
Table 3-26  
Collect data from RAM (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run reports</td>
<td>After data is synchronized, run the following reports to view the RAM data:</td>
</tr>
<tr>
<td></td>
<td>■ Policy Compliance by Asset</td>
</tr>
<tr>
<td></td>
<td>■ Policy Results by Control</td>
</tr>
<tr>
<td></td>
<td>■ Policy Control Statement Mappings</td>
</tr>
<tr>
<td></td>
<td>See “Scheduling a report” on page 746.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing a report” on page 747.</td>
</tr>
</tbody>
</table>

About Response Assessment Module

The Response Assessment Module (RAM) is a set of innovative components and services and is part of the Symantec Control Compliance Suite (CCS) strategy. RAM is an optional, external module for CCS. RAM formalizes, standardizes, and documents the assessments and audits that are a part of an organization. You can construct a complex business evaluation from prepackaged content packs. RAM lets you create questionnaires to answer your business challenges.

The following are your business challenges:

■ Complexity of regulatory compliance
■ Cost of regulatory compliance
■ Increased accountability from the shareholders, government, and industry
■ Increased civil and criminal liabilities for noncompliance

With the results gathered from the questionnaires, you can make informed decisions. Often, the results are used to gain an understanding of the beliefs and behaviors of a target population under a given set of circumstances. The results provide a snapshot, which reflects these beliefs and behaviors. In the past, to create an assessment was a complicated process that returned inconsistent results.

Previous approaches to assessments typically meant that each executive or manager would have their own Excel spreadsheet. The spreadsheets had no uniformity because they reflected each executive or manager's particular concerns. One assessment may conflict with other collected assessments. The assessment may not reflect an important concern. The members of upper management must spend the time to compile the assessments to gain an overall view of the organization. To create and store assessments can create technical problems.

The following are some of the assessment issues:

■ Not standardized
Not accessible from other applications
■ Difficult to manage
■ Difficult to store
■ Not secure

RAM extends the assessment strategy. Everyone sees the same questions. Executives and managers can provide uniform responses. The responses are compiled easily and the members of upper management can make more informed business decisions. RAM is a comprehensive assessment solution. When the RAM Server is installed, assessments are stored in an SQL Server database and are accessible from the Web. Invited users can create responses from any Web connection. With the necessary permissions, users can generate reports, export report detail information, and create the charts that visualize the information. RAM increases an organization’s ability to manage the flow of information.

RAM is a management tool that collects the following:

- Assessments: Current and new assessments
- Audits: Current and new audits
- Risk alignment: Supports a risk analysis process

Executives and managers can accomplish the following:
- Measure and evaluate their operations
- Distribute the questionnaires at regular intervals
- Improve their organization’s operations based on the results

Executives and managers can measure and evaluate the aspects of the following business processes:
- Compliance
- Business continuity
- Information security
- Physical security
- Governance
- Protection of intellectual property

A Response Assessment Module assessment is taken through the assessment lifecycle.

The following are the parts of the assessment lifecycle:
Questionnaire creation  The process that defines the questionnaire. The creation process may include questionnaire property definitions and the questionnaire layout.

Questionnaire delivery  The process to deliver the questionnaire to the intended attesters.

Response creation  The activities that focus on the response.

Report management  Responses can be grouped together, exported to an Excel spreadsheet, and used to create charts.

Questionnaire management  The activities that focus on the administration of an assessment.

See “Configuring Response Assessment Module in Control Compliance Suite” on page 196.

Adding a link to Control Compliance Suite

You can link the Response Assessment Module (RAM) to Control Compliance Suite (CCS). After you have linked the systems, you can assign the CCS assets to a RAM questionnaire and view RAM evidence in CCS. You must have the RAM Server installed and have a connection to it.

See “Configuring Response Assessment Module in Control Compliance Suite” on page 196.

To add a link to Control Compliance Suite

1. In Start > All Programs > Symantec Corporation, select Response Assessment module > Response Assessment module.
2. In the RAM Server toolbar in the RAM Console, click Settings.
3. In the Settings dialog box, check CCS present in the environment.
4. In Application Server box, provide the server name.
5. In the Port box, provide the number.
6. In the UPN box, provide a valid email address.

Adding a Response Assessment Module user-defined property

In the Response Assessment module (RAM), you can add a user-defined property to an object. You can populate a drop-down list that is displayed in the Web client or the Windows client. You can assign a default value. The default value is displayed at the top of the list. You can set the values to read-only.
User-defined properties are displayed in the RAM Invitation Manager and the RAM Response Wizard reports.

See “Configuring Response Assessment Module in Control Compliance Suite” on page 196.

To add a Response Assessment Module user-defined property

1. In the RAM Console, click Properties.
2. In the Selected Object’s Properties dialog box, in the User Defined Properties node, click Add.
3. In the Create New User Defined Property dialog box, type the name.
4. Click Add.
5. In the DropDown Definition box, type a value. Click OK.
6. Repeat steps 4 and 5, if necessary.
7. Click OK to add the property.

Publishing a questionnaire with invitations in Response Assessment Module

In the Response Assessment module (RAM), you can publish a questionnaire and invite users to respond. To create the invitations, you use the RAM Server toolbar in the RAM Console. You must have the RAM Server installed to use the RAM Server toolbar and Invitation Manager.

You should have the user names available. You can search for the email address in the RAM Server users dialog box.

When you create the invitations, you can also set the following options:

- Enable Expiration Date
- Enable Email Notifications
- Enable Quizzing
- Number of Questions Per Page

These options are not required.

If you select Enable Expiration Date option, you must provide an expiration date.

You should select Enable Email Notifications, if you want emailed invitations. You must have your mail server configured to send emails.

If you want to quiz your users and allow them to answer a questionnaire a specific number of times, select the Enable Quizzing option. You must also provide the minimum passing percentage and the number of extra chances. The minimum
passing percentage is the percentage of correct answers in the quiz. The number of extra chances is the number of times that a user can take the same quiz before it is automatically submitted.

You can change the number in the Number of Questions Per Page option. This option is the number of questions a user may see in one page of the RAM Web Client. The default number per page is 10. The number may be different if you have used the Next Hops tool. The Next Hops tool lets you design a different flow to the questionnaire. For example, a Next Hops question could be if the server room is always locked. If the user responds "Yes", then the user skips any questions about the server room being unlocked.

See “Configuring Response Assessment Module in Control Compliance Suite” on page 196.

To publish a questionnaire with invitations in RAM

1. In the RAM Console, in the RAM Server toolbar, click Publish.
2. In the Publish a Questionnaire to the RAM Server page, click Publish.
3. In the Success message, click OK.
4. In the Invite Users message, click Yes.
5. In the Create Questionnaire Invitations page, provide a title or accept the default.
6. Click Add Users.
7. In the RAM Server users dialog, select the users and click Add Selected Users.
8. Click Close to close the dialog.
9. Click Invite.
10. In the Invitations Created message, click OK.
11. In the Create Questionnaire Invitations page, click Close.

About configuring the Web Console to contact RAM

The Control Compliance Suite (CCS) Web Console works with the Response Assessment module (RAM) Web client. Several settings may be changed to enable connection with RAM.

The IIS CCS application pool uses the Network Server account as the identity. The account is a local account. The account may or may not connect to RAM. You should use the same account that is used as the identity in the RAM application pool.
The identity account has the following requirements:

- Member of the IIS_WPG local group
- Full permissions to the .NET directory
- Full permissions to the Windows\Temp directory

The Control Compliance Suite Web Console is installed with anonymous access setting for the CCS_Web site. You should change the setting to use Windows Integrated authentication. You should disable anonymous access.

In the web.config file for the Control Compliance Suite Web Console, you must set the SPN value. The format for the value should be

account@domain_name.com

Verify that the computer name is used in the following settings:

- AppServer
- RAMServer

If you use Control Compliance Suite assets with the RAM questionnaires, you must use Kerberos authentication.

### About logs and configuration files

The application adds a message to the log when an event occurs. The type of event that triggers a message is based on the level of severity setting. Logs may include event data from the servers. You view the log information to troubleshoot security problems in the network. You delete the events that are no longer needed.

You can use Notepad.exe or another text editor to read a log file or a configuration file.

The logs are found in the following locations:

<table>
<thead>
<tr>
<th>Table 3-27</th>
<th>Log location based on operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Location</td>
</tr>
<tr>
<td>Windows 2003 Server</td>
<td>%ALLUSERSPROFILE%\Application Data\Symantec.CSM\Logs</td>
</tr>
<tr>
<td>Windows 2008 Server</td>
<td>%ALLUSERSPROFILE%\Symantec.CSM\Logs</td>
</tr>
</tbody>
</table>
The logging system is configured on a per-application basis. You must edit the configuration file to change the settings. The configuration file is commonly known as an app.config file.

The Control Compliance Suite Console configuration information location is based on operating system.

The configuration files are found in the following locations:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Configuration name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 Server/XP</td>
<td>%USERPROFILE%\Local Settings\Apps\2.0[HASH][HASH]\syma..tion_[HASH]\SymConsole.exe.config</td>
</tr>
<tr>
<td>Windows 2008 Server/Vista</td>
<td>%USERPROFILE%\AppData\Local\Apps\2.0[HASH][HASH]\syma..tion_[HASH]\SymConsole.exe.config</td>
</tr>
</tbody>
</table>

The following lists the Control Compliance Suite components and the name of their app.config file:

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>&lt;installation directory&gt;\Application Server\Apps\ApplicationServer.exe.config</td>
</tr>
<tr>
<td>Data Processing Service</td>
<td>&lt;installation directory&gt;\DPS\Symantec.CSM.DPS.exe.config</td>
</tr>
<tr>
<td>Worker Process</td>
<td>&lt;installation directory&gt;\DPS\Blade.WorkerProcess.exe.config</td>
</tr>
<tr>
<td>Encryption Management Service</td>
<td>&lt;installation directory&gt;\EncryptionManagement Service\Symantec.CSM.EncryptionManagement.Service.exe.config</td>
</tr>
<tr>
<td>Certificate Management console</td>
<td>&lt;installation directory&gt;\Management Services\CertificateMgrConsole.exe.config</td>
</tr>
<tr>
<td>Directory Support Service</td>
<td>&lt;installation directory&gt;\Directory Support Service\Symantec.CSM.DSS.Service.exe.config</td>
</tr>
</tbody>
</table>

See “About log messages” on page 206.

See “About log levels” on page 206.
About log messages

The log messages conform to a standard logging format. The date and time are based on the UTC or the appropriate time zone information is attached. The category section is optional.

Each log message contains the following:

■ Date
■ Time
■ Category
■ Severity level
■ Identity of the logging computer
■ Message text
  Message text can be used to supply text or additional parameters to a log message.

See “About logs and configuration files” on page 204.

See “About log levels” on page 206.

About log levels

Control Compliance Suite has a hierarchical logging system. The system uses a standard set of levels that are used to capture the required information. You can control how much information is written to the log when you adjust the log level threshold. When you enable logging at a given level, you also enable logging at the lower levels.

The log levels are as follows:

Table 3-30 Log levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Levels captured in log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbose</td>
<td>The component operates properly. The level provides additional information.</td>
<td>This level is the highest level in the hierarchy.</td>
</tr>
<tr>
<td>Error</td>
<td>Operation cannot complete because of an error condition.</td>
<td>The error level logs all unhandled exceptions.</td>
</tr>
<tr>
<td>Warning</td>
<td>A recoverable error occurred.</td>
<td>A warning is often used for handled exceptions.</td>
</tr>
</tbody>
</table>
Table 3-30  Log levels (continued)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Levels captured in log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>The component operates correctly. The level provides general feedback.</td>
<td>The level is used to capture the information that is useful for system management.</td>
</tr>
<tr>
<td>None</td>
<td>No log information is stored.</td>
<td>No log is kept.</td>
</tr>
</tbody>
</table>

The following are the details that each levels writes to the log:

Table 3-31  Log level details

<table>
<thead>
<tr>
<th>Level</th>
<th>Verbose</th>
<th>Error</th>
<th>Warning</th>
<th>Informational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbose</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Error</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Informational</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

See “About logs and configuration files” on page 204.
See “About log messages” on page 206.
About logs and configuration files
Performing the IT governance tasks with Control Compliance Suite

This chapter includes the following topics:

- Preparing for risk assessment
- Assessing the compliance and the risk posture of the system
- Simplifying the remediation process
- Identifying possible threats in the access control system

Preparing for risk assessment

The organization of all the known assets into the system is a crucial step in the process of governance in IT. Control Compliance Suite lets you collect the data for the assets, manage and monitor the assets, and evaluate the assets against a set of standards. You can collect the asset data either from the data collection components in the system or from a CSV file. Control Compliance Suite lets you reconcile the collected asset data based on certain rules.

The Control Compliance Suite supports certain predefined platforms and predefined asset types. The Control Compliance Suite also provides the flexibility to create your own asset types and perform the risk assessment on the custom asset types.

See “Predefined platforms” on page 235.

See “Predefined asset types” on page 236.
You are ready for the risk assessment when you have imported all the known assets into the asset system. Before you begin the asset import, it is recommended that you review the basic concepts in the asset system.

See “Concepts in assets” on page 232.

### Table 4-1  Preparing for risk assessment

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Register Data Processing Service | Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register the DPS, you also assign the DPS to a site and specify the DPS roles.  
See “Registering the Data Processing Service” on page 115.  
See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338.  
Go to Settings > Map View > Register DPS. |
Table 4-1  Preparing for risk assessment (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure data collectors</td>
<td>Go to Settings &gt; Map View &gt; Right-click the site &gt; Edit settings. In the Data Processing Service dialog box, configure the following data collectors:</td>
</tr>
<tr>
<td></td>
<td>■ Navigate to <strong>Collector - General Settings</strong> tab. Configure at least one data collection component to collect the assets. You can configure the data collector for the platform for which you want to import the assets. For example: If you want to collect the data for the Windows platform, you must configure the Windows Information Server settings. See “Configuring the data collectors” on page 138.</td>
</tr>
<tr>
<td></td>
<td>■ Navigate to <strong>Collector settings by site</strong> and click <strong>CSV Settings</strong>. Select <strong>Common</strong> from the platform list. Configure the Common platform through CSV settings if you want to collect the data for the fields that are common for all the asset types. See “Configuring Common platform through CSV settings” on page 326.</td>
</tr>
</tbody>
</table>
Table 4-1  Preparing for risk assessment (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the reconciliation</td>
<td>Go to Manage &gt; Asset System &gt; Reconciliation Rules &gt; Create Rule.</td>
</tr>
<tr>
<td>rules</td>
<td>See “Asset reconciliation” on page 295. Perform one of the following tasks to use the reconciliation rules:</td>
</tr>
<tr>
<td></td>
<td>■ Use the predefined reconciliation rules to add the assets into the asset system for the first time.</td>
</tr>
<tr>
<td></td>
<td>However, the predefined reconciliation rules add all the imported assets into the default folder, Asset System.</td>
</tr>
<tr>
<td></td>
<td>See “Predefined reconciliation rules” on page 284.</td>
</tr>
<tr>
<td></td>
<td>■ Create your own reconciliation rules to organize the assets into the asset system in a specific folder hierarchy.</td>
</tr>
<tr>
<td></td>
<td>See “Creating reconciliation rules without manual review” on page 306.</td>
</tr>
<tr>
<td></td>
<td>See “Reconciliation rules and rule types” on page 276.</td>
</tr>
</tbody>
</table>
Table 4-1  Preparing for risk assessment (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import the assets</td>
<td>Go to Manage &gt; Assets &gt; Asset System &gt; Asset Tasks &gt; Import Assets. Perform the following tasks to import the assets into the asset system:</td>
</tr>
<tr>
<td></td>
<td>■ Identify the primary assets of the asset type that you want to import. See “Primary and secondary assets” on page 275.</td>
</tr>
<tr>
<td></td>
<td>■ Import the primary assets either with the predefined reconciliation rules or with the custom reconciliation rules. See “Importing the assets for the first time” on page 319.</td>
</tr>
<tr>
<td></td>
<td>■ Import the secondary assets either from the default data collector or from the CSV data collector. See “Importing asset-specific fields from the default data collector” on page 329.</td>
</tr>
<tr>
<td></td>
<td>See “Importing asset-specific and common fields using the default data collector” on page 332.</td>
</tr>
<tr>
<td></td>
<td>See “Importing asset-specific and common fields using the CSV data collector” on page 335.</td>
</tr>
<tr>
<td></td>
<td>See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338.</td>
</tr>
</tbody>
</table>
Table 4-1 Preparing for risk assessment (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create asset groups         | Go to Manage > Assets > Asset System > Asset Group Tasks > Create Asset Group. Perform the following tasks with the asset groups:  
  ■ Create static and dynamic asset groups to create asset clusters on the basis of a common logical criteria. See “Creating a static asset group” on page 372. See “Creating a dynamic asset group” on page 370.  
  ■ Use the predefined dynamic asset groups. Copy a relevant predefined asset group to the folder in which you want to create an asset cluster. See “Predefined asset groups” on page 297. |

See “Assessing the compliance and the risk posture of the system” on page 214.

Assessing the compliance and the risk posture of the system

The assessment of the compliance and the risk posture of the system begins when you import all the known assets into the system. Control Compliance Suite lets you proactively assess the assets against a set of standards. The assessment is done based on the data that is collected from the data collection components of the Control Compliance Suite. This comparison of the computer settings to predefined Standards is called an evaluation.

Before you begin the evaluation of the imported assets against the Standards, it is recommended that you review the basic concepts in Standards.

See “Concepts in standards management” on page 549.
Table 4-2  Compliance and risk posture assessment

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Understand and identify the predefined standard for assessment | Go to Manage > Standards. Consider the following to understand the predefined standards:  
  ▪ Browse through the predefined standards in the tree pane under the Standards node.  
  ▪ Identify the predefined standard that you want to use for assessment of the imported assets.  
    See “About standards” on page 550.                                                                 |
| Collecting data for evaluation                  | Go to Manage > Assets > Asset System > Global Tasks. Consider the following when you collect the data for evaluation:  
  ▪ Select the asset type or the asset group for which you want to collect the data for evaluation and select Setup Data Collection.  
    See “Setting up a data collection job from the Assets view” on page 380. |
### Table 4-2  Compliance and risk posture assessment (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Evaluating the assets against the standards | Go to Manage > Assets > Asset System > Global Tasks.  
Consider the following to evaluate the assets against the standards:  
- Create an evaluation job to evaluate the assets for which data is collected.  
The information that you specify during the evaluation process is saved in the evaluation job. Hence, an evaluation job lets you perform the evaluation process repeatedly without having to specify the evaluation criteria again. Evaluation jobs can be scheduled to run at predefined intervals.  
See “Running an evaluation job from the Asset System view” on page 383. |
| Viewing the evaluation results      | Go to Manage > Assets > Asset System.  
Consider the following to view the evaluation results:  
- View the details of the assets that are evaluated against a standard in the Details pane.  
The details pane presents the following information about the evaluation:  
  - Standard against which the evaluation job was run  
  - Evaluation date  
  - Checks evaluated  
  - Checks not evaluated  
  - Compliance score  
  - Risk score  
See “Running an evaluation job from the Asset System view” on page 383.  
See “Viewing the evaluation results in the details pane” on page 400. |
**Table 4-2** Compliance and risk posture assessment *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Generate reports based on evaluation | Go to Reporting > Report Templates  
Consider the following while generating the compliance reports  
- Generate reports that provide a summary of the compliance of assets against the required standards.  
  See “Predefined report descriptions” on page 741.  
  See “Working with reports” on page 745. |
| Create dashboard reports for the evaluated data | Go to Reporting > My Dashboards  
You can do the following to create and generate dashboard reports:  
- Create a tiered dashboard through the Create Tiered Dashboards wizard.  
  See “Creating a tiered dashboard” on page 763.  
- Add a Standards Evaluation Results node to the dashboard.  
  See “Adding an evaluation node” on page 777.  
  Select the asset and the appropriate standard to assess and create the scope for the evaluation node.  
- Schedule the tiered dashboard update job through the Create Tiered Dashboards wizard.  
- View the dashboard details and trends report in the report viewer.  
  See “Viewing the tiered dashboard reports” on page 784. |

See “Simplifying the remediation process” on page 218.
Simplifying the remediation process

After you evaluate the assets against standards, you get the evaluation results and the risk score. You can now identify the assets in the organization that are compliant with the set guidelines. Control Compliance Suite lets you create baselines based on the evaluation results. The baselines make it easier to compare the assets.

Table 4-3  Remediation process

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create baseline</td>
<td>Go to Monitor &gt; Jobs. Create a baseline job. You can mark an asset as a baseline for other assets. Or you can mark the result of an entire job run as a baseline for further jobs. See “Creating a baseline job” on page 672.</td>
</tr>
<tr>
<td>View comparison results</td>
<td>Go to Manage &gt; Baselines. View comparison results for an asset against the baselined asset. See “Viewing the comparison results in the Baselines view” on page 673.</td>
</tr>
<tr>
<td>Create remediation reports</td>
<td>Go to Reporting &gt; Report Templates. Select and schedule the Remediation Report to execute at a specific time interval. The remediation report lets you view the remediation information and the detailed evidence of failed checks for one or more asset groups or asset folders. See “Scheduling a report” on page 746.</td>
</tr>
</tbody>
</table>
Identifying possible threats in the access control system

In a typical environment, IT compliance is confined to configuration management, the firewall, the antivirus systems, and the vulnerability assessment. However, there is a difference between managing security configurations and vulnerabilities and managing access controls and data entitlements. Incidents can occur when a valid user can have access to the data that the user should not access.

Control Compliance Suite facilitates the monitoring of access rights in the organization. The Control Compliance Suite identifies false entitlements. The Entitlements view in the Control Compliance Suite lets you define the data a user is entitled to access. The Entitlements view also monitors whether the system adheres to the defined access controls.

Before you begin to monitor the entitlements of the control points, it is recommended that you review the basic concepts in entitlements management.

See “Concepts in entitlements” on page 496.
Table 4-4 Identifying threats in access control

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Locating the potential control points in the asset system | Go to Manage > Assets > Asset system. Consider the following to locate the potential control points in the asset system:  
  ■ Control points are the data locations in the system at which the access permissions are granted and approved. Locate the type of assets that should be marked as control points. You can decide the potential control points based on the Confidentiality, Integrity, and Availability values of the assets or any other criteria.  
  For example:  
  You might want to frequently review the permissions granted to the assets that belong to the Finance department. In this case, consider the creation of a tag, Finance for a set of assets so that you can easily locate the potential control points.  
  ■ You cannot mark the Windows machines and the UNIX Machines assets as control points.  
  See “Control points” on page 497. |
| Mark the assets as control points         | Go to Manage > Assets > Asset System > Global Tasks > Mark as Control Point. Consider the following to mark the assets as control points:  
  ■ After you locate the assets as potential control points, you can mark the assets as control points.  
  ■ After you mark the assets as control points, they are available for monitoring of entitlements in the Manage > Entitlements view.  
  See “Marking an asset as a control point” on page 378. |
### Table 4-4 Identifying threats in access control (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create Review Cycle Setting   | Go to Manage > Entitlements > Review Cycle Settings.  
Consider the following to create a review cycle setting:  
■ You must have the Entitlements Administrator role to create a review cycle setting.  
See “Predefined roles” on page 97.  
■ Create a review cycle setting to monitor the control points over a specific time period.  
See “Review cycle setting” on page 498.  
■ You can create a Recurring or a Non-recurring review cycle.  
See “Creating a review cycle setting” on page 503. |
| Configure the control point   | Go to Manage > Entitlements > Control Points.  
Consider the following to configure the control points:  
■ You must have the Entitlements Administrator role to configure control points.  
See “Predefined roles” on page 97.  
■ You configure the control point to associate a data owner and a review cycle to the control point.  
See “Configuring control points” on page 501. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Monitor the control point status throughout the review cycle | Go to Manage > Entitlements > Control Points  
Before you begin monitoring the control points in the review cycle, it is recommended that you understand the various control point states.  
See “About the control point status” on page 489.  
Perform the following tasks in the given order as an Entitlements Administrator:  
- Import the entitlements of the control point whenever the control point is in the Entitlement Import Required state.  
  See “Importing the entitlements manually” on page 511.  
  See “Configuring the automatic entitlements import” on page 510.  
- Send an approval request to the data owner  
The control points are then approved by the data owners or the data owners request changes in the control point entitlements.  
To know more about the entire approval workflow visit the following link:  
See “About the entitlements system workflow” on page 485. |
### Table 4-4  Identifying threats in access control (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Generate entitlements report| Go to Reporting > Report Templates  
You can generate the following types of entitlements reports:  
- Entitlement changes report  
- Trustee report  
- Effective permissions report  
- Simple permissions report  
See “Predefined report descriptions” on page 741. |
Performing the IT governance tasks with Control Compliance Suite

Identifying possible threats in the access control system
Getting started with the asset system

To define the known assets that need protection is the first step in the IT process governance. The primary goal of the asset management system is to present a consolidated view of the assets that are present in the organization. The asset system lets you manage the assets in the organization. The system also lets you exchange the context-specific information about the assets so that you can look at your organization from different perspectives. You can use the asset system to manage and monitor the assets that are valuable to your organization.

To understand how the asset system works, review the concepts that you must understand before you begin to use the asset system.

See “Concepts in assets” on page 232.
### Table 5-1  Primary tasks to get started with asset system

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Registering the Data Processing Service        | Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register the DPS, you also assign the DPS to a site and specify the DPS roles. Where appropriate, specify data types to collect.  
  See “Registering the Data Processing Service” on page 115. |
| Configuring the data collectors                | You must configure the data collector for the platform for which you want to import the assets.                                                                                                             |
| Configure Common platform to import common fields | In Control Compliance Suite, the data for the common fields of an asset type is not collected from the default data collector.  
  See “About the working of default data collectors in asset import” on page 322.  
  To collect data for the common fields, you must manually create a CSV file and define all the common fields in a specific format.  
  See “Creating a CSV file for custom application” on page 357.  
  If you do not have the Common platform configured, the assets are still imported into the asset system without the common fields data.  
  See “Configuring Common platform through CSV settings” on page 326. |

The asset system workflow starts with the creation of reconciliation rules. The asset system workflow ends with the evaluation results of the assets that are a part of the asset system. Asset import is the most crucial step in the asset system. You must have reconciliation rules, tags, and the asset groups before you import the assets.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import the primary assets for the first time with the predefined</td>
<td>The day zero asset import is the most important step to get started with the asset system. The asset system facilitates the process of the day</td>
</tr>
<tr>
<td>reconciliation rules</td>
<td>zero asset import with predefined rules. The day zero asset import implies the import of primary assets into the asset system.</td>
</tr>
<tr>
<td></td>
<td>See “Primary and secondary assets” on page 275.</td>
</tr>
<tr>
<td></td>
<td>See “About the first time asset import” on page 316.</td>
</tr>
<tr>
<td></td>
<td>See “Importing the assets for the first time” on page 319.</td>
</tr>
<tr>
<td>Create reconciliation rules for further asset imports</td>
<td>If you have imported assets without the common fields data, you can set the values of the common fields with the reconciliation rules.</td>
</tr>
<tr>
<td></td>
<td>See “Using a Pre rule to set the values of the common fields” on page 309.</td>
</tr>
<tr>
<td></td>
<td>See “Creating reconciliation rules” on page 306.</td>
</tr>
<tr>
<td>Apply tags to the assets</td>
<td>You can now create tags to assign to the assets. You can create tags on the basis of Department, Confidentiality, Location, and so on.</td>
</tr>
<tr>
<td></td>
<td>See “Asset tagging” on page 296.</td>
</tr>
<tr>
<td></td>
<td>See “Applying a tag to the asset” on page 392.</td>
</tr>
<tr>
<td>Create asset groups</td>
<td>After you create the tags, you can group the assets on the basis of the tags or any other logical grouping.</td>
</tr>
<tr>
<td></td>
<td>You can create static and dynamic asset groups or use the predefined asset groups.</td>
</tr>
<tr>
<td></td>
<td>See “Creating asset groups” on page 369.</td>
</tr>
</tbody>
</table>
### About the Asset System view

The Asset System view lets you manage the assets in the Control Compliance Suite.

You can access the Asset System view from Manage > Assets > Asset System.

The Asset System view contains the following panes:

- **Tree pane**: This pane appears on the left side of the console window under the navigation bar. This pane displays the assets under the Asset System node. Under the Asset System node, you can view the Asset Group Templates that contain the predefined asset groups.
  
  See “Creating the asset folders” on page 375.

- **Filter by pane**: This pane appears in the lower left side of the console window under the tree pane. You can use the following filters in the asset management view:
  - Select tags
  - Risk Ratings
  - Created Between
  - Modified Between

  See “Using the Filter by pane in the Asset System view” on page 402.

- **Taskbar**: The taskbar appears across the top of the tree pane and the table pane in the console window.

  See “Performing the tasks in the Asset System view” on page 375.

---

**Table 5-2  Asset system tasks (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import the secondary assets</td>
<td>After you import the primary assets, you can now proceed with the further asset imports with the reconciliation rules and asset groups. See “Working with asset import scenarios” on page 321.</td>
</tr>
<tr>
<td>Table pane</td>
<td>The table pane appears in the right side of the console window under the taskbar. This pane displays the assets and the asset groups. On the top right corner of the table pane, the active assets are displayed. See “Active assets” on page 306.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Details pane</td>
<td>The details pane appears in the lower-right side of the console window under the table pane. This pane displays the details of the asset or the asset group that is selected in the tables pane. See “Viewing asset information in the details pane” on page 394.</td>
</tr>
</tbody>
</table>

The taskbar of the Asset System view is divided into the following major tasks:

<table>
<thead>
<tr>
<th>Asset Group Tasks</th>
<th>You can perform the following asset group tasks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Create Asset Group</td>
<td>See “Creating a dynamic asset group” on page 370. See “Creating a static asset group” on page 372.</td>
</tr>
<tr>
<td>■ Edit Asset Group</td>
<td>See “Editing an asset group” on page 376.</td>
</tr>
<tr>
<td>■ Copy Asset Group</td>
<td>See “Copying and pasting an asset group” on page 377.</td>
</tr>
<tr>
<td>■ Paste Asset Group</td>
<td>See “Copying and pasting an asset group” on page 377.</td>
</tr>
<tr>
<td>■ Rename Asset Group</td>
<td>See “Renaming an asset group” on page 377.</td>
</tr>
</tbody>
</table>
### Global Tasks

You can perform the following global tasks:

- **Mark as Control Point**
  
  See “Marking an asset as a control point” on page 378.

- **Request Exception**
  
  See “Requesting an exception” on page 538.

- **Set up Data Collection**
  
  See “Setting up a data collection job from the Assets view” on page 380.

- **Run Evaluation**
  
  See “Running an evaluation job from the Asset System view” on page 383.

- **Run Collection-Evaluation-Reporting**
  
  See “Running a collection-evaluation-reporting job from the Asset System view” on page 385.

### Asset Tasks

You can perform the following asset tasks:

- **Import Assets**
  
  See “Working with asset import scenarios” on page 321.

- **Edit Assets**
  
  See “Editing assets” on page 391.

- **Move Assets**
  
  See “Moving an asset” on page 392.

- **Export CSV Headers**
  
  See “Exporting CSV headers” on page 393.

### Common Tasks

You can perform the following common tasks:

- **Delete**
  
  See “Deleting assets or asset groups” on page 393.

- **View permissions**
  
  See “Viewing permissions on the asset folders and asset groups” on page 394.

---

### About the Reconciliation Rules view

The Reconciliation Rules view lets you manage the rules in the Control Compliance Suite.

You can access the Reconciliation Rules view from Manage > Assets > Reconciliation Rules.
Tree pane
This pane appears on the left side of the console window under the navigation bar.
This pane displays the reconciliation rules under the Reconciliation Rules node. Under the Reconciliation Rules node, you can view the predefined Rules.

Filter by pane
This pane appears in the lower left side of the console window under the tree pane.
You can use the following filters in the rules management view:
■ Asset Type
■ Rule Type

Taskbar
The taskbar appears across the top of the tree pane and the table pane in the console window.
See “Performing the tasks in the Reconciliation Rules view” on page 404.

Table pane
The table pane appears in the right side of the console window under the taskbar.
This pane displays the rule types and the rules.

Details pane
The details pane appears in the lower-right side of the console window under the table pane.
This pane displays the details of the rule that is selected in the tables pane.

The rules management view lets you perform the following tasks:

■ Create Rule
See “Creating reconciliation rules using the manual review” on page 307.
See “Creating reconciliation rules without manual review” on page 306.

■ Moving Rule
See “Moving a reconciliation rule” on page 405.

■ Editing Rule
See “Editing a reconciliation rule” on page 405.

- Copy Rule
  See “Copying and pasting a reconciliation rule” on page 406.

- Paste Rule
  See “Copying and pasting a reconciliation rule” on page 406.

- Delete Rule
  See “Deleting a reconciliation rule” on page 406.

- Mark as Default Rule
  See “Marking a rule as default” on page 406.

- Unmark as Default Rule
  See “Unmarking a rule as default” on page 407.

## Concepts in assets

To understand the workflow of managing the assets in Control Compliance Suite, you need to understand some of the concepts in the assets.

The following are the concepts of the assets:

- About assets
  See “About assets” on page 233.

- Site
  See “Site as scope in asset import” on page 234.

- Asset folder hierarchy
  See “Asset folder hierarchy” on page 234.

- Predefined platforms
  See “Predefined platforms” on page 235.

- Asset types
  See “Asset types” on page 235.

- Primary and secondary assets
  See “Primary and secondary assets” on page 275.

- Reconciliation rules
  See “Reconciliation rules and rule types” on page 276.

- Asset tagging
  See “Asset tagging” on page 296.

- Asset import
  See “Asset import” on page 288.
About assets

With reference to Control Compliance Suite, an asset is defined as an object in the organization that has certain properties.

### Table 5-3 Features of assets

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>An object must have a value in the organization to become an asset. Without a value, the object is a liability.</td>
</tr>
<tr>
<td>Owner</td>
<td>The owner of the asset carries the responsibility to secure and maintain the value of the asset.</td>
</tr>
<tr>
<td>Restricted access</td>
<td>An asset must also have limited access to safeguard its value. Because an asset has value, some benefit can be derived from its use. Any unlimited access that is granted to assets implies zero value.</td>
</tr>
</tbody>
</table>

In a broader perspective, assets fall into the following major non-technical groups:

- **People assets**
  - Human capital

- **Information assets**
  - Financial data
  - HR data
  - Patent records
  - Business plans
  - Disaster recovery plans

- **Physical assets**
  - Furniture
  - Office campus

Control Compliance Suite deals with the technology assets.

Technology assets are important because of the following reasons:

- Technology assets store information.
Technology assets have role-based access control. People are granted various levels of authority over these assets.

Technology assets often control other physical systems.

Primitive technology assets include User accounts, Computers, Printers, Network Infrastructure, and Services. Control Compliance Suite collects data on these primitive assets.

See “Site as scope in asset import” on page 234.
See “Asset folder hierarchy” on page 234.

Site as scope in asset import

In the asset system, the sites are used as scopes to limit the number of assets to be imported into the asset system. A site is a default scope for asset import for the first time. When you import the assets for the first time, you must select the Site to which the Data Processing Server is associated, as a scope. The asset import job collects the assets from the configured sites.

See “Configuring sites” on page 134.

Asset folder hierarchy

When you install Control Compliance Suite, a default hierarchy structure is created to store objects in the CCS directory. All objects are stored under the root folder. The root folder holds subfolders for each object type. With the individual object type folder, you can create a hierarchical structure that best suits your organizational needs to store objects.

In case of the asset system, the objects that are stored in the CCS directory include the assets and the reconciliation rules.

After installation, the following hierarchical structure is created for storing the assets:

- Asset System
  - Asset Group templates

After installation, the following hierarchical structure is created for storing the reconciliation rules:

- Reconciliation Rules
  - Predefined Reconciliation Rules

See “About organizing objects in the directory” on page 36.
Predefined platforms

Control Compliance Suite lets you collect the asset data in the form of categories that are specific to the predefined platforms.

Control Compliance Suite supports the data collection, analysis, and reporting on the following platforms:
- Enterprise Security Manager
- Oracle
- SQL
- UNIX
- Windows
- Exchange
- NDS
- NetWare

Each predefined platform has certain primary entities. Control Compliance Suite by default supports some of the primary entities of the predefined platforms as asset types. In addition to the primary entities that the predefined platforms support as asset types, you can create your own asset types with other primary entities.

The predefined platforms are not extensible.

See “About platforms” on page 456.
See “About entities” on page 457.
See “Predefined asset types” on page 236.
See “Probable asset types” on page 273.

Asset types

An asset type is an entity of the platform that the asset system supports for the asset import. For example, all directories of the Windows platform can constitute to be the assets. You can categorize the assets into a single category of an asset type called Windows directory.

By default, the asset system supports certain entities of the predefined platforms as asset types. You can perform the asset import operation with the predefined asset types without any customization.

See “Predefined asset types” on page 236.
The asset system does not support certain entities of the predefined platforms by default. But, the asset system makes these entities available for customization to create custom asset types. Probable asset types are created from the entities that the Control Compliance Suite does not support by default as asset types.

See “Probable asset types” on page 273.

The asset system lets you create an entirely new platform and define the entity that the new platform supports. You can use these newly created entity and create a new asset type that is based on the custom entity. The asset types that are created from the custom platform and custom entities are custom asset types.

See “Custom asset types” on page 274.

**Predefined asset types**

Control Compliance Suite lets you collect the asset data in the form of categories that are specific to the supported platforms. Control Compliance Suite supports the data collection, analysis, and reporting on the ESM, Windows, UNIX, Oracle, and SQL platforms.

To gather more specific data for the purpose of monitoring, Control Compliance Suite lets you select the asset types that belong to the supported platforms.

Predefined asset types are based on the entities of the predefined platforms.

See “Predefined platforms” on page 235.

In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong.

See “About platforms” on page 456.

A group of fields that define the common functions of the network element form an entity.

See “About entities” on page 457.

Each asset type has some specific primary, mandatory, and optional fields.

The predefined asset types that are associated with the predefined platforms are as follows:

<table>
<thead>
<tr>
<th>Table 5-4</th>
<th>Predefined asset types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform</strong></td>
<td><strong>Predefined asset type</strong></td>
</tr>
<tr>
<td>Enterprise Security Manager Platform</td>
<td>■ ESM Agent</td>
</tr>
<tr>
<td></td>
<td>See “Fields for ESM Agent” on page 238.</td>
</tr>
<tr>
<td>Platform</td>
<td>Predefined asset type</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exchange</td>
<td>■ Administrative Groups MS-Exchange</td>
</tr>
<tr>
<td></td>
<td>See &quot;Fields for Administrative Groups MS-Exchange&quot; on page 266.</td>
</tr>
<tr>
<td></td>
<td>■ Exchange Server</td>
</tr>
<tr>
<td></td>
<td>See &quot;Fields for Exchange Server&quot; on page 267.</td>
</tr>
<tr>
<td></td>
<td>■ Organization MS-Exchange</td>
</tr>
<tr>
<td></td>
<td>See &quot;Fields for Organization MS-Exchange&quot; on page 269.</td>
</tr>
<tr>
<td>NDS</td>
<td>■ NDS Tree</td>
</tr>
<tr>
<td></td>
<td>See “Fields for NDS Tree” on page 240.</td>
</tr>
<tr>
<td>NetWare</td>
<td>■ NetWare Server</td>
</tr>
<tr>
<td></td>
<td>See “Fields for NetWare File Server” on page 240.</td>
</tr>
<tr>
<td>Oracle Platform</td>
<td>■ Oracle Configured Databases</td>
</tr>
<tr>
<td></td>
<td>See “Fields for Oracle Configured Databases” on page 241.</td>
</tr>
<tr>
<td></td>
<td>■ Oracle Configured Servers</td>
</tr>
<tr>
<td></td>
<td>See “Fields for Oracle Configured Servers” on page 242.</td>
</tr>
<tr>
<td>SQL Platform</td>
<td>■ SQL Database</td>
</tr>
<tr>
<td></td>
<td>See “Fields for SQL Databases” on page 243.</td>
</tr>
<tr>
<td></td>
<td>■ SQL Server</td>
</tr>
<tr>
<td></td>
<td>See “Fields for SQL Server” on page 245.</td>
</tr>
<tr>
<td>UNIX Platform</td>
<td>■ UNIX File</td>
</tr>
<tr>
<td></td>
<td>See “Fields for UNIX File” on page 246.</td>
</tr>
<tr>
<td></td>
<td>■ UNIX Group</td>
</tr>
<tr>
<td></td>
<td>See “Fields for UNIX Group” on page 247.</td>
</tr>
<tr>
<td></td>
<td>■ UNIX Machine</td>
</tr>
<tr>
<td></td>
<td>See “Fields for UNIX Machine” on page 248.</td>
</tr>
</tbody>
</table>
Table 5-4  Predefined asset types (continued)

<table>
<thead>
<tr>
<th>Platform</th>
<th>Predefined asset type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Platform</td>
<td>■ IIS Virtual Directory</td>
</tr>
<tr>
<td></td>
<td>See “Fields for IIS Virtual Directory” on page 269.</td>
</tr>
<tr>
<td></td>
<td>■ IIS Web Site</td>
</tr>
<tr>
<td></td>
<td>See “Fields for IIS Web Site” on page 272.</td>
</tr>
<tr>
<td></td>
<td>■ Windows Directory</td>
</tr>
<tr>
<td></td>
<td>■ Windows Domain</td>
</tr>
<tr>
<td></td>
<td>See “Fields for Windows Domain” on page 249.</td>
</tr>
<tr>
<td></td>
<td>■ Windows File</td>
</tr>
<tr>
<td></td>
<td>See “Fields for Windows File” on page 264.</td>
</tr>
<tr>
<td></td>
<td>■ Windows Group</td>
</tr>
<tr>
<td></td>
<td>See “Fields for Windows Group” on page 254.</td>
</tr>
<tr>
<td></td>
<td>■ Windows Machine</td>
</tr>
<tr>
<td></td>
<td>See “Fields for Windows Machine” on page 256.</td>
</tr>
<tr>
<td></td>
<td>■ Windows Share</td>
</tr>
<tr>
<td></td>
<td>See “Fields for Windows Share” on page 262.</td>
</tr>
</tbody>
</table>

See “Probable asset types” on page 273.
See “Custom asset types” on page 274.

**Fields for ESM Agent**

The Control Compliance Suite lets you create your own asset type schema and extend the existing asset type schema to manage your assets.

**Table 5-5** lists the primary, mandatory, and optional fields for the ESM agents asset type.

**Table 5-5  Fields for ESM Agent**

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Is single valued?</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Name</td>
<td>The name that is used to register agent with ESM manager</td>
<td>String</td>
<td>True</td>
<td>Primary</td>
</tr>
<tr>
<td>OS details</td>
<td>Operating system details</td>
<td>String</td>
<td>True</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
### Table 5-5 Fields for ESM Agent (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Is single valued?</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Version</td>
<td>Operating system version</td>
<td>String</td>
<td>True</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Platform</td>
<td>Operating system platform</td>
<td>String</td>
<td>True</td>
<td>Mandatory</td>
</tr>
<tr>
<td>ESM Manager</td>
<td>Associated ESM Manager</td>
<td>String</td>
<td>True</td>
<td>Mandatory</td>
</tr>
<tr>
<td>ESM SU Version</td>
<td>Security Update version on the ESM agent</td>
<td>String</td>
<td>True</td>
<td>Optional</td>
</tr>
<tr>
<td>ESM Domains</td>
<td>The ESM domains to which the agent belongs</td>
<td>String</td>
<td>False</td>
<td>Optional</td>
</tr>
<tr>
<td>ESM version</td>
<td>ESM version that is installed on the agent</td>
<td>String</td>
<td>True</td>
<td>Optional</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name of the ESM agent</td>
<td>String</td>
<td>True</td>
<td>Optional</td>
</tr>
<tr>
<td>Host Name</td>
<td>Agent's NETBIOS or Host name</td>
<td>String</td>
<td>True</td>
<td>Optional</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address of the ESM agent computer</td>
<td>String</td>
<td>False</td>
<td>Optional</td>
</tr>
</tbody>
</table>
## Fields for NDS Tree

**Table 5-6**  
Fields for NDS Tree

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Data type</th>
<th>Single valued or multi-valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree name</td>
<td>This field contains the name of the NDS tree.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>

## Fields for NetWare File Server

**Table 5-7**  
Fields for NetWare File Server

<table>
<thead>
<tr>
<th>Display name (DN)</th>
<th>Description</th>
<th>Data type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>This field contains the Distinguished Name of the report object. The DN is the unique name of the object including all the folders up to the root folder.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Tree name</td>
<td>This field contains the name of the NDS tree.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
# Fields for Oracle Configured Databases

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the domain or the workgroup name of the computer that hosts the Oracle Server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Server Name (Instance)</td>
<td>This field returns the name of the Oracle Server instance, not the name of the host.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Host Name (Node)</td>
<td>This field returns the name of the Windows NT server that hosts the instance of Oracle Server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Database Name</td>
<td>This field returns the name of the database.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Windows Domain Name or Unix IP Address</td>
<td>This field reports Domain Name for the Windows server and IP Address for a Unix server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Server Name</td>
<td>This field reports the name of the Oracle server</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Table 5-8  Oracle Configured Databases (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server NetBIOS Name</td>
<td>This field reports the NetBIOS name of the Oracle server</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>OS Type</td>
<td>This field reports the Operating System type of the Oracle server.</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>List of IP network addresses of the Oracle server</td>
<td>String</td>
<td>Multi-valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Database Version</td>
<td>This field reports on the database version</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used by the listener service for the configured database.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Fields for Oracle Configured Servers

### Table 5-9  Fields for Oracle Configured Servers

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>This field reports the name of the Oracle server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Table 5-9  Fields for Oracle Configured Servers (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server NetBIOS Name</td>
<td>This field reports the NetBIOS name of the Oracle server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Windows Domain Name or UNIX IP Address</td>
<td>This field reports Domain Name for Windows server and IP Address for a UNIX Server</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>OS Type</td>
<td>This field reports the Operating System type of the Oracle server</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

### Fields for SQL Databases

### Table 5-10  Fields for SQL Database

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the domain or the workgroup name of the computer that hosts the SQL Server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Server Name (Instance)</td>
<td>This field returns the name of the SQL Server instance, not the name of the host.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Table 5-10  Fields for SQL Database (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (Node)</td>
<td>This field returns the name of the Windows NT server that hosts the instance of SQL Server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Database Name</td>
<td>This field returns the name of the database.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Owner</td>
<td>The owner of the SQL server element.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Host name (DNS)</td>
<td>The name of the Windows NT server that hosts the SQL server database.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>This field returns all the TCP/IP addresses that are configured for the computer that contains the database.</td>
<td>String</td>
<td>Multi valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Fields for SQL Server

**Table 5-11** Fields for SQL Server

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the domain or the workgroup name of the computer that hosts the SQL Server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Server Name (Instance)</td>
<td>This field returns the name of the SQL Server instance, not the name of the host.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Host Name (Node)</td>
<td>This field returns the name of the Windows NT server that hosts the instance of SQL Server.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Major Version</td>
<td>The major version of the SQL server instance.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Minor Version</td>
<td>The minor version of the SQL server instance.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Login Mode</td>
<td>The default login mode for the server. The valid values are Integrated, Mixed, Normal and Unknown</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Table 5-11  Fields for SQL Server (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>The underlying operating system.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Platform</td>
<td>The platform.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Product Level</td>
<td>The SQL Server product level. The possible values include B1 and RTM. This field is applicable only for SQL server 2000 and above.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Product Version</td>
<td>The SQL server product version.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Version String</td>
<td>The complete version of the SQL server product instance.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Host Name (DNS)s</td>
<td></td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Fields for UNIX File

### Table 5-12  Fields for UNIX File

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Name</td>
<td>This field returns the name of the target.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Host IP Address</td>
<td>This field returns the host IP address.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Table 5-12: Fields for UNIX File (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name (With Path)</td>
<td>This field returns the file name (with path).</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>The list of IP network addresses on the target</td>
<td>String</td>
<td>Multi valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Fields for UNIX Group

### Table 5-13: Fields for UNIX Group

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Name</td>
<td>This field returns the name of the computer that hosts the group.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>IP Address</td>
<td>This field returns the IP address used to connect to the target.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Group Database</td>
<td>This field returns the database from where the group information is retrieved.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Group Name</td>
<td>This field returns the name of the group.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Fields for UNIX Machine

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Name</td>
<td>This field returns the name of the target.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>IP Address</td>
<td>This field returns the IP address that is used to connect to the target.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Open Distribution Field</td>
<td>This field returns the operating distribution field that is running on this target. For example: Red Hat Linux i686</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Operating System</td>
<td>This field returns the operating system that is running on this target. For example: Linux, SunOS</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Operating System Version</td>
<td>This field returns the operating system version that is running on this target.</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>The list of IP network addresses on the target</td>
<td>String</td>
<td>Multi valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Fields for Windows Domain

**Table 5-15**  
Fields for Windows Domain

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>This field returns the Pre-Windows 2000 name of the domain</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Domain Full Name</td>
<td>This field contains the distinguished name of the reported domain. This field returns [N/A] for NT4 domains.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Domain Mode</td>
<td>This field returns the mode in which the domain is running. For Windows NT 4.0 domains the field returns 'Pre-Windows 2000 mode'. For the domains that are running in Mixed mode the field returns Mixed Mode otherwise Native Mode. This field is only accurate when the Query Engine is installed on a Windows 2000 or later OS.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Table 5-15  Fields for Windows Domain (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Type</td>
<td>This field returns the type of the operating system that is installed on the Primary Domain Controller.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>DNS Forest Name</td>
<td>This field returns the name of the forest (in the DNS format) where the domain resides.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Description</td>
<td>This field returns the description text that is associated with the Domain from the Active Directory. This field returns N/A for NT4 domains.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Domain Functional Level</td>
<td>This field returns the domain functionality level. The domain functionality activates the features that affect the whole domain and that domain only.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Forest Functional Level</td>
<td>This fields returns the forest functionality level. The forest functionality level activates the features across all the domains in your forest.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
# Fields for Windows Directory

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the domain or the workgroup membership (which ever is appropriate for that computer) of the computer that contains the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'domain Workgroup Name (Machine Setting)' to determine the domain or workgroup that the computer is a member of.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Machine Name</td>
<td>This field returns the name of the directory's computer.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Directory Name</td>
<td>This field returns the full path name of the directory.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Owner</td>
<td>This field returns the name of the account that currently owns the directory. The owner has the ability to change the permission assignments to the directory.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Member of Domain</td>
<td>This field returns True, if the computer that contains the directory is the member of the domain</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
## Fields for Windows Group

### Table 5-17 Fields for Windows Group

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the domain or workgroup membership (which ever is</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td></td>
<td>appropriate for that machine) of the machine containing the directory. This</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>field obtains the name from the Query Engine's reporting domain settings.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use the field 'Domain / Workgroup Name (Machine Setting)' to determine the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>domain or workgroup that the machine is a member of.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Name (Pre-Windows 2000)</td>
<td>This field returns the Pre-Windows 2000 name of the group object.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Machine Name</td>
<td>This field returns the name of the machine that contains the file.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>----------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Group Type</td>
<td>This field returns group type, i.e. domain local, domain global, universal local.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Host Machine Member of Domain</td>
<td>This field returns true if the group is owned by a machine that is a member of a domain.</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Fields for Windows Machine

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the domain or workgroup membership (which ever is appropriate for that machine) of the machine containing the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'Domain / Workgroup Name (Machine Setting)' to determine the domain or workgroup that the machine is a member of.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Machine Name</td>
<td>This field returns the name of the machine that contains the file.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>------------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>OS Major Version Number</td>
<td>This field returns the major version number of the machine’s NT operating system. Ex. For NT 3.51, the major version is 3. The &quot;OS Major Version Number (Browser)&quot; field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.</td>
<td>Integer</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
Table 5-18  Fields for Windows Machine *(continued)*

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Minor Version Number</td>
<td>This field returns the minor version number of the machine's NT operating system. Ex. For NT 3.51, the minor version is 51. The &quot;OS Minor Version Number (Browser)&quot; field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available/</td>
<td>Integer</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>OS Type</td>
<td>This field returns machine's Windows operating system type. It also indicates if the machine has Terminal Services capability.</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
### Table 5-18  Fields for Windows Machine *(continued)*

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Is Server</td>
<td>This field returns true if the machine is running the NT Server operating system. The &quot;Machine Is Server? (Browser)&quot; field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>--------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Machine Is BDC</td>
<td>This field returns true if the machine is a backup domain controller. The &quot;Machine Is BDC? (Browser)&quot; field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Machine Is PDC</td>
<td>This field returns true if the machine is a primary domain controller. The &quot;Machine Is PDC? (Browser)&quot; field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Member of Domain</td>
<td>This field returns true if the machine is a member of a domain.</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Host Name (DNS)</td>
<td>This field returns the host name of the computer by querying the name server. The configured name server of the Query Engine computer is used to resolve the host name query.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>TCP/IP Addresses (List)</td>
<td>This field returns a list of the TCP/IP addresses that are configured for the computer.</td>
<td>String</td>
<td>Multi valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
## Fields for Windows Share

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the domain or workgroup membership (which ever is appropriate for that machine) of the machine containing the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'Domain / Workgroup Name (Machine Setting)' to determine the domain or workgroup that the machine is a member of.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Machine Name</td>
<td>This field returns the name of the machine that contains the file.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Share Name</td>
<td>This field returns the name assigned to the share.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Table 5-19  Fields for Windows Share (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hidden</td>
<td>This field returns True if the Windows share is hidden for normal browsing. The Shares are hidden by adding a &quot;$&quot; at the end of the share name.</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Comment</td>
<td>This field returns the comment text that is assigned to the share. This is usually a description of the share.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
# Fields for Windows File

**Table 5-20**

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain/Workgroup Name</strong></td>
<td>This field returns the domain or the workgroup membership (which ever is appropriate for that computer) of the computer that contains the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'Domain / Workgroup Name (Machine Setting)' to determine the domain or workgroup that the machine is a member of.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td><strong>Machine Name</strong></td>
<td>This field returns the name of the machine that contains the file.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td><strong>File Name (With Path)</strong></td>
<td>This field returns the full path name of the file.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Last Modified Date/Time</td>
<td>This field returns the date and time the file was last modified.</td>
<td>DateTime</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Owner</td>
<td>This field returns the name of the account that currently owns the file. The owner has the ability to change permission assignments for the file.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Size (MB)</td>
<td>This field returns the logical size of the file in megabytes.</td>
<td>Double</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Member of Domain</td>
<td>This field returns true if the machine that contains the file is a member of a domain.</td>
<td>Boolean</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Table 5-20  Fields for Windows File (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (DNS)</td>
<td>This field returns the host name of the computer by querying the name server. The configured name server of the Query Engine computer is used to resolve the host name query.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>TCP/IP Addresses (List)</td>
<td>This field returns a list of the TCP/IP addresses that are configured for the computer.</td>
<td>String</td>
<td>Multi valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Fields for Administrative Groups MS-Exchange

### Table 5-21  Fields for Administrative Groups MS-Exchange

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Group DN</td>
<td>This field returns the full distinguished name of the Administrative Group.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Administrative Group Name</td>
<td>This field returns the common name value of the object. Typically, this is identical to the admin display name and name values.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Object Class Type</td>
<td>This field returns the object class type.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Note:** If you want to import the assets of the Administrative Groups MS Exchange asset type from a CSV file with Organization MS Exchange as scope, you must enter Organization DN field manually in the CSV file.

### Fields for Exchange Server

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server DN</td>
<td>This field returns the full distinguished name of this object that is system created.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
Table 5-22  Fields for Exchange Server (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Version / Build (String)</td>
<td>This field returns version and the build number of Microsoft Exchange on that server. If the Internet Explorer version is older than 4.0, then the data returns as &lt;unknown&gt;.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Server Roles</td>
<td>This field returns all the roles that are currently configured for the Exchange 2007 server.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
<tr>
<td>Server name</td>
<td>This field returns the computer name, as per the registry.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Note:** If you want to import the assets of the Exchange Server asset type from a CSV file with Organization MS Exchange as scope, you must enter Organization DN field manually in the CSV file.
### Fields for Organization MS-Exchange

**Table 5-23**

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization DN</td>
<td>This field returns the full distinguished name of the organization.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Organization Name</td>
<td>This field returns the organization name from the organization DN.</td>
<td>String</td>
<td>Single valued</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Fields for IIS Virtual Directory

**Table 5-24**

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Directory Name</td>
<td>This field returns the name (without path) of the virtual directory, directory, or the file object.</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>ADSI Path</td>
<td>This field returns the ADSI path of the IISAdmin object that is associated with the record.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Parent Web Site Name</td>
<td>This field returns the user-friendly name of the item's parent Web Site.</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the name of the domain or workgroup that contains the computer on which the device driver is found. This field obtains the name from the Query Engine's reporting domain settings.</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>PrimKey Machine</td>
<td>This field returns the primary key of the machine.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Display name</td>
<td>Description</td>
<td>Type</td>
<td>Single valued or multi valued</td>
<td>Field type</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Is In Domain (internal)</td>
<td>This field returns the domain membership of the computer on which the process is running. If the computer is not the member of the domain, this field returns &quot;N/A.&quot; This field obtains the domain from the Query Engine's reporting domain settings. Use the Domain / Workgroup Name (Machine Settings) field to determine the domain or a workgroup of which the computer is a member.</td>
<td>String</td>
<td>Single valued</td>
<td></td>
</tr>
<tr>
<td>PrimKey Domain</td>
<td>This field returns the primary key of the domain.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Fields for IIS Web Site

**Table 5-25**

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Site Name</td>
<td>This field returns the name of the object.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>ADSI Path</td>
<td>This field returns the ADSI path of the IISAdmin object that is associated with the record.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>Domain/Workgroup Name</td>
<td>This field returns the name of the domain or workgroup that contains the computer on which the device driver is found. This field obtains the name from the Query Engine's reporting domain settings.</td>
<td>String</td>
<td>Single valued</td>
<td>Mandatory</td>
</tr>
<tr>
<td>PrimKey Machine</td>
<td>This field returns the primary key of the machine.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
</tbody>
</table>
### Table 5-25  Fields for IIS Web Site (continued)

<table>
<thead>
<tr>
<th>Display name</th>
<th>Description</th>
<th>Type</th>
<th>Single valued or multi valued</th>
<th>Field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is In Domain (internal)</td>
<td>This field returns the domain membership of the computer on which the process is running. If the computer is not the member of the domain, this field returns &quot;N/A.&quot; This field obtains the domain from the Query Engine's reporting domain settings. Use the Domain / Workgroup Name (Machine Settings) field to determine the domain or a workgroup of which the computer is a member.</td>
<td>String</td>
<td>Single valued</td>
<td>Primary</td>
</tr>
<tr>
<td>PrimKey Domain</td>
<td>This field returns the primary key of the domain.</td>
<td>String</td>
<td>Single valued</td>
<td></td>
</tr>
</tbody>
</table>

**Probable asset types**

The probable asset types are the entities for the predefined platforms that the asset system does not support by default.

The Control Compliance Suite supports certain entities of the predefined platforms to be the asset types. The predefined asset types are the entities of the predefined platforms.
See “Predefined asset types” on page 236.

In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong.

See “Predefined platforms” on page 235.

See “About platforms” on page 456.

A group of fields that define the common functions of the network element form an entity.

See “About entities” on page 457.

In addition to the predefined asset types, Control Compliance Suite provides certain probable asset types. You can use the Schema Manager view and create your own asset type with the entities that are not supported by default.

See “About the Schema Manager view” on page 444.

The probable asset types for the SQL platform are as follows:

- Stored procedure
- Database Users

The probable asset types for the UNIX platform are as follows:

- User

The probable asset types for the Windows platform are as follows:

- IIS virtual directories
- IIS Web sites
- Registry
- Service

See “Custom asset types” on page 274.

**Custom asset types**

Control Compliance Suite lets you create custom asset types from the custom platforms and custom entities that you can create from the Schema Manager view.

See “About the entity schema” on page 445.

You can import the assets from the custom asset types in the same way as you import the assets from any other asset type.

Asset types are based on the entities of the platform. In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong. A
group of fields that define the common functions of the network element form an entity.

See “About platforms” on page 456.

See “About entities” on page 457.

When you create your own platform and define fields for the platform to create an entity, you can define an asset type also. The custom asset type imports the data of the fields that are defined in the custom entity.

See “Creating a new asset type” on page 446.

See “Extending an existing asset type” on page 451.

### Primary and secondary assets

Primary assets are the assets that should be imported first to import certain other kind of assets. Primary assets act as the default scope to import the other asset types. The assets that are imported after the primary assets are the secondary assets. Primary assets constitute the super-set of the secondary assets.

For example, in the Control Compliance Suite, you must import the Windows Domain before you import the Windows Machines. In this example, Windows Domain is the primary asset and the Windows Machine is the secondary asset. In the asset system Windows Domain is the default scope for the Windows Machines.

See “Default scope and supported scope” on page 351.

In the asset system, Site is the primary asset for all the asset types. When you import the assets of any asset type, you can use the Site as the scope. But, it is not recommended to use the Site as a scope even if it is a supported scope for all the asset types. You are recommended to use the default scopes.

Using the default scope implies the import of the primary assets before the secondary assets.

See “About scopes in asset import” on page 349.

**Table 5-26** Predefined asset types and primary assets

<table>
<thead>
<tr>
<th>Asset type</th>
<th>Primary asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM Agents</td>
<td>Site</td>
</tr>
<tr>
<td>ESM Agents</td>
<td>ESM Agents</td>
</tr>
<tr>
<td>Oracle Configured Databases</td>
<td>Site</td>
</tr>
<tr>
<td>Oracle Configured Servers</td>
<td>Site</td>
</tr>
</tbody>
</table>
Table 5-26  Predefined asset types and primary assets (continued)

<table>
<thead>
<tr>
<th>Asset type</th>
<th>Primary asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Databases</td>
<td>SQL Server</td>
</tr>
<tr>
<td>SQL Server</td>
<td>Site</td>
</tr>
<tr>
<td>UNIX Machine</td>
<td>Site</td>
</tr>
<tr>
<td>UNIX Group</td>
<td>UNIX Machine</td>
</tr>
<tr>
<td>UNIX File</td>
<td>UNIX Machine</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>Site</td>
</tr>
<tr>
<td>Windows Machine</td>
<td>Windows Domain</td>
</tr>
<tr>
<td>Windows Group</td>
<td>Windows Machine</td>
</tr>
<tr>
<td>Windows Directory</td>
<td>Windows Machine</td>
</tr>
<tr>
<td>Windows File</td>
<td>Windows Machine</td>
</tr>
<tr>
<td>IIS Virtual Directory</td>
<td>Windows Machine</td>
</tr>
<tr>
<td>IIS Web Site</td>
<td>Windows Machine</td>
</tr>
<tr>
<td>Windows Share</td>
<td>Windows Machine</td>
</tr>
<tr>
<td>Administrative Group MS-Exchange</td>
<td>Organization MS-Exchange</td>
</tr>
<tr>
<td>Exchange Server</td>
<td>Organization MS-Exchange</td>
</tr>
<tr>
<td>Organization MS-Exchange</td>
<td>Site</td>
</tr>
</tbody>
</table>

Site is the primary asset for ESM Agents, Oracle Configured Databases, Oracle Configured Servers, SQL Servers, UNIX Machine, Windows Domain, and Organization MS-Exchange.

The primary asset for the SQL asset types is SQL Server.
The primary asset for the UNIX asset types is UNIX Machine.
The primary asset for the Windows asset types is Windows Domain.

Reconciliation rules and rule types

The asset reconciliation helps you organize the assets that already exist in the asset store in a logical hierarchy. Reconciliation provides you the flexibility to manage the asset records conditionally when the records get into the assets system.
The reconciliation rule lets the administrator manage the asset information when imported into the system. A reconciliation rule consists of a condition and an action. A set of actions is executed when the imported asset satisfies the specified set of conditions.

Reconciliation is based on the priority. A reconciliation rule that is enabled and is at the top in order, takes highest priority. If the rule is not satisfied, then the second rule takes priority with succeeding rules, if necessary. If an asset does not satisfy any reconciliation rule, the asset is forwarded to the manual review store. Control Compliance Suite performs the asset reconciliation that is based on some rules. Every rule that you create must be compliant with one of the rule-types that the asset system defines. All the reconciliation rules are displayed in Manage > Assets > Reconciliation Rules view.

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Rule description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre rule</td>
<td>A Pre rule is executed on the assets that are in the process of import before the assets are brought into the assets system. The Pre rule lets you set a value for a particular asset field. The Pre rule also lets you discard the asset.</td>
</tr>
<tr>
<td>Add rule</td>
<td>An Add rule is executed to add the assets that are in the process of import to the asset system. The Add rule lets you add new assets to the asset system at a specific location. The Add rule also lets you add assets to the manual review store.</td>
</tr>
</tbody>
</table>

See “Pre rule” on page 278.

See “Add rule” on page 280.
Table 5-27  Types of reconciliation rules (continued)

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Rule description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update rule</td>
<td>An Update rule is applied on the existing assets to update their fields with the values of the assets that in the process of import. The update rule updates the assets that already exist in the system. The update rule also lets you add assets to the manual review store.</td>
</tr>
</tbody>
</table>

| Post rule | A Post rule is executed at the end in the order of the reconciliation rules. The Post rule is executed only for the imported asset records for which there is a corresponding addition or update in the asset system. |

**Note:** Every asset import job must have at least one add or update rule.

In addition to the rules that you can create, Control Compliance Suite also provides predefined rules. You can use any of the predefined rules to import the assets for the very first time.

See “Predefined reconciliation rules” on page 284.

See “Creating reconciliation rules without manual review” on page 306.

See “Creating reconciliation rules using the manual review” on page 307.

**Pre rule**

A Pre rule is executed on the assets being imported before the assets are brought into the assets system.

Table 5-28 are as follows:
Table 5-28  Conditions for Pre rule

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>The specified action is performed on the assets every time.</td>
</tr>
<tr>
<td>If an asset being imported does not exist in the asset system</td>
<td>The action is performed only if the asset that is being imported does not exist already in the asset system.</td>
</tr>
<tr>
<td>If an asset being imported exists in the asset system</td>
<td>The action is performed only if the asset that is being imported already exists in the asset system.</td>
</tr>
<tr>
<td>If field of an asset being imported is not set</td>
<td>The action is performed only if the asset field is not set.</td>
</tr>
<tr>
<td>If field of an asset being imported has a relation with a specified value</td>
<td>The action is performed only if the field of the asset that is being imported has a specified relation with the specified value. For example, <code>&lt;field&gt;&lt;operator&gt;&lt;value&gt;&lt;Asset Custodian&gt;&lt;equals&gt;&lt;ABC&gt;</code></td>
</tr>
</tbody>
</table>

Table 5-29 are as follows:

Table 5-29  Actions for Pre rule

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard an asset being imported</td>
<td>Ignores the asset that is being imported. The asset is not added to the asset system if no Add Rule is specified.</td>
</tr>
<tr>
<td>Set the field value of an asset being imported as specified</td>
<td>Sets the field value of the asset that is being imported as the value that you specify. Lets you select the asset field for which you want to set the value. You can also specify the value that you want to set.</td>
</tr>
</tbody>
</table>

Example for the Pre rule:
If an asset being imported exists in the asset system THEN Set the field value of an asset being imported as specified.

This rule condition checks if the asset to be imported exists in the system. If the asset already exists, it sets the value of the selected field for that asset according to the given value.

See “Using a Pre rule to set the values of the common fields” on page 309.

**Add rule**

The Add rule is executed to add the assets being imported to the asset system.

**Table 5-30** are as follows:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If an asset being imported does not exist in the asset system</td>
<td>The action is performed only if the asset that is being imported does not exist already in the asset system.</td>
</tr>
<tr>
<td>If field of an asset being imported has a relation with a specified value</td>
<td>The action is performed only if the field of the asset that is being imported has a specified relation with the specified value. For example, <code>&lt;field&gt;&lt;operator&gt;&lt;value&gt;&lt;Asset Custodian&gt;&lt;equals&gt;&lt;ABC&gt;</code></td>
</tr>
</tbody>
</table>

**Table 5-31** are as follows:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add an asset being imported to the specified folder</td>
<td>Adds the asset that is being imported to the folder that you specify.</td>
</tr>
<tr>
<td>Add to manual review store</td>
<td>Adds the asset to the manual review store. See “Manual review” on page 295.</td>
</tr>
</tbody>
</table>

Example for the Add rule:

If field of an asset being imported has a relation with a specified value THEN Add an asset being imported to the specified folder.
This rule condition checks the value of the selected field of the asset being imported with the existing asset. If the value matches the existing asset, it adds the asset to the specified folder.

See “Using an Add rule to dynamically create asset folders” on page 310.

**Update rule**

Update rule is applied on the existing assets to update their fields with the values of the assets being imported.

Table 5-32 are as follows:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If an asset being imported exists in the asset system</td>
<td>The action is performed only if the asset that is being imported already exists in the asset system.</td>
</tr>
<tr>
<td>If an existing asset field has a relation with a specified value</td>
<td>The action is performed if the existing asset field has a specified relation with the specified value For example, <code>&lt;imported asset field&gt; &lt;operator&gt; &lt;value&gt;</code></td>
</tr>
<tr>
<td>If field of an asset being imported has a relation with a specified value</td>
<td>The action is performed only if the field of the asset that is being imported has a specified relation with the specified value For example, <code>&lt;field&gt; &lt;operator&gt; &lt;value&gt; &lt;Asset Custodian&gt; &lt;equals&gt; &lt;ABC&gt;</code></td>
</tr>
<tr>
<td>If field of an asset being imported has a relation with an existing asset field</td>
<td>The action is performed only if the field of an asset that is being imported has a specified relation with the field of an existing asset. For example, <code>&lt;current asset field&gt; &lt;operator&gt; &lt;imported asset field&gt; &lt;Asset Custodian&gt; &lt;equals&gt; &lt;Asset Owner&gt;</code></td>
</tr>
</tbody>
</table>

Table 5-33 are as follows:
### Table 5-33  Actions for Update rule

<table>
<thead>
<tr>
<th>Update rule- action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the field value of an existing asset as specified</td>
<td>Sets the field value of an existing asset as that you specify. [Description] [Sets the field value of an existing asset as that you specify.] [Lets you select the asset field for which you want to set the value. You can also specify the value that you want to set.] [If you select Asset Tags as the field, you can also select the Tag Set Options that work as follows:] [] Clear [Removes all the tags from the asset before the asset is imported to the asset system.] [] Append [Adds the tag to the asset alongwith the existing tags before the asset is imported to the asset system.] [This option is selected by default. If you do not select any tag set option, the new tag is appended to the asset.] [] Overwrite [Replaces the existing tag with the new tag.]</td>
</tr>
<tr>
<td>Update specified fields of an existing asset with the fields of the asset being imported</td>
<td>Replaces the values of the selected fields of an existing asset with the values of the fields of the asset that is being imported. <strong>Note:</strong> This action has a different behavior in case you choose to update the tags of an asset. This action adds the new tags of an asset being imported to the tags of the existing asset. The existing tags remain intact and do not get overwritten.</td>
</tr>
<tr>
<td>Add to manual review store</td>
<td>Adds the asset to the manual review store. [Description] [Adds the asset to the manual review store. See “Manual review” on page 295.]</td>
</tr>
</tbody>
</table>

**Examples for Update rule:**

If field of an asset being imported has a relation with a specified value THEN Update specified fields of an existing asset with the fields of the asset being imported.
This condition updates the values of the assets that are present in the asset system. See “Using an Update rule to update the existing field values” on page 311.

**Post rule**

The Post rule is executed at the end in the order of the reconciliation rules. **Table 5-34** are as follows:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If an asset being imported exists in the asset system</td>
<td>The action is performed only if the asset that is being imported already exists in the asset system.</td>
</tr>
<tr>
<td>If an asset being imported is added in the asset system</td>
<td>The action is performed only if the asset that is being imported is added in the asset system.</td>
</tr>
<tr>
<td>If an asset being imported is updated in the asset system</td>
<td>The action is performed only if the asset that is being imported is updated in the Asset System.</td>
</tr>
<tr>
<td>If an existing asset field has a relation with the specified value</td>
<td>The action is performed if the field of the existing asset has a specified relation with the specified value. For example, <code>&lt;imported asset field&gt; &lt;operator&gt; &lt;value&gt;</code></td>
</tr>
<tr>
<td>If field of an asset being imported has a relation with a specified value</td>
<td>The action is performed only if the field of the asset that is being imported has a specified relation with the specified value. For example, <code>&lt;field&gt; &lt;operator&gt; &lt;value&gt; &lt;Asset Custodian&gt; &lt;equals&gt; &lt;ABC&gt;</code></td>
</tr>
</tbody>
</table>
Table 5-34  Conditions for Post rule (continued)

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If field of an asset being imported has a relation with an existing asset field</td>
<td>The action is performed only if the field of an asset that is being imported has a specified relation with the field of an existing asset. For example, <code>&lt;current asset field&gt;&lt;operator&gt;&lt;imported asset field&gt;</code> <code>&lt;Asset Custodian&gt;&lt;equals&gt;&lt;Asset Owner&gt;</code></td>
</tr>
</tbody>
</table>

Table 5-35 are as follows:

Table 5-35  Actions for Post rule

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move the existing asset to the specified folder</td>
<td>Moves the existing asset from its current location to the specified location in the asset system.</td>
</tr>
</tbody>
</table>

Example for Post rule:

IF an asset being imported is updated in the asset system THEN Move the existing asset to the specified folder.

This condition moves the assets that are already present in the asset store to the specified folder.

See “Using a Post rule to mark the assets as control points” on page 312.

Predefined reconciliation rules

To create an asset import job for the first time, Control Compliance Suite provides predefined rules. You can use the predefined rules for importing the assets for the first time without creating custom reconciliation rules.

See “Asset folder hierarchy” on page 234.

See “About organizing objects in the directory” on page 36.

See “Creating the asset folders” on page 375.
Table 5-36  Predefined reconciliation rules

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Rule statement</th>
<th>Rule description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Rule</td>
<td>IF an asset being imported does not exist in the asset system Then Add an asset</td>
<td>The rule is applicable to all the asset types. The rule adds all the assets that are being imported to the asset system if they do not exist already in the system. The assets are added to the Asset System folder.</td>
</tr>
<tr>
<td>Rule Name: Add asset to the asset system</td>
<td>being imported to the Asset System folder</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre Rule</td>
<td>IF an asset being imported does not exist in the asset system Then Set the value</td>
<td>The rule is applicable to all the asset types. The rule checks if the asset that is the process of import is in the asset system or not. If the asset is not in the asset system, it sets the value of the Confidentiality, Integrity, and Availability attributes of the assets to NotDefined.</td>
</tr>
<tr>
<td>Rule Name: Set CIA values before adding asset to the asset system</td>
<td>of the Confidentiality field as NotDefined Set the value of the Integrity field as NotDefined Set the value of the Availability field as NotDefined</td>
<td></td>
</tr>
<tr>
<td>Pre Rule for Exchange</td>
<td>IF object class type does not equal msExchAdminGroup Then discard an asset</td>
<td>The rule is applicable to the Administrative Groups MS-Exchange asset type only. The rule checks if the asset that is in the process of import is an administrative group or not. If the asset is not an administrative group, the rule discards the asset.</td>
</tr>
<tr>
<td>Rule Name: Filter Exchange Administrative Groups</td>
<td>being imported</td>
<td></td>
</tr>
<tr>
<td>Rule type</td>
<td>Rule statement</td>
<td>Rule description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pre Rule for Exchange</td>
<td>IF object class type does not equal msExchEdgeServer THEN discard an asset being imported</td>
<td>The rule is applicable to the Exchange Server asset type only. The rule checks if the asset that is in the process of import is an Exchange Edge Server or not. If the asset is an Exchange Server, the rule discards the asset.</td>
</tr>
<tr>
<td>Rule Name: Filter Exchange Edge Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Rule</td>
<td>IF an asset being imported exists in the asset system THEN update all fields of the existing asset with the values of the current asset.</td>
<td>The rule is applicable to all the asset types. The rule checks if the asset that in the process of import exists in the asset system or not. If the asset is in the asset system, the rule overwrites the values of all the existing asset fields with the values of the asset being imported.</td>
</tr>
<tr>
<td>Rule Name: Update asset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Rule for ESM</td>
<td>IF an asset being imported exists in the asset system THEN update only selected fields Host Name, IP Address, FQDN of an existing asset with the fields of the asset being imported. (Manual review enabled)</td>
<td>The rule is applicable only to the ESM Agent asset type. The rule checks if the asset that in the process of import exists in the asset system or not. If the asset exists in the asset system, the rule overwrites the values of the fields Host Name, IP Address, and FQDN with the values of the new asset. The asset records are sent to the manual review store.</td>
</tr>
<tr>
<td>Rule Name: Update Host Name, IP Address, and FQDN for ESM agents</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
See “Creating reconciliation rules without manual review” on page 306.
See “Creating reconciliation rules using the manual review” on page 307.

**Asset being imported**

The term 'assets being imported' is used with reference to the creation of reconciliation rules. The reconciliation rules are applied on the assets being imported.

An asset being imported is a potential asset, which is yet not a part of the asset system. It is the asset that is collected from the data collector but can only be called the asset when it passes through the reconciliation rules. After the reconciliation rules are applied, the asset to be imported becomes an asset.

For example, consider that you want to add Windows Machines from a specific site as assets to the asset system.

Your rule statement reads as follows:

If an asset being imported does not exist in the asset system

THEN Add an asset being imported to the specified folder

In this case, the Windows Machines remain the 'asset being imported' until the rule verifies that the computers are not present in the asset system and adds those into the asset system. The Windows Machines that are already present in the system are not added to the asset system and do not become assets.

**Existing assets**

The term existing assets is used with reference to the creation of reconciliation rules. The existing assets are the assets that are already a part of the asset system. The existing assets are present in the asset store in the CCS directory.

The objects that are collected from the data collectors are referred to as asset being imported until the reconciliation rules are applied.

See “Asset being imported” on page 287.

When the rules are applied on the asset being imported, the assets that satisfy the rules criteria become a part of the asset system. These assets are then referred to as the existing assets.

For example, consider that you want to update the values of specific asset fields with the Update rule.

Your rule statement reads as follows:

IF an asset being imported exists in the asset system
THEN Update specified fields of an existing asset with the fields of the asset being imported

In this case, the rule checks the field values of the existing assets which are the assets that are already in the asset store. If the asset being imported exists in the asset system, the rule overwrites the values of the existing assets with those of the asset being imported.

Asset import

In the asset system, asset import involves the import of the following data:

- Data for the common fields
  Common fields are the fields that are common across all the asset types. See “Common fields for all asset types” on page 345. The data for the common fields is imported from the CSV data collector.

- Data for the asset-specific fields
  Asset-specific fields are the fields that are specific to the asset type that you select to import. See “Predefined asset types” on page 236. The data for the asset-specific fields is imported from the default data collector.

Go through the following concepts to perform the asset import more effectively:

- Default data collectors
  See “Default data collectors” on page 288.

- Data collectors and asset types
  See “Data collectors and asset types” on page 289.

- Asset field filters
  See “Examples of asset filters” on page 292.

- Filter statement operators
  See “Filter statement operators” on page 293.

- Asset reconciliation
  See “Asset reconciliation” on page 295.

- Manual review
  See “Manual review” on page 295.

Default data collectors

You can choose to import the assets from the default or the CSV data collector.

The asset system assigns the following default data collectors for various platforms:
### Table 5-37  Platform and data collectors

<table>
<thead>
<tr>
<th>Platform</th>
<th>Data collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM platform</td>
<td>ESM data collector</td>
</tr>
<tr>
<td>Oracle platform</td>
<td>Oracle data collector</td>
</tr>
<tr>
<td>SQL platform</td>
<td>SQL data collector</td>
</tr>
<tr>
<td>UNIX platform</td>
<td>UNIX data collector</td>
</tr>
<tr>
<td>Windows platform</td>
<td>Windows data collector</td>
</tr>
<tr>
<td>Exchange platform</td>
<td>Exchange data collector</td>
</tr>
<tr>
<td>NDS platform</td>
<td>NDS data collector</td>
</tr>
<tr>
<td>NetWare platform</td>
<td>NetWare data collector</td>
</tr>
</tbody>
</table>
| Custom platform     | You can use the following data collector for the custom platform:  
  ■ CSV data collector  
  ■ ODBC data collector |
| Common platform     | The following data collector can be used to collect the Common fields:  
  ■ CSV data collector  
  ■ ODBC data collector |

Note: For custom platforms, if you select CSV or ODBC data collector during entity schema creation, then the selected data collector becomes the default data collector. When importing assets of the custom platform, the option, Default appears in the drop-down list of the Create or Edit Asset Import wizard.

See “About the working of default data collectors in asset import” on page 322.

### Data collectors and asset types

The asset types associated with the available data collectors are as follows:

- CSV
  - SQL Database
- SQL Server
- ESM Agent
- Oracle Configured Databases
- Oracle Configured Servers
- UNIX File
- UNIX Group
- UNIX Machine
- Windows Directory
- Windows Domain
- Windows File
- Windows Machine
- Windows Share
- Organization MS-Exchange
- Administrative Groups MS-Exchange
- Exchange Server
- NDS Tree
- NetWare File Server

- ESM
- ESM Agent

- Oracle
  - Oracle Configured Databases
  - Oracle Configured Servers

- SQL
  - SQL Database
  - SQL Server

- UNIX
  - UNIX File
  - UNIX Group
  - UNIX Machine
- Windows
  - Windows Directory
  - Windows Domain
  - Windows File
  - Windows Machine
  - Windows Share
- Exchange
  - Organization MS-Exchange
  - Administrative Groups MS-Exchange
  - Exchange Server
- NDS
  - NDS Tree
- NetWare
  - NetWare File Server
- ODBC
  - SQL Database
  - SQL Server
  - ESM Agent
  - Oracle Configured Databases
  - Oracle Configured Servers
  - UNIX File
  - UNIX Group
  - UNIX Machine
  - Windows Directory
  - Windows Domain
  - Windows File
  - Windows Machine
  - Windows Share
  - Organization MS-Exchange
  - Administrative Groups MS-Exchange
Examples of asset filters

You create the filter statements that are based on the asset fields when you create an asset group and an asset import job.

In case of creation of an asset import job, you need to create the filters that are based on the asset type that you select.

The following table describes certain filter statements that you can use to import assets under specific scenarios.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Filter statement</th>
<th>Job result</th>
</tr>
</thead>
<tbody>
<tr>
<td>To import assets of the Windows Directory with Machine 1 and Machine 2 as scope</td>
<td><code>((Root Path EqualTo D: Or Root Path EqualTo C:) and depth GreaterThanOrEqualTo 1) and Is Shared? = True</code></td>
<td>The job returns all the shared folders under the C: \ and the D: \ drive.</td>
</tr>
<tr>
<td>To import the Files and the Directories with name like <em>Accounting</em></td>
<td><code>(Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1) and Directory Name Like %Accounts%</code></td>
<td>The job returns all the directories and the files that contain Accounting in the name.</td>
</tr>
<tr>
<td>To import all the directories and the files &quot;n&quot; level below the directory, D:\DATA</td>
<td><code>Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1</code></td>
<td>The job returns all the directories under the D: \ directory as per the available depth.</td>
</tr>
<tr>
<td>To import the Windows Directories with Machine 1 and domain as a scope</td>
<td><code>(Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1) and PermissionsDifferentThanParent(Include Owner) / (Ignore Owner) EqualTo Different</code></td>
<td>The job returns all the directories of which the permissions differ from the parent.</td>
</tr>
</tbody>
</table>
Table 5-38  Examples of asset filters (continued)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Filter statement</th>
<th>Job result</th>
</tr>
</thead>
<tbody>
<tr>
<td>To import UNIX Files under the directory, etc and the sub-directories</td>
<td><code>Filename(With Path) like /etc%</code></td>
<td>The job returns all the UNIX files under the directory, etc and from under the sub-directories.</td>
</tr>
</tbody>
</table>

Filter statement operators

The filter statement operators are the operators that are used for creating filter statements in the asset import job and the asset groups. These operators are used to make a comparison between the two given values.

Table 5-39  Filter statement operators

<table>
<thead>
<tr>
<th>Operator Name</th>
<th>Description</th>
<th>Filter Statement examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal To (=)</td>
<td>A must be equal to B</td>
<td>Directory Name EqualTo 'Admin'</td>
</tr>
<tr>
<td>NotEqualTo (!=)</td>
<td>A must not be equal to B</td>
<td>Directory Name NotEqualTo 'HR'</td>
</tr>
<tr>
<td>Like</td>
<td>The SQL like operator, with same syntax and semantics.</td>
<td>Database Name like DB2</td>
</tr>
<tr>
<td>Not Like</td>
<td>The SQL not like operator. Note the space between not and like. Any amount of white space (blanks, tabs, new lines, or carriage returns) is allowed here. The white space is not strictly required, but it is best not to omit it.</td>
<td>Database Name NotLike DB2</td>
</tr>
<tr>
<td>Match (=~)</td>
<td>The regular expression matching operator.</td>
<td>Directory Name Match 'CM*'</td>
</tr>
<tr>
<td>NoMatch (!~)</td>
<td>The negative of the expression matching operator.</td>
<td>Directory Name NotMatch 'CM**'</td>
</tr>
</tbody>
</table>
### Table 5-39 Filter statement operators (continued)

<table>
<thead>
<tr>
<th>Operator Name</th>
<th>Description</th>
<th>Filter Statement examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>IsNull</td>
<td>The SQL is null operator. A filter statement that uses this operator must not have a value specified. At least one white space character is required between is and null.</td>
<td>Depth IsNull</td>
</tr>
<tr>
<td>IsNotNull</td>
<td>The negative of is null. The white space between not and null is not strictly required, but it is best not to omit it.</td>
<td>Depth IsNotNull</td>
</tr>
<tr>
<td>Exact</td>
<td>Forces case-sensitive string comparison.</td>
<td>Directory Name Exact 'ERCT'</td>
</tr>
<tr>
<td>Inexact</td>
<td>Forces case-insensitive string comparison.</td>
<td>Directory Name Inexact 'ERCT'</td>
</tr>
<tr>
<td>Contains (%)</td>
<td>In case of single valued field, value on RHS has to be partially or completely matching with LHS. In case of multi valued field, every value on RHS has to be present on the LHS.</td>
<td>Owner Contains John</td>
</tr>
<tr>
<td>ContainsMatch (%)~</td>
<td>In case of single valued field, the regular expression on RHS should match field value on LHS. In case of multi valued field, every regular expression on RHS should match at least one element on LHS.</td>
<td>Owner ContainsMatch John</td>
</tr>
<tr>
<td>NotContains (%)</td>
<td>The negative of the Contains operator.</td>
<td>A NotContains B</td>
</tr>
<tr>
<td>NotContainsMatch (%)~</td>
<td>The negative of the ContainsMatch operator.</td>
<td>A NotContainsMatch B</td>
</tr>
</tbody>
</table>

For example, if you select Description as the field to be used as the filter for the ESM Agent asset type, your filter statement could be as follows:

IF Description <Operator> <Value>
Asset reconciliation

The asset reconciliation helps you organize the assets that already exist in the asset store in a logical hierarchy. Reconciliation provides you the flexibility to manage the asset records conditionally when the records get into the asset system.

A reconciliation rule that you specify in the asset import job decides the action that should be taken on the asset that is being imported.

The reconciliation rules are executed in the following order:

- **Pre rule**
  
  See “Pre rule” on page 278.

- **Add rule**
  
  See “Add rule” on page 280.

- **Update rule**
  
  See “Update rule” on page 281.

- **Post rule**
  
  See “Post rule” on page 283.

The reconciliation process performs the following tasks on the assets that are imported into the asset system:

- Perform actions like discarding the asset, setting CIA values before the asset is added to the asset system.

- Add the newly discovered assets to the asset store.

- Update the properties of the assets that already exist.

- Mark the assets for the manual review that is based on the rule conditions.

  See “Reconciliation rules and rule types” on page 276.

  See “Creating reconciliation rules without manual review” on page 306.

  See “Creating reconciliation rules using the manual review” on page 307.

Manual review

Control Compliance Suite lets you review the assets manually before you choose to add the assets to the asset system. The assets that are marked for manual review are added to the manual review store.

The assets form a part of the manual review store in any of the following cases:

- If you choose to add the assets to the manual review store in the Add Action dialog box during the creation of the Add Rule.
● If you choose to add the assets to the manual review store in the Update Action dialog box during the creation of the Update Rule.

● If the assets do not satisfy any of the reconciliation rules that are associated with the import job.

● If you associate more than one Add or Update rule with an asset import job and one of the rules marks the assets for manual review.

After the asset is stored in the manual review store, the following actions are possible:

● Edit the import job and add new reconciliation rules.

● Re-run the reconciliation on the manual review records from the Monitor > Jobs view using the Reconcile Records option.

See “Viewing the manual review records” on page 368.
See “Reconciling the manual review records” on page 368.

Asset tagging

Control Compliance Suite provides a mechanism to tag and identify assets for report and scope purposes.

Tagging is a way to define an asset with meta information. Tagging helps you identify assets in some context that might prove helpful to determine the value of the asset. You can use the tags to filter the assets.

For example, you can create a tag that is called SOX and associate it with a relevant asset.

Asset groups

An asset group consists of the assets of one or more types. For example, Windows servers, UNIX servers, or Oracle databases can become asset groups.

The asset groups may be created based on various criteria. You can attach the tags to the asset groups and create an asset group that is based on the tags. Similarly, you can create the asset groups that are based on location, owner, risk rating and so on.

The asset groups are of the following types:

● Dynamic asset group
  See “Dynamic asset groups” on page 297.

● Static asset group
  See “Static asset groups” on page 297.
Predefined asset group

See “Predefined asset groups” on page 297.

See “Creating a dynamic asset group” on page 370.

See “Creating a static asset group” on page 372.

See “Editing an asset group” on page 376.

Dynamic asset groups

A dynamic asset group is updated with every asset import job if more assets meet the criteria that is specified in the dynamic group definition. The update to the asset group is done on the basis of the criteria of the group. After the import job, the new assets become a part of the asset group if they match the dynamic filters of that asset group. At the time of query execution, the asset groups are resolved to discrete assets.

The dynamic groups can be created on the basis of the following criteria:

- Common fields of all the asset types
  - You can create the asset groups on the basis of the common field values of all the asset types. The common fields include the asset name, location, department, custodian, owner, tags, and risk rating.

- Specific fields of the asset type

- Both

See “Creating a dynamic asset group” on page 370.

Static asset groups

You can create static asset groups on the basis of the asset type.

The asset count in the static asset groups does not change automatically with the import job. You manually add assets to the static asset groups.

See “Creating a static asset group” on page 372.

Predefined asset groups

The asset system provides predefined asset groups for all the predefined platforms.

See “Predefined platforms” on page 235.

The predefined asset groups are dynamic in nature. The predefined dynamic asset groups are created by default at the time of installation. The predefined asset groups are based on certain asset-specific field filters. The filters for the asset groups form the definitions for the assets that are included in the asset group.
Note: You can use the predefined asset groups only after you copy the asset group to the folder in which you want to group the assets.

You can use the predefined asset groups to provide scope for asset import. The predefined asset groups for the ESM platform are as follows:

**Table 5-40** Predefined asset groups for the ESM platform

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ESM Windows Agents</td>
<td>ESM Agent – OS Version = 'WIN*'</td>
</tr>
<tr>
<td>All ESM UNIX Agents</td>
<td>ESM Agent – OS Version= 'UNIX'</td>
</tr>
<tr>
<td>All ESM Windows 2003 Agents</td>
<td>ESM Agent – OS Version= 'WIN2003'</td>
</tr>
<tr>
<td>All ESM OpenVMS Agents</td>
<td>ESM Agent – OS Version = 'VMS'</td>
</tr>
</tbody>
</table>

The predefined asset groups for the Exchange platform are as follows:

**Table 5-41** Predefined asset groups for the Exchange platform

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Exchange Organizations</td>
<td>-</td>
</tr>
<tr>
<td>All Exchange Servers</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 5-41 Predefined asset groups for the Exchange platform (continued)

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Exchange Administrative Groups</td>
<td>-</td>
</tr>
<tr>
<td>Exchange 2007 Mailbox Servers</td>
<td>Exchange Server – Exchange Version/Build = 'Version8' and Exchange Server - Server Role(s) = 'Mailbox'</td>
</tr>
</tbody>
</table>

The predefined asset groups for the NDS platform are as follows:

### Table 5-42 Predefined asset groups for the NDS platform

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All NDS Trees</td>
<td>NDS Tree - Tree name Equal To (=) '*'</td>
</tr>
</tbody>
</table>

The predefined asset groups for the NetWare platform are as follows:

### Table 5-43 Predefined asset groups for the NetWare platform

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All NetWare Servers</td>
<td>NetWare Server- Object Name (DN) Equal To (=) '*'</td>
</tr>
<tr>
<td>NetWare 6.5 Servers</td>
<td>NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server-NetWare Version = '<em>NetWare 5.70</em>'</td>
</tr>
<tr>
<td>NetWare 5.X Servers</td>
<td>NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server-NetWare Version = '<em>NetWare 5.00</em>'</td>
</tr>
<tr>
<td>NetWare 4.X Servers</td>
<td>NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server-NetWare Version = '<em>NetWare 4.</em>'</td>
</tr>
</tbody>
</table>
Table 5-43  Predefined asset groups for the NetWare platform *(continued)*

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetWare 6 Servers</td>
<td>NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server- NetWare Version = &quot;NetWare 5.60&quot;</td>
</tr>
</tbody>
</table>

The predefined asset groups for the Oracle platform are as follows:

Table 5-44  Predefined asset groups for the Oracle platform

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Oracle Servers</td>
<td>-</td>
</tr>
<tr>
<td>All Oracle 9i Databases</td>
<td>Oracle Configured Databases- Database Version = '9''</td>
</tr>
<tr>
<td>All Oracle 10g Databases</td>
<td>Oracle Configured Databases- Database Version = '10''</td>
</tr>
<tr>
<td>All Oracle 8i Databases</td>
<td>Oracle Configured Databases- Database Version = '8''</td>
</tr>
<tr>
<td>All Oracle 11g Databases</td>
<td>Oracle Configured Databases- Database Version = '11''</td>
</tr>
<tr>
<td>All Oracle installations on UNIX Machines</td>
<td>Oracle Configured Databases- OS Type = 'UNIX' or Oracle Configured Servers- OS Type='UNIX'</td>
</tr>
<tr>
<td>All Oracle installations on Windows Machines</td>
<td>Oracle Configured Databases- OS Type = 'Windows' or Oracle Configured Servers- OS Type='Windows'</td>
</tr>
<tr>
<td>All Oracle objects</td>
<td>-</td>
</tr>
<tr>
<td>All Oracle Databases</td>
<td>-</td>
</tr>
</tbody>
</table>

The predefined asset groups for the SQL platform are as follows:
### Table 5-45  Predefined asset groups for the SQL platform

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All SQL Server 7 Instances</td>
<td>SQL Server- Major Version = '7'</td>
</tr>
<tr>
<td>All SQL Server 2005 Instances</td>
<td>SQL Server- Major Version = '9'</td>
</tr>
<tr>
<td>All SQL Server Instances</td>
<td></td>
</tr>
<tr>
<td>All SQL Server 2000 Instances</td>
<td>SQL Server- Major Version = '8'</td>
</tr>
<tr>
<td>All SQL Server 2008 Instances</td>
<td>SQL Server- Major Version = '10'</td>
</tr>
</tbody>
</table>

### Table 5-46  Predefined asset groups for the UNIX platform

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All UNIX Servers</td>
<td></td>
</tr>
<tr>
<td>AIX 5.1 Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;AIX&quot;' and UNIX Machine- Operating System Version= '5.1'</td>
</tr>
<tr>
<td>Sun Solaris Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;SunOS&quot;'</td>
</tr>
<tr>
<td>Red Hat Linux Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Red Hat Linux&quot;'</td>
</tr>
<tr>
<td>AIX 5.2 Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;AIX&quot;' and UNIX Machine- Operating System Version= '5.2'</td>
</tr>
<tr>
<td>Red Hat Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Red Hat&quot;'</td>
</tr>
<tr>
<td>All AIX Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;AIX&quot;'</td>
</tr>
<tr>
<td>Group name</td>
<td>Filter / Definition of the dynamic group</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AIX 5.3 Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;AIX&quot; and UNIX Machine-Operating System Version = '5.3'</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;Red Hat Enterprise Linux&quot;</td>
</tr>
<tr>
<td>SuSE Linux Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;SuSE Linux&quot; and Not UNIX Machine-Operating Distribution Field =&quot;SuSE Linux Enterprise Server&quot;</td>
</tr>
<tr>
<td>HP-UX Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;HP-UX&quot;</td>
</tr>
<tr>
<td>SuSE Enterprise Linux Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;SuSE Linux Enterprise Server&quot;</td>
</tr>
<tr>
<td>All SuSE Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;SuSE&quot;</td>
</tr>
<tr>
<td>AIX 6.1 Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;AIX&quot; and UNIX Machine-Operating System Version = '6.1'</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 2.1 Servers</td>
<td>UNIX Machine-Operating Distribution Field =&quot;Red Hat Enterprise Linux&quot; and UNIX Machine-Operating System Version = '2.1'</td>
</tr>
</tbody>
</table>
Table 5-46  Predefined asset groups for the UNIX platform (continued)

<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 3.0 Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Red Hat Enterprise Linux&quot; and UNIX Machine- Operating System Version = '3.0'</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 4.0 Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Red Hat Enterprise Linux&quot; and UNIX Machine- Operating System Version = '4.0'</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.0 Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Red Hat Enterprise Linux&quot; and UNIX Machine- Operating System Version = '5.0'</td>
</tr>
<tr>
<td>VMware ESX 3 Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Vmware ESX&quot; and UNIX Machine- Operating System Version = '3'</td>
</tr>
<tr>
<td>VMware ESX 3.5 Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Vmware ESX&quot; and UNIX Machine- Operating System Version = '3.5'</td>
</tr>
<tr>
<td>VMware ESX Servers</td>
<td>UNIX Machine- Operating Distribution Field =&quot;Vmware ESX&quot;</td>
</tr>
</tbody>
</table>

The predefined asset groups for the Windows platform are as follows:
<table>
<thead>
<tr>
<th>Group name</th>
<th>Filter / Definition of the dynamic group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Domain Controllers</td>
<td>Windows Machine - Machine Is Server= 'True'</td>
</tr>
<tr>
<td></td>
<td>and</td>
</tr>
<tr>
<td></td>
<td>(Windows Machine - Machine Is PDC= 'True')</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Windows Machine - Machine Is BDC= 'True'</td>
</tr>
<tr>
<td>Windows Backup Domain Controllers</td>
<td>Windows Machine- Machine Is BDC= 'True'</td>
</tr>
<tr>
<td>Windows 2003 Machines</td>
<td>Windows Machine- OS Major Version Number= '5'</td>
</tr>
<tr>
<td></td>
<td>and</td>
</tr>
<tr>
<td></td>
<td>Windows Machine OS Minor Version Number= '2'</td>
</tr>
<tr>
<td>All IIS Web Sites</td>
<td>IIS Web Site - Name Equal To(=) &quot;**&quot;</td>
</tr>
<tr>
<td></td>
<td>or IIS Web Site- ADSI Path Equal To(=) &quot;**&quot;</td>
</tr>
<tr>
<td>Windows XP Machines</td>
<td>Windows Machine- OS Major Version Number= '5'</td>
</tr>
<tr>
<td></td>
<td>and</td>
</tr>
<tr>
<td></td>
<td>Windows Machine OS Minor Version Number= '1'</td>
</tr>
<tr>
<td>Windows Primary Domain Controllers</td>
<td>(Windows Machine- Machine Is PDC= 'True')</td>
</tr>
<tr>
<td>Windows 2000 Professional</td>
<td>Windows Machine - OS Type= 'Windows 2000 Professional'</td>
</tr>
<tr>
<td>Windows Workstations</td>
<td>Windows Machine - Machine Is Server= 'False'</td>
</tr>
<tr>
<td>All Windows Machines</td>
<td>-</td>
</tr>
<tr>
<td>Group name</td>
<td>Filter / Definition of the dynamic group</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows 2000 Servers</td>
<td>Windows Machine-OS Type='Windows 2000<em>Server'</em></td>
</tr>
<tr>
<td>Windows Servers</td>
<td>Windows Machine-Machine Is Server='True'</td>
</tr>
<tr>
<td>Windows NT 4.x Machines</td>
<td>Windows Machine - OS Major Version Number = '4'</td>
</tr>
<tr>
<td>Windows 2008 Machines</td>
<td>Windows Machine - Machine Is Server Equal To(=) 'True' and Windows Machine - OS Major Version Number Equal To (=) '6' and Windows Machine - OS Minor Version Number Equal To (=)'0'</td>
</tr>
<tr>
<td>All IIS Virtual Directories</td>
<td>IIS Virtual Directory - ADSI Path Equal To(=) '*'</td>
</tr>
<tr>
<td>Windows 2000 Machines</td>
<td>Windows Machine- OS Major Version Number= '5' and Windows Machine OS Minor Version Number= '0'</td>
</tr>
<tr>
<td>Windows 2008 R2 Machine</td>
<td>Windows Machine-</td>
</tr>
</tbody>
</table>

See “Creating a dynamic asset group” on page 370.
See “Creating a static asset group” on page 372.
See “Editing an asset group” on page 376.
**Active assets**

The active assets are the assets that are created or updated in the past six months. The Asset System view displays the number of active assets in the top right corner of the table pane.

You can configure the period for which the active assets should be displayed. You can specify the number of days for which the active assets should be displayed in the ActiveAssetsConfig.xml. The XML can be found at the `<installdir>\CCS\Reporting And Analytics\Applications\AssetSystem`.

The active assets are displayed only for the following asset types:

- Windows Machines
- UNIX Machines
- ESM Agents

**Creating reconciliation rules**

The asset reconciliation helps you organize the assets that already exist in the asset store in a logical hierarchy. Reconciliation provides you the flexibility to manage the asset records conditionally when the records get into the assets system.

You can use the reconciliation rules to facilitate the process to add the assets to the asset system. You use the reconciliation rules to update the field values of the existing assets too.

See “Asset reconciliation” on page 295.

See “Creating reconciliation rules using the manual review” on page 307.

See “Creating reconciliation rules without manual review” on page 306.

See “Using a Pre rule to set the values of the common fields” on page 309.

**Creating reconciliation rules without manual review**

The creation of reconciliation rules is a crucial step in the asset system workflow. You can create the reconciliation rules with the use of the Create or Edit Reconciliation Rules wizard.

**To create reconciliation rules**

1. Go to Manage > Assets > Reconciliation Rules.
2. On the taskbar, click **Create Rule**.
3. In the **Specify Rule Details** panel of the **Create Reconciliation Wizard**, type the rule name and select the rule type.
You can select from the following rule types:

- Pre rule
- Add rule
- Update rule
- Post rule

See “Reconciliation rules and rule types” on page 276.

4 Select the asset type to associate the rule with.

You can also create the reconciliation rule for all the asset types.

5 Select the folder to save the reconciliation rule in.

6 Type the description for the reconciliation rule and click Next.

7 In the Select Rule Conditions and Actions panel, click the Add Condition.

8 In the Add Condition dialog box, select a condition from the drop-down list and click OK.

9 In the Select Rule Conditions and Actions panel, click Add Action.

10 In the Add Action dialog box, select an action that should be performed on the imported asset when it meets the specified condition and click OK.

11 Click Next in the Select Rule Conditions and Actions panel after you set the condition and the action.

12 In the Summary panel, review the rule and click Finish.

You can choose to go back and edit the rule any time.

See “Creating reconciliation rules using the manual review” on page 307.

See “Working with reconciliation rules scenarios” on page 308.

See “Quick start with minimum configuration” on page 76.

Creating reconciliation rules using the manual review

Manual review is the process of manually reviewing the assets that are imported into the system by an import job.

See “Manual review” on page 295.

The assets are added into the asset system with the Add Rule. The field values for the newly imported assets are updated in the asset system with the Update Rule.

See “Reconciliation rules and rule types” on page 276.
The Add and the Update type of reconciliation rules let you mark the assets for manual review.

**To create a reconciliation rule using the manual review**

1. Go to Manage > Assets > Reconciliation Rules.
2. On the taskbar, click **Create Rule**.
3. In the **Specify Rule Details** panel, type the rule name and select the rule type.

To mark the assets to add to the manual review store, you can select from the following rule types:

- Add rule
- Update rule

4. Select the asset type to associate the rule with.
   You can also create the reconciliation rule for all the asset types.

5. Select the folder to save the reconciliation rule in.

6. Type the description for the reconciliation rule and click **Next**.

7. In the **Select Rule Conditions and Actions** panel, click the **Add Condition** icon.

8. In the **Add Condition** dialog box, select a condition from the drop-down list and click **OK**.

9. In the **Select Rule Conditions and Action** panel, click the Add Action icon.

10. In the **Add Action** dialog box, select **Add to manual review store** and click **OK**.

11. In the **Select Rule Conditions and Actions** panel, click **Next**.

12. In the **Summary** panel, review the rule and click **Finish**.

   You can choose to go back and edit the rule at any time.

See “**Viewing the manual review records**” on page 368.
See “**Working with reconciliation rules scenarios**” on page 308.
See “**Creating reconciliation rules without manual review**” on page 306.

**Working with reconciliation rules scenarios**

The reconciliation rules help you handle the situations of organizing the assets effectively in the asset system.

Go through the following scenarios to learn how reconciliation rules work:
Using a Pre rule to set the values of the common fields
See “Using a Pre rule to set the values of the common fields” on page 309.

Using an Add rule to dynamically create asset folders
See “Using an Add rule to dynamically create asset folders” on page 310.

Using an Update rule to update the existing field values
See “Using an Update rule to update the existing field values” on page 311.

Using a Post rule to dynamically create folders and move assets to the folders
See “Using a Post rule to mark the assets as control points” on page 312.

Using a Pre rule to set the values of the common fields

Pre rule is the rule that is executed before the assets are added to the asset system. Use the Pre rule to discard the asset before it is added to the asset system or to set the values of the fields before the asset is added. The asset system provides a Predefined rule that sets the values of the Confidentiality, Integrity, and Availability fields to NotDefined. The rule is applicable to all the asset types.

See “Common fields for all asset types” on page 345.

Similarly, you can create a Pre Rule to set the values of the common fields.

Consider the following scenario:

Assume, that you want to set the name of the asset owner as xyz before the asset is added to the asset system.

To set the values of the common fields

1. Go to Manage > Reconciliation Rules.
2. From the taskbar, select Create Rule.
3. In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.
4. From the Rule type drop-down list, select Pre Rule.
5. From the Asset type drop-down list select the asset type for which you want to create the rule.
6. In the Save in box, browse and select the folder where you want to save the rule and click Next.
7. In the Select Rule Conditions and Actions panel, select Add Condition.
8. In the Add Condition dialog box, select If an asset being imported exists in the asset system and click OK.
9. In the Select Rule Condition and Actions panel, select Add Action.
10 In the Add Action dialog box, select **Set the field value of an existing asset as specified**.

Select the field **Asset Owner** and type the value **xyz** and click **OK**.

11 Click **Finish** in the Summary panel.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See “Using an Add rule to dynamically create asset folders” on page 310.
See “Using an Update rule to update the existing field values” on page 311.
See “Using a Post rule to mark the assets as control points” on page 312.

**Using an Add rule to dynamically create asset folders**

Add rule is the rule that lets you add the assets to the asset system in a specified folder. The Add rule is executed on the assets that are being imported. You can also create folders dynamically based on the common field values of the assets.

Consider the following scenario:

Assume that you want to categorize the assets of the Oracle Configured Databases based on the name of the database. The Add rule lets you create the folders dynamically based on the field value. The assets are then added to the folder that is created based on the field value.

**To create asset folders dynamically with an Add rule**

1 Go to Manage > Reconciliation Rules.
2 From the taskbar, select **Create Rule**.
3 In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.
4 From the Rule type drop-down list, select **Add Rule**.
5 From the Asset type drop-down list select **Oracle Configured Databases**.
6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.
7 In the Select Rule Conditions and Actions panel, select **Add Condition**.
8 In the Add Condition dialog box, select **If an asset being imported does not exist in the asset system** and click **OK**.
9 In the Select Rule Condition and Actions panel, select **Add Action**.
10 In the Add Action dialog box, select **Add an asset being imported to the specified folder**.

   Click the Browse (...) icon and click **New** in the Select Folder dialog box.

   In the Custom Folder dialog box, select **Folder based on field value**.

   In the Fields list, select **Database Name** and click **OK**.

   Click **OK** in the Select Folder dialog box and click **Next** in the Specify Rule Conditions and Actions panel.

11 Click **Finish** in the Summary panel.

   If you add this rule to the asset import job for the Oracle Configured Databases, different folders are created with the name of the databases and the assets are added to the proper folders.

   Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See “**Using a Pre rule to set the values of the common fields**” on page 309.

See “**Using an Update rule to update the existing field values**” on page 311.

See “**Using a Post rule to mark the assets as control points**” on page 312.

**Using an Update rule to update the existing field values**

The Update rule lets you update the field values of the existing assets with new values. The Update rule is executed on the existing assets during an asset import job to check the existing field values.

Consider the following scenario:

Assume that the Operating System of the assets in your enterprise that belongs to the Finance Department, changes from Windows to Linux. You have the asset group based on the tag,, Finance Department. The Update rule lets you update the value of the operating system field.

To **update the existing field value with an update rule**

1 Go to Manage > Reconciliation Rules.

2 From the taskbar, select **Create Rule**.

3 In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.

4 From the Rule type drop-down list, select **Add Rule**.

5 From the Asset type drop-down list select **Windows Machine**.
Creating reconciliation rules

6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.

7 In the Select Rule Conditions and Actions panel, select **Add Condition**.

8 In the Add Condition dialog box, select **If an asset being imported exists in the asset system** and click **OK**.

9 In the Select Rule Condition and Actions panel, select **Add Action**.

10 In the Add Action dialog box, select **Set the field value of an existing asset as specified**.

   In the Fields list, select **OS Type**.

   In the Value box, type **Linux** and click **OK**.

11 Click **Finish** in the Summary panel.

   Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See “Using a Pre rule to set the values of the common fields” on page 309.

See “Using an Add rule to dynamically create asset folders” on page 310.

See “Using an Update rule to update the existing field values” on page 311.

**Using a Post rule to mark the assets as control points**

The Post rule lets you move an asset to a specified folder after the asset is added to the asset system. The Post rule is executed on the assets that are already a part of the asset system.

Consider the following scenario:

Assume that you have imported the assets for the Oracle Configured Databases. You want to mark all the assets as control points. You can create a Post rule to mark the assets for Oracle Configured Databases as control points.

**To create folders dynamically and move assets to the folders**

1 Go to Manage > Reconciliation Rules.

2 From the taskbar, select **Create Rule**.

3 In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.

4 From the Rule type drop-down list, select **Post Rule**.

5 From the Asset type drop-down list select **Oracle Configured Database**.

6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.
7. In the Select Rule Conditions and Actions panel, select Add Condition.

8. In the Add Condition dialog box, select If an asset being imported exists in the asset system and click OK.

9. In the Select Rule Condition and Actions panel, select Add Action.

10. In the Add Action dialog box, select Mark an existing asset as control point. Click OK and click Next in the Specify Rule Conditions and Actions panel.

11. Click Finish in the Summary panel.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See “Using a Pre rule to set the values of the common fields” on page 309.

See “Using an Add rule to dynamically create asset folders” on page 310.

See “Using an Update rule to update the existing field values” on page 311.

---

**Importing assets**

In the asset system, asset import involves the import of the following data:

- Data for the asset-specific fields
  Asset-specific fields are the fields that are specific to the asset type that you select to import.
  See “Predefined asset types” on page 236.

- Data for the common fields
  Common fields are the fields that are common across all the asset types.
  See “Common fields for all asset types” on page 345.

To import assets, you must select either a default data collector, CSV data collector, or an ODBC data collector.
### How data collectors work in asset import

<table>
<thead>
<tr>
<th>Selected data collector</th>
<th>How the data collector works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Asset import from default data collector involves the import from the data collection components as well as the CSV data collector.</td>
</tr>
<tr>
<td></td>
<td>■ The default data collector gathers the information about the asset-specific fields from the data collection components in the Control Compliance Suite.</td>
</tr>
<tr>
<td></td>
<td>■ A data collection component is assigned to the import query internally, depending on the platform for which the asset import should be performed. A separate data collector is assigned to each platform for data collection. The data collection components are, Windows data collector, UNIX data collector, SQL data collector, Oracle data collector, ESM data collector, Exchange data collector, NDS data collector, and NetWare data collector.</td>
</tr>
<tr>
<td></td>
<td>■ Note: For custom platforms, if you select CSV or ODBC data collector during entity schema creation, then the selected data collector becomes the default data collector.</td>
</tr>
<tr>
<td></td>
<td>■ The default data collector gathers information about the common fields from the CSV.</td>
</tr>
<tr>
<td></td>
<td>■ The data for the common fields is imported from the Common platform. You must configure the Common platform with a CSV share to import the data for the common fields of the assets.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring Common platform through CSV settings” on page 326.</td>
</tr>
<tr>
<td>Selected data collector</td>
<td>How the data collector works</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>CSV</td>
<td>■ The CSV data collector gathers the information about the asset-specific fields from a CSV file.</td>
</tr>
<tr>
<td></td>
<td>■ The CSV data collector reads from the CSV files that are specific to platforms. You must create different CSV files for different platforms, if you want to import the asset-specific fields data from the CSV file.</td>
</tr>
<tr>
<td></td>
<td>■ In addition to the CSV file specific to the platform, you also need the CSV file that is configured for the Common platform to import the information about the common fields.</td>
</tr>
<tr>
<td></td>
<td>To know more about configuring the CSV data collector, click on the following link: See “Configuring the CSV data collector” on page 156.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring Common platform through CSV settings” on page 326.</td>
</tr>
<tr>
<td>ODBC</td>
<td>The ODBC data collector gathers information about the asset-specific fields that are defined in the table columns of the ODBC databases. The ODBC data collector collects both asset-specific and common fields data that are defined for the asset in the database tables.</td>
</tr>
<tr>
<td></td>
<td>To know more about configuring the ODBC data collector, click on the following link: See “Configuring the ODBC data collector” on page 158.</td>
</tr>
<tr>
<td></td>
<td>The ODBC data collector reads data from the configured tables of the ODBC compliant databases. The database tables are configured for different platforms as per the entity schema. You must define the table names and the table column names appropriately as per the entity schema for successful data collection.</td>
</tr>
</tbody>
</table>

See “Importing the assets for the first time” on page 319.

See “Importing asset-specific fields from the default data collector” on page 329.
See “Importing asset-specific and common fields using the default data collector” on page 332.

See “Importing asset-specific and common fields using the CSV data collector” on page 335.

See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338.

About the first time asset import

The first time asset import implies the asset import on the first day after you install and configure Control Compliance Suite.

Before you import the assets for the first time, you must review the following concepts that are related to asset import.

■ Predefined platforms
  See “Predefined platforms” on page 235.

■ Predefined asset types
  See “Predefined asset types” on page 236.

■ Primary and secondary assets
  See “Primary and secondary assets” on page 275.

■ Default data collectors for the supported platforms
  See “Default data collectors” on page 288.

■ Working of the default data collector in asset import
  See “About the working of default data collectors in asset import” on page 322.

■ Working of the CSV data collector in asset import
  See “About the working of CSV data collector in asset import” on page 324.

When you import the assets for the first time, you import the primary assets into the asset system.

Note: You might not have the Common platform configured through the CSV settings when you import the assets for the first time. In this case, the asset import job does not import the data for the common fields. You must have at least one data collector configured.

See “Configuring Common platform through CSV settings” on page 326.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch the Create or Edit Asset Import Job wizard</td>
<td>Go to Manage &gt; Assets &gt; Asset System &gt; Import Assets to launch the Create or Edit Asset Import Job wizard.</td>
</tr>
<tr>
<td>Identify the primary assets to be imported</td>
<td>You must first identify the type of assets that you want to import and then identify the primary assets for the asset type that should be imported first. For example, if you want to import the Windows Files, you must first import the Windows Machines. To import the Windows Machines, you must first import the Windows Domain. <strong>Note:</strong> You can import the primary assets only for the data collector that you have configured. For example, if you have installed the bv-Control for Windows for data collection, you can import only Windows assets. See “Primary and secondary assets” on page 275.</td>
</tr>
<tr>
<td>Select the scope to import the assets</td>
<td>You must select the correct scope to import the assets. After you identify the primary assets to import, you can select the correct scope. It is recommended that you select the default scope. See “About scopes in asset import” on page 349. See “Default scope and supported scope” on page 351.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Select the Add Rule from the predefined reconciliation rules</td>
<td>You can use the Add rule from the predefined reconciliation rules when you import the assets for the first time. The Add rule checks if the asset that is being imported is already in the asset system. If the asset is not in the asset system, the Add rule adds the asset to the asset system. See “Predefined reconciliation rules” on page 284.</td>
</tr>
<tr>
<td>Complete the Create or Edit Asset Import Wizard</td>
<td>You need not create any asset field filters when you import the assets for the first time. After you add the reconciliation rules, you can proceed through the Create or Edit Asset Import Job wizard till the Summary page. Make sure that you select the Run Now option in the Schedule panel to run the import job immediately.</td>
</tr>
<tr>
<td>Monitor the job status</td>
<td>You can monitor the status of the asset import job from the Jobs view. Go to Manage &gt; Jobs to monitor the status.</td>
</tr>
<tr>
<td>View the assets in the asset system</td>
<td>After the asset import job completes, you can view the primary assets in the asset system. Go to Manage &gt; Assets &gt; Asset System You can use the Display filter in the table pane and select the asset type for which you have created the import job. The assets for the selected asset type are displayed in the table pane.</td>
</tr>
</tbody>
</table>
**Table 5-49  First time asset import steps (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the common field values with the reconciliation rules</td>
<td>The asset import job on the first day does not import the common fields if the Common platform is not configured through CSV settings. You can set the values of the common fields with the reconciliation rules after the asset import job. See “Using a Pre rule to set the values of the common fields” on page 309.</td>
</tr>
</tbody>
</table>

See “Importing the assets for the first time” on page 319.

**Importing the assets for the first time**

When you import the assets into the asset system for the first time, the scenario can be as follows:

- You have a DPS registered to a site.
- You have at least one data collector configured. The configuration of the CSV data collector and the configuration of the Common platform through CSV settings are optional.
- You have identified the asset type for which you want to import the assets.
- You have at least one Add rule created through the reconciliation rule to add the assets of the identified asset type in the system. See “Creating reconciliation rules without manual review” on page 306. If you do not have any custom rule, you can use the Add rule from the predefined rules. See “Predefined reconciliation rules” on page 284.

**Note:** On the first day, if you do not have the CSV data collector configured, the data for the fields that are common across all asset types is not imported. You can set the common fields data later using the reconciliation rules. See “Using a Pre rule to set the values of the common fields” on page 309.

The asset import involves the following steps:

- Creating an asset import job
Executing the asset import job

To import the assets for the first time

1. Go to Manage > Assets > Asset System.
2. On the taskbar, from the Asset Tasks select Import Assets.
3. In the Specify Name and Description panel, in the Name box, type the name for the import job.
   You can optionally type the description for the import job and click Next.
4. In the Select Platform, Asset Type, and Data Collector panel, select the platform and the asset type to import the assets.
5. In the Select Platform, Asset Type, and Data Collector panel, from the Asset Source drop-down list, select Default and click Next.
   See “About the working of default data collectors in asset import” on page 322.
6. In the Select Asset Import Scope panel, select the default scope with the Add option and click Next.
   See “About scopes in asset import” on page 349.
   Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.
   Click Browse (...) to view and select the scope.
   In the Limit Asset Import Scope dialog box, you can select the additional scope from the list of the supported scopes and click OK.
   See “Default scope and supported scope” on page 351.
7. In the Add Reconciliation Rules panel, click Add Rules.
8. In the Select Reconciliation Rules panel, from the left pane, navigate to Reconciliation Rules > predefined rules.
   In the right pane, select Add asset to the Asset System and click Add. Click OK.
   The rule adds all the assets to the asset system.
   See “Predefined reconciliation rules” on page 284.
9. In the Specify Asset Field Filters panel click Next.
   You do not need to filter the assets with the field filters when you import the assets for the first time.
10. In the Schedule panel, click Run now.
11 In the **Specify Notification Details** panel, if you want to send the notification of job completion or job failure, do the following:

- Type the subject and message of the notification mail.
- Type the email ID of the sender and the receiver.

12 In the **Summary** panel, review the configurations for the import job and click **Finish**.

Go to the Monitor > Jobs view to monitor the current status of the job.

See “About the first time asset import” on page 316.

See “Quick start with minimum configuration” on page 76.

### Working with asset import scenarios

After you import the primary assets on day zero, you can proceed with the creation of further asset import jobs for the secondary assets.

See “About the first time asset import” on page 316.

<table>
<thead>
<tr>
<th>Data collector</th>
<th>Asset import scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default data collector</td>
<td>The scenarios are as follows:</td>
</tr>
<tr>
<td>See “About the working of default data collectors in asset import” on page 322.</td>
<td></td>
</tr>
</tbody>
</table>

- To import the asset-specific fields
  See “Importing asset-specific fields from the default data collector” on page 329.

- To import the asset-specific and common fields
  See “Importing asset-specific and common fields using the default data collector” on page 332.

The import of common fields from the default data collector involves the configuration of CSV data collector for Common platform.

See “Configuring Common platform through CSV settings” on page 326.
Table 5-50  
Asset import scenarios (continued)

<table>
<thead>
<tr>
<th>Data collector</th>
<th>Asset import objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV data collector</td>
<td>The scenarios are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ To import the asset-specific and common fields from the CSV data collector</td>
</tr>
<tr>
<td></td>
<td>See “Importing asset-specific and common fields using the CSV data collector” on page 335.</td>
</tr>
<tr>
<td></td>
<td>■ To import the custom asset-specific fields and common fields from the CSV data collector</td>
</tr>
<tr>
<td></td>
<td>See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338.</td>
</tr>
<tr>
<td></td>
<td>■ To import only the specific assets manually, only once.</td>
</tr>
<tr>
<td></td>
<td>See “Importing specific assets manually only once from the CSV file” on page 359.</td>
</tr>
<tr>
<td>ODBC data collector</td>
<td>The scenario is as follows:</td>
</tr>
<tr>
<td></td>
<td>■ To import the asset-specific and common fields from the ODBC data collector</td>
</tr>
<tr>
<td></td>
<td>See “Importing asset-specific and common fields using the ODBC data collector”</td>
</tr>
<tr>
<td></td>
<td>■ To import the custom asset-specific fields and common fields from the ODBC data collector</td>
</tr>
</tbody>
</table>

About the working of default data collectors in asset import

To import the assets in the asset system, you select a data collector. You can select a default data collector, a CSV data collector, or an ODBC data collector.

See “Data collectors and asset types” on page 289.

The default data collector imports the data for the asset fields that are specific to the asset type from the data collection components. A data collection component is internally assigned to the import query based on the selected platform to collect the asset-specific data.
Table 5-51  Platform and data collectors

<table>
<thead>
<tr>
<th>Platform</th>
<th>Data collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM platform</td>
<td>ESM data collector</td>
</tr>
<tr>
<td>Oracle platform</td>
<td>Oracle data collector</td>
</tr>
<tr>
<td>SQL platform</td>
<td>SQL data collector</td>
</tr>
<tr>
<td>UNIX platform</td>
<td>UNIX data collector</td>
</tr>
<tr>
<td>Windows platform</td>
<td>Windows data collector</td>
</tr>
<tr>
<td>Exchange platform</td>
<td>Exchange data collector</td>
</tr>
<tr>
<td>NDS platform</td>
<td>NDS data collector</td>
</tr>
<tr>
<td>NetWare platform</td>
<td>NetWare data collector</td>
</tr>
</tbody>
</table>
| Custom platform of a custom application | You can use the following to collect data from the custom platforms:  
  - CSV data collector  
  - ODBC data collector |
| Note: For custom platforms, if you select CSV or ODBC data collector during the entity schema creation, then the selected data collector becomes the default data collector. When importing assets of the custom platform, the option, Default appears in the drop-down list of the Create or Edit Asset Import wizard. |
| Common platform    | You can use any of the following data collectors to import the common fields:  
  - CSV data collector  
  - ODBC data collector |
| The Common platform is the platform that is used to import the common fields across the asset types. |
| By default, the CSV data collector is used to import the common fields of the Common platform. |

Consider the following example:

You select Oracle Configured Servers as the asset type and select the default data collector. The default data collector imports the data for the fields like Server Name, Server NetBIOS Name, Windows Domain Name or UNIX IP Address, OS Type. These fields are specific to the Oracle Configured Servers asset type.
The default data collector imports the data for the common fields from the CSV data collector. To import the data for the common fields of the selected asset type, you must configure the Common platform through CSV settings.

See “Configuring Common platform through CSV settings” on page 326.

See “Importing the assets for the first time” on page 319.

See “Importing asset-specific fields from the default data collector” on page 329.

See “Importing asset-specific and common fields using the default data collector” on page 332.

### About the working of CSV data collector in asset import

To import the assets in the asset system, you select a data collector. You can select a default data collector, a CSV data collector, or an ODBC data collector.

See “Data collectors and asset types” on page 289.

#### Table 5-52 Role of CSV data collector

<table>
<thead>
<tr>
<th>Role of the CSV data collector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To import the data of a predefined platform and you explicitly select the CSV data collector for asset import.</td>
<td>To import the entire data in case you explicitly select the CSV data collector for asset import.</td>
</tr>
<tr>
<td>In this case, the data for the asset-specific fields and for the common fields, is imported from the CSV data collector.</td>
<td></td>
</tr>
<tr>
<td>If you want to import the entire asset data from the CSV data collector, you need to create a CSV file with a specific format.</td>
<td></td>
</tr>
<tr>
<td>After you create the CSV file, you need to configure the CSV data collector.</td>
<td></td>
</tr>
<tr>
<td>See “Importing asset-specific and common fields using the CSV data collector” on page 335.</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-52  Role of CSV data collector (continued)

<table>
<thead>
<tr>
<th>Role of the CSV data collector</th>
<th>Description</th>
</tr>
</thead>
</table>
| To import the data for the common fields even if you select the Default data collector for asset import. | To import the data for the common fields even if you select the Default data collector for asset import.  
In this case, the data for the common fields only is imported from the CSV data collector. The default data collector imports the data for the asset-specific fields.  
To import the data for the common fields, you must configure the Common platform through CSV settings.  
See “Configuring Common platform through CSV settings” on page 326.  
See “About the working of default data collectors in asset import” on page 322. |
| To import the data in case you import the data for the custom asset type. | In this case, the CSV data collector becomes the default data collector.  
See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338. |

See “Creating a CSV file for custom application” on page 357.

See “Configuring the CSV data collector” on page 156.

**About the working of the ODBC data collector in asset import**

To import the assets in the asset system, you select a data collector. You can select a default data collector, a CSV data collector, or an ODBC data collector.

See “Data collectors and asset types” on page 289.
Table 5-53  Role of an ODBC data collector

<table>
<thead>
<tr>
<th>Role of the ODBC data collector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To import the data of a predefined or custom platform and you explicitly select the ODBC data collector for asset import.</td>
<td>To import the entire data of an asset and you explicitly select the ODBC data collector for asset import. In this case, the data for the asset-specific fields and the common fields, are imported by the ODBC data collector. See “Importing asset-specific and common fields using the ODBC data collector” on page 341.</td>
</tr>
<tr>
<td>To import the data for the common fields and you select ODBC data collector for asset import.</td>
<td>By default, data for the common fields are collected from the CSV files using the CSV data collector. If you want to collect data for the common fields using the ODBC data collector, then switch the CSV to ODBC data collector. See “Switching between CSV and ODBC data collectors” on page 161. To import the data for the common fields, you must configure the Common platform through the ODBC settings. See “Configuring Common platform through ODBC settings” on page 328.</td>
</tr>
</tbody>
</table>

Configuring Common platform through CSV settings

In Control Compliance Suite, the default data collector does not collect the data for the common fields such as Confidentiality, Integrity, Availability and so on. To collect data for the common fields, you must manually create a CSV file and define all the common fields in a specific format. You must then configure a DPS as a CSV data collector to collect data for the common fields of the predefined asset type. So, to import the predefined asset types even if you select a default data collector you still require a CSV data collector to collect the common fields data.

The overall sequence to collect data for the common fields of an asset type are as follows:

- Export the data fields of an asset type into a CSV file.
Create a CSV file that contains the data for the common fields. See “Common fields for all asset types” on page 345. Ensure that you know the primary fields of the predefined asset type for which the common fields are to be specified in the CSV file. The primary fields are asset type identifiers that are used to map the common fields of the asset type correctly. For example, for the predefined asset type, Windows directory of the predefined platform, you must know the primary fields, Host and DomainName. See “Predefined asset types” on page 236.

Configure the CSV data collector. See “Configuring the CSV data collector” on page 156.

**Note:** Ensure that you select the platform, Common in the **Edit Settings** dialog box for configuring the CSV data collector.

Import the asset type using the Asset Import wizard. See “About the working of default data collectors in asset import” on page 322.

**To create and configure the common fields of an asset type through CSV settings**

1. Select the platform and the asset type for which the common fields must be defined.

2. Get the primary fields of the asset type. If you want to specify the common fields of the predefined asset types, then you must know the primary fields of those asset types. See “Predefined asset types” on page 236.
3 Create a CSV file with headers in the following format:

```
<platform.entity.primaryfield1>, <platform.entity.primaryfield2>,
<Common.platform.entity.baseattributefield1>,
<Common.platform.entity.baseattributefield2>
```

For example, for the common fields of a predefined asset type, Windows directory, the CSV file headers are as follows:

```
Wnt.Domain.DomainName, Wnt.Domain.Host,
Common.WntDomain.Confidentiality, Common.WntDomain.Integrity,...
```

Here, DomainName and Host are the primary fields of the predefined asset type and Wnt is the platform.

For an asset type, it is important that you ensure the correct correlation between the primary fields and the common fields. The data of the common fields correspond to the assets, whose unique identifiers are the primary fields.

For example, for an asset type, Windows directory, the data representation for the primary and common fields in the CSV file are as follows:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TestDomain</td>
<td>Test1Machine</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>TestDomain</td>
<td>Test2Machine</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

As per the example, common fields data for the assets, Test1Machine and Test2Machine are collected.

4 Place the CSV file in the network share path of the Windows computer.

5 In the console, go to **System Topology > Grid View** and configure the DPS as CSV data collector.

See “Configuring the CSV data collector” on page 156.

6 In the console, go to Settings > System Topology > Map View and click **Infrastructure Tasks > Sync Configuration**.

**Configuring Common platform through ODBC settings**

In Control Compliance Suite, the default data collector does not collect the data for the common fields such as Confidentiality, Integrity, Availability and so on. To collect data for the common fields, you manually create ODBC database tables
and define all the common fields in a specific format. You must then configure a
DPS as an ODBC data collector to collect data for the common fields of the asset
type. For the predefined asset types, you can either import the common fields
data from a CSV file or from an ODBC database table.

To create and configure the common fields of an asset type through ODBC settings

1 Select the platform and the asset type for which the common fields must be
defined.

2 Get the primary fields of the asset type.

   If you want to specify the common fields of the predefined asset types, then
   you must know the primary fields of those asset types. The primary fields
   are asset type identifiers that are used to map the common fields of the asset
   type correctly. For example, for the predefined asset type, Windows Machine
   of the predefined asset type, you must know the primary fields, Machine
   Name and Domain/Workgroup Name.

   See “Predefined asset types” on page 236.

3 Create an ODBC database table for the common fields of the asset type.

   See “Common fields for all asset types” on page 345.

4 Ensure that the database table or view names and column names are as per
the defined naming conventions.

   See “Format to create ODBC compliant database tables” on page 363.

5 Configure the data locations for connecting to the ODBC database table.

6 Configure a DPS as an ODBC data collector.

   See “Configuring the ODBC data collector” on page 158.

   **Note:** Ensure that you select the platform, Common for the drop-down list,
   Platform in the **Edit Settings** dialog box. You configure the DPS as ODBC data
   collector by specifying the ODBC settings.

7 Import the asset type and the common fields using the Asset Import wizard.

   See “About the working of default data collectors in asset import” on page 322.

Importing asset-specific fields from the default data collector

To import the data for the asset-specific fields from the default data collector is
a simple task.
The import of the asset-specific fields from the default data collector works on the basis of the following assumptions:

■ You select an asset type
■ You select the Default data collector
■ You want to import the data of the fields that are specific to the asset type that you select.

See “About the working of default data collectors in asset import” on page 322.

To import asset-specific fields from the default data collector

1. Go to Manage > Assets > Asset System.
2. On the taskbar, from the Asset Tasks select Import Assets.
3. In the Specify Name and Description panel, in the Name box, type the name for the import job.
   You can optionally type the description for the import job and click Next.
4. In the Select Platform, Asset Type, and Data Collector panel, select the platform and the asset type to import the assets for.
5. In the Select Platform, Asset Type, and Data Collector panel, from the Asset Source drop-down list, select Default and click Next.
   See “About the working of default data collectors in asset import” on page 322.
6. In the Select Asset Import Scope panel, click the ... option to select the scope for the asset type.
   Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.
   Click Browse (...) to view and select the scope.
   In the Limit Asset Import Scope dialog box, you can select the additional scope from the list of the supported scopes and click OK.
   See “About scopes in asset import” on page 349.
7. In the Select Asset Import Scope panel, browse through the assets hierarchy and select a folder to add the assets from. Click Add to add it as a scope and click Next.
8. In the Add Reconciliation Rules panel, you can do one of the following:
   ■ Use the Add Rule option to add a rule to the import job from the existing rules.
     The Add Rule option displays the Select Reconciliation Rules panel.
Use the **Delete Rule** option to delete the rule that is already added and click **Next**.

Use the Move Up and Move Down options to arrange the rules in an order and click **Next**.

9 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.

Click **OK**.

10 In the **Specify Asset Field Filters** panel you can do one of the following:

- Use the **Edit Selected Statement** option to edit the existing filter and click **Next**.
- Use the **Delete Selected Statement** option to delete the existing filter and click **Next**.
- Use the **Add Statement** option to create a new statement.

   Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.

   The **Add Statement** option displays the **Create Filter Statement** dialog box.

11 In the **Create Filter Statement** dialog use the parameter type and the conditions to create a filter statement.

   See “**Examples of asset filters**” on page 292.

   See “**Filter statement operators**” on page 293.

12 In the **Schedule** panel, select any one of the following:

- If you want to run the job after the wizard closes, check **Run now**.
- If you want to run the job at a specified interval, check **Run periodically** and enter the following information:
  - In the **Start On** box, enter the start date and time to run the job.
  - Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the **Run Every Day** list box. Click **Next**.

13 In the **Specify Notification Details** panel, if you want to send the notification of job completion or job failure, do the following:
Type the subject and message of the notification mail.
Type the email ID of the sender and the receiver.

In the Summary panel, review the configurations for the import job and click Finish.
You can go back to the previous panels and edit the configurations any time.
You can go to the Monitor > Jobs view to monitor the current status of the job.
The asset import job can be in one of the following states:

- Custom
  This state indicates that the state of the asset import job run is Awaiting Manual Review.

- Completed
  This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- Executing
  This state indicates that the job is running.

- Awaiting manual review
  This state indicates that the records that are returned by the data collector should be manually reviewed. The job goes into the Awaiting for manual review status, if the reconciliation rule marks the asset for manual review or if the assets do not satisfy any condition in the reconciliation rules. See “Reviewing the assets manually” on page 367.

Importing asset-specific and common fields using the default data collector
If you want to import the asset-specific and common fields from the default data collector, it is mandatory that you configure the Common platform from the CSV settings.

See “Configuring Common platform through CSV settings” on page 326.
See “About the working of default data collectors in asset import” on page 322.
See “About the working of CSV data collector in asset import” on page 324.
You must also ensure that the default data collector for the platform for which you want to import the assets, is configured.

See “Default data collectors” on page 288.
To import asset-specific and common fields from the default data collector

1 Go to Manage > Assets > Asset System.

2 On the taskbar, from the Asset Tasks select Import Assets.

3 In the Specify Name and Description panel, in the Name box, type the name for the import job.
   You can optionally type the description for the import job and click Next.

4 In the Select Platform, Asset Type, and Data Collector panel, select the platform and the asset type to import the assets for.

5 In the Select Platform, Asset Type, and Data Collector panel, from the Asset Source drop-down list, select Default and click Next.
   See “About the working of default data collectors in asset import” on page 322.

6 In the Select Asset Import Scope panel, click the ... option to select the scope for the asset type.
   Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.
   Click Browse (...) to view and select the scope.
   In the Limit Asset Import Scope dialog box, you can select the additional scope from the list of the supported scopes and click OK.
   See “About scopes in asset import” on page 349.

7 In the Select Asset Import Scope panel, browse through the assets hierarchy and select a folder to add the assets from. Click Add to add it as a scope and click Next.

8 In the Add Reconciliation Rules panel, you can do one of the following:
   ■ Use the Add Rules option to add a rule to the import job from the existing rules.
     The Add Rule option displays the Select Reconciliation Rules panel.
   ■ Use the Delete Rule option to delete the rule that is already added and click Next.
   ■ Use the Move Up and Move Down options to arrange the rules in the order and click Next.

9 In the Select Reconciliation Rules panel, browse through the Reconciliation Rules folder and use the Add option to add the existing reconciliation rules to the import job.
   Click OK.

10 In the Specify Asset Field Filters panel you can do one of the following:
Use the Edit Selected Statement option to edit the existing filter and click Next.

Use the Delete Selected Statement option to delete the existing filter and click Next.

Use the Add Statement option to create a new statement. The Add Statement option displays the Create Filter Statement dialog box. Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.

11 In the Create Filter Statement dialog box, use the parameter type and the conditions to create a filter statement. See “Examples of asset filters” on page 292. See “Filter statement operators” on page 293.

12 In the Schedule panel, select any one of the following:

- If you want to run the job after the wizard closes, check Run now.
- If you want to run the job at a specified interval, check Run periodically and enter the following information:
  - In the Start On box, enter the start date and time to run the job.
  - Under Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click Next.

13 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:

- Type the subject and message of the notification mail.
- Type the email ID of the sender and the receiver.

14 In the Summary panel, review the configurations for the import job and click Finish.

You can go back to the previous panels and edit the configurations any time. You can go to the Monitor > Jobs view to monitor the current status of the job.

The asset import job can be in one of the following states:

- Custom
This state indicates that the state of the asset import job run is Awaiting Manual Review.

- Completed
  This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- Executing
  This state indicates that the job is running.

- Awaiting manual review
  This state indicates that the records that are returned by the data collector should be manually reviewed.
  See “Reviewing the assets manually” on page 367.

**Importing asset-specific and common fields using the CSV data collector**

You can use the CSV data collector as any other default data collector to import the assets of a predefined platform.

Before you start using the CSV data collector for asset import, ensure that you have performed the following tasks:

- Create a CSV file in the supported format.
  See “Creating a CSV file for predefined asset types” on page 356.

- Share the CSV file on the computer where you have installed the Control Compliance Suite Console.

Consider the following cases when you share the CSV file:

- You create a single CSV file to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file must be copied at both the locations.

- You create two separate CSV files to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file for the common fields data must be copied to the share location of the common platform and the CSV file for the default platform must be copied to the share location of the default platform.

- Configure the CSV settings for the platform for which you want to import the assets.
  See “Configuring the CSV data collector” on page 156.
To import asset-specific and common fields from the CSV data collector

1. Go to Manage > Assets > Asset System.

2. On the taskbar, from the Asset Tasks select **Import Assets**.

3. In the **Specify Name and Description** panel, in the Name box, type the name for the import job.
   
   You can optionally type the description for the import job and click **Next**.

4. In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type to import the asset.

5. In the **Select Platform, Asset Type, and Data Collector** panel, from the **Asset Source** drop-down list, select **CSV Data Collector** and click **Next**.
   
   See “About the working of CSV data collector in asset import” on page 324.

6. In the **Select Asset Import Scope** panel, click the ... option to select the scope for the asset type.
   
   Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.
   
   Click **Browse (…)** to view and select the scope.
   
   In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.
   
   See “About scopes in asset import” on page 349.

7. In the **Select Asset Import Scope** panel, browse through the assets hierarchy and select a folder to add the assets from. Click **Add** to add it as a scope and click **Next**.

8. In the **Add Reconciliation Rules** panel, you can do one of the following:
   
   - Use the **Add Rules** option to add a rule to the import job from the existing rules.
     
     The Add Rule option displays the Select Reconciliation Rules panel.
   
   - Use the **Delete Rule** option to delete the rule that is already added and click **Next**.
   
   - Use the **Move Up and Move Down** options to arrange the rules in the order and click **Next**.

9. In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.
   
   Click **OK**.

10. In the **Specify Asset Field Filters** panel you can do one of the following:
Use the Edit Selected Statement option to edit the existing filter and click Next.

Use the Delete Selected Statement option to delete the existing filter and click Next.

Use the Add Statement option to create a new statement.
The Add Statement option displays the Create Filter Statement dialog box.
Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.

11 In the Create Filter Statement dialog box, use the parameter type and the conditions to create a filter statement.

See “Examples of asset filters” on page 292.
See “Filter statement operators” on page 293.

12 In the Schedule panel, select any one of the following:

■ If you want to run the job after the wizard closes, check Run now.

■ If you want to run the job at a specified interval, check Run periodically and enter the following information:
  ■ In the Start On box, enter the start date and time to run the job.
  ■ Under Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click Next.

13 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:

■ Type the subject and message of the notification mail.

■ Type the email ID of the sender and the receiver.

14 In the Summary panel, review the configurations for the import job and click Finish.

You can go back to the previous panels and edit the configurations any time.
You can go to the Monitor > Jobs view to monitor the current status of the job.
The asset import job can be in one of the following states:

■ Custom
This state indicates that the state of the asset import job run is Awaiting Manual Review.

- Completed
  This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- Executing
  This state indicates that the job is running.

- Awaiting manual review
  This state indicates that the records that are returned by the data collector should be manually reviewed.
  See “Reviewing the assets manually” on page 367.

**Importing the specific and common fields for custom asset using the CSV data collector**

To import the asset data for the custom asset type, you use the CSV data collector. For the new asset type, CSV data collector works as the default data collector.

See “Default data collectors” on page 288.

Before you start using the CSV data collector for asset import, ensure that you have performed the following tasks:

- Create a CSV file in the supported format.
  See “Creating a CSV file for custom application” on page 357.

- Share the CSV file on the computer where you have installed the Control Compliance Suite Console.

Consider the following cases when you share the CSV file:

- You create a single CSV file to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file must be copied at both the locations.

- You create two separate CSV files to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file for the common fields data must be copied to the share location of the common platform and the CSV file for the default platform must be copied to the share location of the default platform.

- Configure the CSV settings for the platform for which you want to import the assets. You must configure the CSV settings if you have created a new platform. See “Configuring the CSV data collector” on page 156.
To import custom asset-specific and common fields from the CSV data collector

1. Go to Manage > Assets > Asset System.

2. On the taskbar, from the Asset Tasks select **Import Assets**.

3. In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

   You can optionally type the description for the import job and click **Next**.

4. In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type that you have created.

5. In the **Select Platform, Asset Type, and Data Collector** panel, from the **Asset Source** drop-down list, select **CSV Data Collector** and click **Next**.

   See “About the working of CSV data collector in asset import” on page 324.

6. In the Select Asset Import Scope panel, click the ... option to select the scope for the asset type.

   Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.

   Click **Browse (…)** to view and select the scope.

   In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.

   See “About scopes in asset import” on page 349.

7. In the Select Asset Import Scope panel, browse through the assets hierarchy and select a folder to add the assets from. Click **Add** to add it as a scope and click **Next**.

8. In the **Add Reconciliation Rules** panel, you can do one of the following:

   - Use the Add Rules option to add a rule to the import job from the existing rules.
     The Add Rule option displays the Select Reconciliation Rules panel.
   - Use the Delete Rule option to delete the rule that is already added and click **Next**.
   - Use the Move Up and Move Down options to arrange the rules in the order and click **Next**.

9. In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.

   Click **OK**.

10. In the **Specify Asset Field Filters** panel you can do one of the following:
Use the Edit Selected Statement option to edit the existing filter and click Next.

Use the Delete Selected Statement option to delete the existing filter and click Next.

Use the Add Statement option to create a new statement.

The Add Statement option displays the Create Filter Statement dialog box.

Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.

11 In the Create Filter Statement dialog box, use the parameter type and the conditions to create a filter statement.

See “Examples of asset filters” on page 292.

See “Filter statement operators” on page 293.

12 In the Schedule panel, select any one of the following:

- If you want to run the job after the wizard closes, check Run now.

- If you want to run the job at a specified interval, check Run periodically and enter the following information:
  
  - In the Start On box, enter the start date and time to run the job.
  
  - Under Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click Next.

13 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:

- Type the subject and message of the notification mail.

- Type the email ID of the sender and the receiver.

14 In the Summary panel, review the configurations for the import job and click Finish.

You can go back to the previous panels and edit the configurations any time.

You can go to the Monitor > Jobs view to monitor the current status of the job.

The asset import job can be in one of the following states:

- Custom
This state indicates that the state of the asset import job run is Awaiting Manual Review.

- **Completed**
  This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- **Executing**
  This state indicates that the job is running.

- **Awaiting manual review**
  This state indicates that the records that are returned by the data collector should be manually reviewed.
  See “Reviewing the assets manually” on page 367.

**Importing asset-specific and common fields using the ODBC data collector**

You can use an ODBC data collector as any other default data collector to import the assets of any predefined platform or of a custom platform. The custom platform represents a custom application that is defined through the entity schema for the Control Compliance Suite.

See “Creating a new entity schema” on page 461.

Before you start using the ODBC data collector for asset import, ensure that you meet the following prerequisites:

- Format the ODBC database table or view names and column names as per the entity schema.
  See “Format to create ODBC compliant database tables” on page 363.

**Note:** If you are using ODBC data collector to import assets of predefined asset types, then it is recommended that you use the Entity-Table mapping option. You require to map all the primary and mandatory fields of the asset type for successful data collection.

- Configure a DPS as the ODBC data collector.
  See “Configuring the ODBC data collector” on page 158.

**To import asset-specific and common fields using the ODBC data collector**

1. Go to Manage > Assets > Asset System.
2. On the taskbar, from the Asset Tasks select **Import Assets**.
3 In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

You can optionally type the description for the import job and click **Next**.

4 In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type to import the assets.

You can select either a predefined platform or a custom platform that is defined for a custom application based on your requirement. For the type of platform that you select, ensure that you configure the database accordingly as mentioned in the prerequisites.

5 In the **Select Platform, Asset Type, and Data Collector** panel, from the **Asset Source** drop-down list, select **ODBC Data Collector** and click **Next**.

6 In the **Select Asset Import Scope** panel, click the ... option to select the scope for the asset type.

Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.

Click **Browse (...)** to view and select the scope.

In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.

See “**About scopes in asset import**” on page 349.

7 In the **Select Asset Import Scope** panel, browse through the assets hierarchy and select a folder to add the assets from. Click **Add** to add it as a scope and click **Next**.

8 In the **Add Reconciliation Rules** panel, you can do one of the following:

- Use the Add Rules option to add a rule to the import job from the existing rules.
  The Add Rule option displays the Select Reconciliation Rules panel.

- Use the Delete Rule option to delete the rule that is already added and click **Next**.

- Use the Move Up and Move Down options to arrange the rules in the order and click **Next**.

9 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.

Click **OK**.

10 In the **Specify Asset Field Filters** panel you can do one of the following:
■ Use the Edit Selected Statement option to edit the existing filter and click Next.

■ Use the Delete Selected Statement option to delete the existing filter and click Next.

■ Use the Add Statement option to create a new statement.
  The Add Statement option displays the Create Filter Statement dialog box.

11 In the Create Filter Statement dialog box, use the parameter type and the conditions to create a filter statement.

See “Examples of asset filters” on page 292.

See “Filter statement operators” on page 293.

12 In the Schedule panel, select any one of the following:

■ If you want to run the job after the wizard closes, check Run now.

■ If you want to run the job at a specified interval, check Run periodically and enter the following information:
  ■ In the Start On box, enter the start date and time to run the job.
  ■ Under Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click Next.

13 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:

■ Type the subject and message of the notification mail.

■ Type the email ID of the sender and the receiver.

14 In the Summary panel, review the configurations for the import job and click Finish.

You can go back to the previous panels and edit the configurations any time.

You can go to the Monitor > Jobs view to monitor the current status of the job.

The asset import job can be in one of the following states:

■ Custom
  This state indicates that the state of the asset import job run is Awaiting Manual Review.

■ Completed
  This state indicates that the job is complete.
The asset import job run can be in one of the following states:

- Executing
  This state indicates that the job is running.

- Awaiting manual review
  This state indicates that the records that are returned by the data collector should be manually reviewed.
  See “Reviewing the assets manually” on page 367.

### Updating the assets in the system after the import

Once you import the assets in the asset system, you can use the Update rule to update the field values of the existing assets.

Consider the following scenario:

Assume that the operating system of the assets in your enterprise that belonged to the Finance Department, changes from Windows to Linux. You have the asset group based on the tag, Finance Department. The Update rule lets you update the value of the operating system field.

**To update the existing field value with an update rule**

1. Go to Manage > Reconciliation Rules.
2. From the taskbar, select **Create Rule**.
3. In the **Create or Edit Reconciliation Rule** wizard, in the Specify Rule details panel type the rule name.
4. From the Rule type drop-down list, select **Add Rule**.
5. From the Asset type drop-down list select **Windows Machine**.
6. In the Save in box, browse and select the folder where you want to save the rule and click **Next**.
7. In the **Select Rule Conditions and Actions** panel, select **Add Condition**.
8. In the **Add Condition** dialog box, select If an asset being imported exists in the asset system and click **OK**.
9. In the **Select Rule Condition and Actions** panel, select **Add Action**.
10 In the Add Action dialog box, select **Set the field value of an existing asset as specified**.

In the Fields list, select **OS Type**.

In the Value box, type **Linux** and click **OK**.

11 Click **Finish** in the Summary panel.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

**Common fields for all asset types**

Control Compliance Suite supports certain predefined asset types.

See “Predefined asset types” on page 236.

All the asset types have certain common fields. To import the data for the common fields, you must configure the Common platform either through CSV or ODBC settings. The CSV or ODBC settings can be specified through the **Edit Settings** dialog box while configuring the DPS. In the asset import job, data for the common fields can be imported either through a CSV or an ODBC data collector.

See “Configuring Common platform through CSV settings” on page 326.

See “Configuring Common platform through ODBC settings” on page 328.

All the asset types have the following common fields:

- **Confidentiality**
  Confidentiality is the act of limiting the access and disclosure of information to only authorized users. The impact of unauthorized disclosure of confidential information can lead to security risk, loss of public confidence, or legal action against the organization.

  You can set the value of this field as one of the following:

  - **Not Defined**
    This is represented by 0 in the CCS directory. You must specify 0 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 0 defines the asset value of Confidentiality as NotDefined after the asset import.

  - **Low**
    This is represented by 1 in the CCS directory. You must specify 1 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 1 defines the asset value of Confidentiality as Low after the asset import.

  - **Medium**
This is represented by 2 in the CCS directory. You must specify 2 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 2 defines the asset value of Confidentiality as Medium after the asset import.

■ High
This is represented by 3 in the CCS directory. You must specify 3 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 3 defines the asset value of Confidentiality as High after the asset import.

**Note:** If you specify the value of this field in the CSV file or in the ODBC database columns as anything greater than 3, the asset system marks it as NotDefined.

■ Integrity
Integrity refers to the genuineness of the information. Integrity dictates that information must be protected from improper modification. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. Continuous use of corrupted data can result in inaccuracy, fraud, or erroneous decisions.

You can set the value of this field as one of the following:

■ Not Defined
This is represented by 0 in the CCS directory. You must specify 0 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 0 defines the asset value of Integrity as NotDefined after the asset import.

■ Low
This is represented by 1 in the CCS directory. You must specify 1 in the CSV file, in case you want to define the asset value of Integrity as Low after the asset import.

This is represented by 1 in the CCS directory. You must specify 1 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 1 defines the asset value of Integrity as Low after the asset import.

■ Medium
This is represented by 2 in the CCS directory. You must specify 2 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 2 defines the asset value of Integrity as Medium after the asset import.
High
This is represented by 3 in the CCS directory. You must specify 3 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 3 defines the asset value of Integrity as High after the asset import.

Note: If you specify the value of this field in the CSV file or in the ODBC database as anything greater than 3, the asset system marks it as NotDefined.

Availability
Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space affect the availability of a system. If a mission-critical asset is unavailable to its end users, the organization's mission may be affected.

You can set the value of this field as one of the following:

■ Not Defined
This is represented by 0 in the CCS directory. You must specify 0 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 0 defines the asset value of Availability as NotDefined after the asset import.

■ Low
This is represented by 1 in the CCS directory. You must specify 1 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 1 defines the asset value of Availability as Low after the asset import.

■ Medium
This is represented by 2 in the CCS directory. You must specify 2 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 2 defines the asset value of Availability as Medium after the asset import.

■ High
This is represented by 3 in the CCS directory. You must specify 3 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 3 defines the asset value of Availability as High after the asset import.

Note: If you specify the value of this field in the CSV file or in the ODBC database as anything greater than 3, the asset system marks it as NotDefined.
Compliance Score
The compliance score is a percentage value between 0 and 100 that represents the level of adherence to a standard. This score is derived from the checks that are present in a standard.
The checks in the Not Applicable status are not considered when you calculate the compliance score.
The compliance score is available when you evaluate an asset against one or more standard. The result of the evaluation process provides the compliance and the risk score.

Risk Score
A risk score is used to quantify the risk that is associated with an asset in your organization. The risk score is calculated on the basis of the CIA values for an asset and the risk attributes of a check. You should give due consideration before you specify these values in the product.

Risk Rating
Risk Rating is the maximum risk score that is calculated based on the maximum weight for a risk property provider.

Tags
Tagging is a way to define an asset with meta information. Tagging helps you identify assets in some context that might prove helpful to determine the value of the asset. You can use the tags to filter the assets.
For example, you can create a tag that is called SOX and associate it with a relevant asset.

Asset Custodian
User who is the business owner of the asset data. There can be one or more custodians for a set of assets. For example, Finance Manager and the Human Resource Manager can be the custodians for the data of all the assets that include the data related to the employee's salary.

Asset Department
The department to which the asset belongs.

Asset Location
The location of the asset in the organization.

Asset Owner
Asset owner is the user who has the permissions to import, update, rename, and delete the assets in the asset system.

Asset Site
The site to which the asset belongs.

Source Name
Name of the source from which the asset is being imported. The source can be one of the pre-defined data collectors, the CSV data collector, the ODBC data collector, or any other source that is used for asset import.

- **Source ID**
  Unique identification of the asset in the source.

You can set the values of the common fields with the Pre rule.

See “Using a Pre rule to set the values of the common fields” on page 309.

See “Importing asset-specific and common fields using the default data collector” on page 332.

See “Importing asset-specific and common fields using the CSV data collector” on page 335.

See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338.

See “Importing asset-specific and common fields using the ODBC data collector” on page 341.

### About scopes in asset import

You add a scope to the asset import job to gather more specific asset data.

To provide a scope for the asset import, you first limit the scope to a location in the system. The location can be a site, a domain in case of Windows, or a database in case of SQL and Oracle. When you specify a scope at the location level, the asset import query returns the specified asset type from the specified location only.

After you provide the scope at the location level, you can select a specific folder, an asset group, or an asset. The asset import query looks for the specified folder, the asset group, or the asset at the specified location and returns the asset type. Provide asset groups or containers as scopes instead of providing individual assets as scopes.

Consider the following example:

Assume that you want to import the Windows Files. You limit the scope to Windows Machine, which is the default scope for the Windows Files. You select a folder as a scope that contains the Windows Machine and Windows Domain. In this case, the asset import query does not consider the Windows Domain as you have limited the scope to Windows Machine only.

*Table 5-54* explains how the default scopes and the supported scopes work in the asset import.

You can scope the assets in the following ways:
■ Use the default scope
The default scope includes the primary assets for the asset type that you want to include. You import the selected asset type from the primary asset for that asset type.
See “Primary and secondary assets” on page 275.

■ Use any or all the supported scopes
The supported scopes include all the asset types or sites from which you can import the selected asset type.

Table 5-54 Asset import scope options

<table>
<thead>
<tr>
<th>Scope</th>
<th>Scenario</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default scope</td>
<td>■ You select Windows File as the asset type to import.</td>
<td>■ With the default scope, you can obtain more specific asset data.</td>
</tr>
<tr>
<td></td>
<td>■ The supported scopes for the Windows File asset type are Domain, Machine, Directory, and File.</td>
<td>■ The query execution is comparatively faster due to specific scope.</td>
</tr>
<tr>
<td></td>
<td>■ The default scope for the Windows File asset type is Machine.</td>
<td>■ You can use the default scope effectively if you want to update the fields of certain existing assets.</td>
</tr>
<tr>
<td></td>
<td>■ You use the default scope.</td>
<td>■ The order of asset type import is important if you want to use the default scope.</td>
</tr>
<tr>
<td></td>
<td>■ The asset import query looks for the Windows files only in the machines.</td>
<td>For example, to import the Windows file with the default scope, you should have the Windows machines already imported in the asset system.</td>
</tr>
<tr>
<td></td>
<td>■ If you explicitly select the machines A, B, C, and D, the asset import query looks for the Windows files only in the machines. In the scope, the asset import query looks for the Windows files on the specified machines only.</td>
<td>See “Default scope and supported scope” on page 351.</td>
</tr>
</tbody>
</table>
Table 5-54  Asset import scope options (continued)

<table>
<thead>
<tr>
<th>Scope</th>
<th>Scenario</th>
<th>Results</th>
</tr>
</thead>
</table>
| Supported scope | ■ The supported scopes for the Windows File asset type are Domain, Machine, Directory, and File.  
                      ■ The default scope for the Windows File asset type is Machine.  
                      ■ You use Domain, Machines, and Directory from the supported scope.  
                      ■ The asset import query looks for the Windows files in domains, machines, and directories. | ■ The query execution takes longer if you do not scope the query properly. See “Default scope and supported scope” on page 351. |

See “Default scope and supported scope” on page 351.

**Default scope and supported scope**

You add a scope to the asset import job to gather more specific asset data.

You can scope the assets in the following ways:

- **Use the default scope**
  The default scope includes the primary assets for the asset type that you want to include. You import the selected asset type from the primary asset for that asset type.
  See “Primary and secondary assets” on page 275.

- **Use any or all the supported scopes**
  The supported scopes include all the asset types or sites from which you can import the selected asset type.

**Table 5-55**  Supported and default scopes for the asset types

<table>
<thead>
<tr>
<th>Asset type</th>
<th>Default scope</th>
<th>Supported scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom</td>
<td>Site</td>
<td>Site</td>
</tr>
<tr>
<td>In case you create a custom asset type from a custom platform</td>
<td>Asset type</td>
<td>Asset type</td>
</tr>
<tr>
<td>Asset type</td>
<td>Default scope</td>
<td>Supported scope</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ESM Agent</td>
<td>ESM Agent, Site</td>
<td>ESM Agent, Site</td>
</tr>
<tr>
<td>Oracle Configured Databases</td>
<td>Site</td>
<td>Site, Oracle Configured Databases, Oracle Configured Servers</td>
</tr>
<tr>
<td>Oracle Configured Servers</td>
<td>Site</td>
<td>Site, Oracle Configured Servers</td>
</tr>
<tr>
<td>SQL Database</td>
<td>SQL Server</td>
<td>SQL Database, SQL Server</td>
</tr>
<tr>
<td>SQL Server</td>
<td>Site</td>
<td>SQL Server, Site</td>
</tr>
<tr>
<td>UNIX File</td>
<td>UNIX Machine</td>
<td>UNIX Machine, UNIX File</td>
</tr>
<tr>
<td>UNIX Group</td>
<td>UNIX Machine</td>
<td>UNIX Machine, UNIX Group</td>
</tr>
<tr>
<td>UNIX Machine</td>
<td>Site</td>
<td>UNIX Machine, Site</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>Site</td>
<td>Windows Domain, Site</td>
</tr>
</tbody>
</table>
Table 5-55  Supported and default scopes for the asset types (continued)

<table>
<thead>
<tr>
<th>Asset type</th>
<th>Default scope</th>
<th>Supported scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Group</td>
<td>Windows Machine</td>
<td>Windows Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Machine</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Domain</td>
</tr>
<tr>
<td>Windows Machine</td>
<td>Windows Domain</td>
<td>Windows Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Machine</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Site</td>
</tr>
<tr>
<td>Windows Share</td>
<td>Windows Machine</td>
<td>Windows Share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Machine</td>
</tr>
</tbody>
</table>

See “About scopes in asset import” on page 349.

Importing assets from a CSV file

In Control Compliance Suite, you can maintain assets in a CSV file, which can be imported into the infrastructure for data collection. The assets are categorized into various asset types, which are imported into Control Compliance Suite through the Create or Edit Asset Import Job wizard. The assets of any application can either belong to a predefined asset type or you can define a new asset type.

See “Predefined asset types” on page 236.

Before performing an asset import operation from a CSV file, you must first export the assets into a CSV file. You can use any third-party utility to export the assets into the CSV file. The assets that are exported into the CSV file must be arranged in a specific format. You must configure the CSV data collector before you import the assets into Control Compliance Suite.

See “Creating a new asset type” on page 446.

See “Configuring the CSV data collector” on page 156.

See “About format of the CSV file headers” on page 353.

About format of the CSV file headers

After you export the assets and the data that is related to the assets into a CSV file, you must arrange them in a specific format. A single CSV file can contain assets that belong to a specific asset type. Assets can belong either to a predefined asset type or to the asset types that are defined by you through Control Compliance Suite.
See “Creating a new asset type” on page 446.

The CSV file must contain headers under which the assets along with the data that is related to the assets are arranged. A header is defined containing the name of the platform, the name of the asset type or entity, and the property or field that defines the asset. For every asset, you can categorize the properties or fields into asset-specific and common.

The format of the headers for the asset-specific and common fields are as follows:

- **Asset-specific fields**
  The asset-specific fields of an asset type comprise the unique identifiers of the asset type along with all fields that define the asset type.
  The header format for the asset-specific fields is as follows:
  
  `<platform>.<entity>.<field>`
  
  The details of the fields are as follows:

  - The platform header represents the platform to which the asset type belongs. For example, the platform of a predefined asset type, Windows Domain is Windows. See “About platforms” on page 456.

  - The entity header represents the asset type. For example, Windows Domain can be an asset type for all computers or assets of the Windows domain. See “About entities” on page 457.

  - The field header represents the property that defines the asset. For example, an asset can have properties such as machine name, IP address, domain name. See “About fields of an entity” on page 457.

  An example of the header of the asset-specific fields of an asset that belongs to a predefined asset type, Windows Domain is as follows:
  
  `Wnt.Domain.Host, Wnt.Domain.IPaddress, Wnt.Domain.DomainName`
  
  The properties of the asset are Host (computer name), IP address, and DomainName.

  Every asset is identified easily with their unique identifiers such as IP address, machine name, or domain name. In Control Compliance Suite, these identifiers are known as primary and mandatory fields. You must identify the primary and mandatory fields of an asset type during creation. These primary and mandatory fields are a part of the asset-specific fields and must be specified in the CSV file for every asset.

- **Common fields**
  The common fields of an asset type are confidentiality, integrity, availability, and tags.
  The header format for the common fields is as follows:
See “Common fields for all asset types” on page 345.

An example header format for the common fields of an asset type, Windows Domain is as follows:

*Common.WntDomain.Confidentiality, Common.WntDomain.Integrity*

The common fields of the asset are confidentiality and integrity.

For the predefined asset types, you can retrieve the headers directly into a CSV file from the Asset View of the console. You can use the option, Export CSV Headers of the Asset View to export the headers into the CSV file.

See “Exporting CSV headers” on page 393.

For example, the assets that belong to a predefined asset type, Windows File, the headers that are exported using the option, Export CSV Headers are as follows:


**Note:** To import assets of the asset type, Windows File with directory as the scope using the CSV data collector, add a new column in the CSV file. The column, WntFile.PARENTDIRECTORYINT is added in the CSV file besides the other fields that are required for the asset type. The data for this column must contain the directory names, which are specified as the scope during the asset import.

For the custom applications, you need to define the headers for the asset type through the Create New Entity Schema wizard.

See “Creating a new entity schema” on page 461.

See “Predefined asset types” on page 236.

See “About the list field format in CSV file” on page 359.

See “Creating a CSV file for custom application” on page 357.

See “Creating a CSV file for predefined asset types” on page 356.
Creating a CSV file for predefined asset types

A comma-separated value (CSV) file is one of the means to import data into the Control Compliance Suite. Data is arranged in a specific format in the CSV file for easy interpretation by the infrastructure. A CSV data collector is configured to collect data from the CSV file. Reports of the collected data is generated and displayed in the Control Compliance Suite console. In the CSV file, you must organize data in a comma-separated manner as per a specific format.

See “About format of the CSV file headers” on page 353.

You can create a CSV file for any custom application or for any of the predefined asset types of Control Compliance Suite.

See “Creating a CSV file for custom application” on page 357.

Note: To import assets of the ESM asset type, Agent, you can use the file, ESMAgentAsset.csv. This file is located in the directory, <install directory>\Symantec\CCS\Reporting and Analytics\Applications\Data Collectors\ESM.

To create a CSV file

1. Go to Manage > Assets > Asset System.
2. On the right-hand side table pane of the Asset System view, select a predefined asset type from the Display drop-down box.
3. From the taskbar select Asset Tasks > Export CSV Headers.

The CSV headers for the selected predefined asset type is exported to a .csv file that is created instantaneously. The .csv file contains headers for the asset-specific and common fields of an asset type.
In the CSV file, arrange the assets and the corresponding data of the predefined asset type.

For example, for the predefined asset type, Windows Directory, the data representation of the asset-specific and common fields of the asset type is as follows:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TestDomain</td>
<td>Test1Machine</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>TestDomain</td>
<td>Test2Machine</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Import the assets of the predefined asset type through the Create or Edit Asset Import Job wizard.

See “Importing asset-specific and common fields using the CSV data collector” on page 335.

Ensure that you select CSV data collector in the Create or Edit Asset Import Job wizard.

See “Configuring the CSV data collector” on page 156.

Creating a CSV file for custom application

A comma-separated value (CSV) file is one of the means to import data into the Control Compliance Suite. Data is arranged in a specific format in the CSV file for easy interpretation by the infrastructure. A CSV data collector is configured to collect data from the CSV file. Reports of the collected data is generated and displayed in the Control Compliance Suite console. In the CSV file, you must organize data in a comma-separated manner in a specific format.

For a custom application, you must define an entity, which maps to an asset type. An entity is defined in the entity schema, which is created using the Create New Entity Schema wizard. The entity schema contains the blueprint of the asset type. The assets that you import can either belong to any of the predefined asset types or you can create a new asset type. If the assets belong to a predefined asset type, then you must know the details of the fields of the predefined asset type.

See “Predefined asset types” on page 236.
To create a CSV file

1 Export the data of the custom application into a CSV file.

2 Identify whether the asset type or entity of the custom application belongs to any of the predefined asset type.

3 If the asset type or entity does not belong to any of the predefined asset type, then identify the following for the asset type:
   - Platforms
     See “About platforms” on page 456.
   - Entity
     See “About entities” on page 457.
   - Fields
     See “About fields of an entity” on page 457.

4 For a custom application, you must first define an entity schema before creating the CSV file.
   See “Creating a new entity schema” on page 461.
   The schema is created using the Create New Entity Schema wizard. In the entity schema, you must specify the primary fields of the entity besides defining the other asset-specific and common fields.

5 Copy the CSV file headers from the Summary panel of the Create New Entity Schema wizard and paste it in the CSV file.
   Ensure that the CSV headers are arranged in the supported format. The best practice is to specify the header information of the primary fields as the starting columns in the CSV file.
   See “About format of the CSV file headers” on page 353.
   For example, you can have a network of servers that are installed with a custom application, DB2 and you want to collect the server name of all the servers. In the entity schema, you can define the platform as DB2, the entity as Server and the field as Server Name.
   The header information for the DB2 application in the CSV file is of the following format:
   DB2.Server.ServerName
   If the asset type or entity belongs to a predefined asset type or an already defined asset type, then export the CSV headers from the console. The header information of the asset type can be retrieved from the Asset view of the console.
   See “Exporting CSV headers” on page 393.
6 Arrange the data of the custom application for the defined CSV headers in the CSV file.

7 Configure the CSV data collector.

See “Configuring the CSV data collector” on page 156.

See “Creating a new asset type” on page 446.

See “Creating a CSV file for predefined asset types” on page 356.

About the list field format in CSV file

The Control Compliance Suite accepts data from the CSV file for data collection only if the data is specified in a specific format.

See “About format of the CSV file headers” on page 353.

If you want to define a string type data, which is an array in the CSV file, then you must ensure that the data is represented in a specific list field format. Control Compliance Suite does not report on string type array data, which is not specified as per the list field format in the CSV file.

Control Compliance Suite supports the following list field formats in a CSV file:

- Multi-line text enclosed in double quotes
- The format, @:<total number of items in the list>:<char count>:<char text>
  For example, @:3:10:TestDomain:7:Domain1:9:ESMDomain

The list field details of the format in the example are as follows:

- The number, 3 represents the total number of items in the list. The items in the list are, TestDomain, Domain1, and ESMDomain.
- The number, 10 is the character count of the list item, TestDomain. Similarly, the number, 7 is the character count of the list item, Domain1.
- The character text is the name of the list item such as TestDomain, Domain1, and ESMDomain.

Importing specific assets manually only once from the CSV file

The Control Compliance Suite lets you import only the specific assets into the asset system. The Create or Edit Asset Import Job wizard provides a One time, manual entry job option that lets you import specific assets.

You can import such assets manually from a CSV file. The import of this type only works if you want to import the assets into the system only once.
You must use a CSV file to import specific assets. The CSV file can contain only the primary fields of the asset type that you want to import.

The **Onetime, manual entry job** option is available only for the following platforms and asset types:

**Table 5-56** Exported headers for the asset type

<table>
<thead>
<tr>
<th>Platform</th>
<th>Asset type</th>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange</td>
<td>Organization MS-Exchange</td>
<td>Mailadmin.BROWSEE2KORG.orgDN</td>
</tr>
<tr>
<td>SQL</td>
<td>SQL Server</td>
<td>■ Dbif.server.SQLServerDomainName&lt;br&gt; ■ Dbif.server.serverName&lt;br&gt; ■ Dbif.server.hostName&lt;br&gt; ■ Dbif.server.versionMajor</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows Domain</td>
<td>Wnt.Domain.DomainName</td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Configured Databases</td>
<td>■ ORCL.CONFIGUREDDATABASES.servername&lt;br&gt; ■ ORCL.CONFIGUREDDATABASES.ServerNetBIOSName&lt;br&gt; ■ ORCL.CONFIGUREDDATABASES.DomainNameOrlIPAddress&lt;br&gt; ■ ORCL.CONFIGUREDDATABASES.dbname&lt;br&gt; ■ ORCL.CONFIGUREDDATABASES.dbversion&lt;br&gt; ■ ORCL.CONFIGUREDDATABASES.OSTYPE</td>
</tr>
</tbody>
</table>
Table 5-56  Exported headers for the asset type (continued)

<table>
<thead>
<tr>
<th>Platform</th>
<th>Asset type</th>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>Oracle Configured Servers</td>
<td>ORCL.CONFIGUREDSERVERS.VERS.SERVERNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ORCL.CONFIGUREDSERVERS.VERS.ServerNetBIOSName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ORCL.CONFIGUREDSERVERS.VERS.DomainNameOrlIPAddress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ORCL.CONFIGUREDSERVERS.OSTYPE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unix.Machine.IPAddress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unix.Machine.OSSystem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unix.Machine.ODistributionField</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unix.Machine.OSVersionString</td>
</tr>
</tbody>
</table>

To import specific assets manually only once from a CSV file

1. Go to Manage > Assets > Asset System.
2. On the taskbar, from the Asset Tasks select Import Assets.
3. In the Specify Name and Description panel, in the Name box, type the name for the import job.
   You can optionally type the description for the import job and click Next.
4. In the Select Platform, Asset Type, and Data Collector panel, select the platform and the asset type to import the assets for.
5. In the Select Platform, Asset Type, and Data Collector panel, from the Asset Source drop-down list, select One time, manual entry and click Next.
   See “About the working of CSV data collector in asset import” on page 324.
In the **Specify Individual Assets** panel, provide the following information and click **Next**.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Lets you specify the fully-qualified domain name and the machine name of the asset.</td>
</tr>
<tr>
<td>Export Grid to CSV</td>
<td>Lets you export the headers and the other information of the primary fields that belong to the specified platform and asset type. The headers are exported to a CSV file.</td>
</tr>
<tr>
<td>Import Grid from CSV</td>
<td>Lets you import the fully-qualified domain name and the machine name for the assets from a CSV file.</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>Only the primary fields from the CSV file are displayed in the grid. The other fields are displayed but the details of those fields are imported during the asset import.</td>
</tr>
<tr>
<td>Site</td>
<td>Lets you select the sites to which the specified assets belong.</td>
</tr>
<tr>
<td>Specify reconciliation rules before finishing</td>
<td>Lets you specify the reconciliation rules for the asset import, if you select the option.</td>
</tr>
</tbody>
</table>

If you select the **Specify reconciliation rules before finishing** option in the **Specify Individual Assets** panel, add the reconciliation rules in the **Add Reconciliation Rules** panel. Click **Next**.

In the **Summary** panel, review the configurations for the import job and click **Finish**.

### Importing assets from an ODBC database table

In Control Compliance Suite, you can store the asset information in an ODBC database and import them into the infrastructure for data collection. The assets are categorized into various asset types and are imported into the infrastructure using the Create or Edit Asset Import Job wizard. The assets of any application can either belong to a predefined asset type or you can define a new asset type.

See “**Predefined asset types**” on page 236.

Before performing an asset import operation from an ODBC database table, ensure that the table contains the asset information. The database table or view names
and the column names must be defined in a specific format. The ODBC data collector interprets the database table or view names to import assets from the tables.

See “Creating a new asset type” on page 446.

See “Configuring the ODBC data collector” on page 158.

See “Format to create ODBC compliant database tables” on page 363.

**Format to create ODBC compliant database tables**

To import data from the ODBC compliant databases using the ODBC data collector, you must configure the database table as per the defined format. The defined format is easily interpreted by the ODBC data collector for effective data collection. As per the defined format, the table name or view name and the column names must be mapped with the entity name and the fields, respectively.

The format of the database table naming convention depends on the attributes of the entity schema that you create for an application. Every entity schema is the blue-print for the data collector to collect data and contains the definition of the platform, entity, and the entity fields.

See “Creating a new entity schema” on page 461.

Configure the ODBC data collector for the custom platform that you define in the entity schema.

See “Configuring the ODBC data collector” on page 158.

**Table 5-57** Mapping between an entity schema attribute and the ODBC database table element

<table>
<thead>
<tr>
<th>Entity schema attribute</th>
<th>ODBC database element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform name and entity name</td>
<td>Database table or view name</td>
<td>The database table or view name is a combination of the platform name and the entity name. The format of the table or view name must be in the following format: <code>&lt;platformnameentityname&gt;</code></td>
</tr>
<tr>
<td>Field name</td>
<td>Database table column name</td>
<td>The database table's column name must be same as the field name of the entity.</td>
</tr>
</tbody>
</table>

The format of naming the ODBC database tables are as follows:
Format to create database table or view names for all platforms
You manually create the database table or view names based on the attributes of the entity schema. The table or view name is a combination of the platform name and the entity name.
The format to create the database table or view names is as follows:
platformnameentityname
For example, you want to configure an ODBC data collector for the platform, DB2, whose entity is Server. As per the defined format, the database table or view name must be DB2Server.

Format to create database table or view names for the Common platform only
The format to create database table or view names for the Common platform is different when compared to the format for other platforms. The Common platform defines the CIA field values and by default, is configured for the predefined asset types. Hence, the table or view name is a combination of the predefined platform name and the entity name.
The format to create the database table or view names for the Common platform is as follows:
predefinedplatformnameentityname
For example, you want to configure an ODBC data collector for the Common platform of a predefined asset type, Windows Machine. For this asset type, the predefined platform is, Wnt and the entity is, Machine. As per the defined format, table or view name for the Common platform must be WntMachine.

Format to create database table column names for all platforms
The fields of an entity that are defined in the entity schema must be the database table column names.
For example, you want to configure an ODBC data collector for the platform, UNIX, whose entity is, Machine. The entity fields are, IPAddress and Hostname for the entity, Machine. As per the defined format, the database table column names must be IPAddress and Hostname.

Format to create database tables for the predefined platforms and their asset types
You can create the database tables for the predefined platforms and their asset types using the following standard naming convention:
predefinedplatformnameentityname
You must use the internal names of the predefined platforms to define the database table names or view names. For the predefined platforms, the predefined asset types represent the entities. Hence, you can specify the name of the asset type in place of the entity in the defined format. For example, for the Windows platform, the internal name is Wnt. The table or view name for the predefined asset type, Windows Machine is, WntMachine.
The predefined platforms and their internal names are as follows:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Internal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Wnt</td>
</tr>
<tr>
<td>UNIX</td>
<td>Unix</td>
</tr>
<tr>
<td>Oracle</td>
<td>ORCL</td>
</tr>
<tr>
<td>SQL</td>
<td>Dbif</td>
</tr>
<tr>
<td>Exchange</td>
<td>Mailadmin</td>
</tr>
<tr>
<td>NDS</td>
<td>NDS</td>
</tr>
<tr>
<td>NetWare</td>
<td>NW</td>
</tr>
<tr>
<td>ESM</td>
<td>ESM</td>
</tr>
</tbody>
</table>

You must know the predefined asset types of the predefined platform to define the table name or view name for the specific asset type.

See “Predefined asset types” on page 236.

If you do not create table name or view name manually as per the entity schema, then you can use the Entity Table Mapping dialog box. This dialog box lets you map the entities to the existing database table or view names for the selected platform. You can also map the database table column names with the field names of the entities. You use this mapping option only if the database table or view names are not compliant with the defined format.

**Creating an ODBC database table for custom application**

The Control Compliance Suite can import assets of any custom application that are stored in the ODBC compliant databases. The assets are imported using the configured ODBC data collector. For example, you can import assets of a custom application such as DB2 using the ODBC data collector into the infrastructure. Before you import the assets, you must create asset types for the custom application and store the asset information in the ODBC compliant database.

You must define the asset information of the custom application in a specific format for easy interpretation by the ODBC data collector.

**To create an ODBC database table**

1. Export the data of the custom application into the ODBC database tables.
2. Identify whether the asset type or entity of the custom application belongs to any of the predefined asset type.

See “Predefined asset types” on page 236.
3 If the asset type or entity does not belong to any of the predefined asset type, then identify the following for the asset type:

- Platforms
  See “About platforms” on page 456.

- Entity
  See “About entities” on page 457.

- Fields
  See “About fields of an entity ” on page 457.

4 For a custom application, you must first define an entity schema before creating the database tables.

See “Creating a new entity schema” on page 461.

The schema is created using the Create New Entity Schema wizard. In the entity schema, you must specify the primary fields of the entity besides defining the other asset-specific and common fields.

5 Based on the entity that you create, you must create asset types for the custom application.

See “Creating a new asset type” on page 446.

6 Create tables with table or view names in a specific format combining the platform and the entity name.

The format is as follows:
<platformnameentityname>

For example, you can have a network of servers that are installed with a custom application, DB2 and you want to collect the server name of all the servers. In the entity schema, you define the platform as DB2 and the entity as Server.

One of the table or view name of the ODBC database is as follows:

DB2Server

7 Arrange the table column names as per the field names that are defined in the entity schema.

For example, you define an entity schema, for platform, DB2, with entity, Server and fields, ServerName, HostName, IPAddress. The database table column names must be same as the field names.

8 Configure the ODBC data collector.

See “Configuring the ODBC data collector” on page 158.

See “Format to create ODBC compliant database tables” on page 363.
About the list field format in ODBC database table

The Control Compliance Suite imports assets and collects data from the ODBC-compliant databases, only if the tables and columns are named in a specific format.

See “Format to create ODBC compliant database tables” on page 363.

If you want to define a string type data, which is an array in the ODBC database table, then the data must be represented in a specific list field format. Control Compliance Suite does not report on string type array data, which is not specified as per the list field format in the ODBC database.

The format of the list fields for the ODBC databases is as follows:

@:<total number of items in the list>:<char count>:<char text>

For example, @:3:10:TestDomain:7:Domain1:9:ESMDomain

The list field details of the format in the example are as follows:

■ The number, 3 represents the total number of items in the list.
■ The items in the list are, TestDomain, Domain1, and ESMDomain.
■ The number, 10 is the character count of the list item, TestDomain. Similarly, the number, 7 is the character count of the list item, Domain1.
■ The character text is the name of the list item such as TestDomain, Domain1, and ESMDomain.

Reviewing the assets manually

The assets that are marked for manual review in the reconciliation rules are added to the manual review store. The assets that do not satisfy any reconciliation rules are also included in the manual review store.

See “Manual review” on page 295.

See “Creating reconciliation rules using the manual review” on page 307.

You must manually review the records in the manual review store and decide whether the records should be added to the asset system or not.

The manual review of assets involve the following steps:

■ Viewing the manual review records
  See “Viewing the manual review records” on page 368.
■ Reconciling the manual review records
  See “Reconciling the manual review records” on page 368.
Viewing the manual review records

The assets that are marked for manual review in the asset import job appear in the Monitor > Jobs view. The status of the job run of the asset import job, that is marked for manual review is, Awaiting Manual Review. The parent asset import job, that is marked for manual review is, Custom.

To view the manual review records

1. Go to Monitor > Jobs.
2. In the table pane, navigate to the asset import job for which you want to view the manual review records.
3. In the table pane, right-click the job run that displays the status, Awaiting Manual Review.

   View the records in the Review Records - Monitor dialog box.

See “Manual review” on page 295.

See “Reconciling the manual review records” on page 368.

Reconciling the manual review records

After viewing the asset records that await the manual review, you can reconcile those assets again.

To reconcile the manual review records

1. Go to Monitor > Jobs.
2. In the table pane, right-click the job run that displays the status Awaiting Manual Review.
3 Select **Review Records**.

4 In the **Review Records - Monitor** dialog box, review the records. If you want to execute the add rule or the update rule that is associated with the asset import job on all the records, click **Reconcile Records**.

When you reconcile the records, another job run is created in the Jobs view. The status of the job that was marked as Awaiting Manual Review is not updated. The new job run shows the updated status after the records are reconciled according to the reconciliation rules. You can view the number of job runs in the original job with the status Awaiting Manual Review.

When you decide to reconcile the records, the job query ignores the manual review entry in the reconciliation rules. The job query only considers the original rule definition of the add rule or the update rule. The asset records for manual review are then added to the asset system or the field values are updated depending on the rule.

If you want to add another reconciliation rule to the records that await manual review, you can edit the parent asset import job. You can then associate a new reconciliation rule with the job and then reconcile the manual review records.

See “**Manual review**” on page 295.

See “**Viewing the manual review records**” on page 368.

### Creating asset groups

An asset group consists of the assets of one or more types. For example, Windows servers, UNIX servers, or Oracle databases can become asset groups. The grouping is represented in a hierarchical fashion with nested subsets.

You can create dynamic and static asset groups to organize the assets into logical groups. You can create asset groups on the basis of tags, CIA values, asset types, and other asset fields.

See “**Dynamic asset groups**” on page 297.

See “**Creating a dynamic asset group**” on page 370.

See “**Static asset groups**” on page 297.

See “**Creating a static asset group**” on page 372.

See “**Editing an asset group**” on page 376.
Creating a dynamic asset group

You create a dynamic asset group, if you want the assets in a folder to be organized dynamically based on certain properties. The dynamic asset group gets updated with every asset import job if more assets from the relevant asset folder meet the dynamic group filters.

**Note:** You can add assets to the asset group only from the folder that contains the asset group or from the folders in the same hierarchy.

**To create a dynamic asset group**

1. In the taskbar, from the Asset Group Tasks, select Create Asset Group.
2. In the *Specify Asset Group Details* panel, specify the following:
   - Name of the asset group
   - Description of the asset group
   - Folder path from which to include the assets
3. Select **Dynamic group** in the Asset Group Type section:
4. Click **Next**.
5. In the *Select Asset Type* panel, select the asset type for which you want to create an asset group and click **Next**.
6. In the Create Common Asset Field Filters panel, specify the value for the common asset field filters and click Next.

The Create Common Asset Field Filters panel lets you create a filter that is based on the values of the common fields. The panel presents a list of common asset fields. You can specify the values for the selected fields. The asset group is formed based on the values that you specify in this panel.

The Create Common Asset Field Filters panel presents the following options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you specify the asset name. Assets with the specified name are included in the asset group.</td>
</tr>
<tr>
<td>Location</td>
<td>Lets you specify the asset location. Assets that reside at the specified location are included in the group.</td>
</tr>
<tr>
<td>Department</td>
<td>Lets you specify the asset department. Assets that belong to the specified department are included in the asset group.</td>
</tr>
<tr>
<td>Owner</td>
<td>Lets you specify the asset owner. Assets with the specified owner are included in the asset group.</td>
</tr>
<tr>
<td>Custodian</td>
<td>Lets you specify the custodian for the assets. Assets with the specified custodian are included in the asset group.</td>
</tr>
<tr>
<td>Tags</td>
<td>Lets you specify the tag name and the tag path. Assets that have the specified tag are included in the asset group.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>Lets you specify the risk rating. Assets with the specified risk rating are included in the asset group.</td>
</tr>
<tr>
<td>Include assets with any of the above filters</td>
<td>Includes the asset in the asset group if the asset meets the criteria that is specified in any of the above filters.</td>
</tr>
</tbody>
</table>
7 In the **Create Specific Asset Type Filters** panel, select a field from the drop-down list on the basis of which you want to create the dynamic asset group. Click **Add Statement**.

The **Create Specific Asset Type Filters** panel lets you edit, delete, arrange, and configure the asset field filters. You can select a field that should be used as a filter for the selected asset type and create a filter statement. You can use the Add Statement option on the panel to create a new filter statement.

You can edit or delete the existing filter statement using the Edit option and the Delete option.

The asset field that you can select depends on the asset type that you selected.

You can use the AND and OR operators to specify the filter after adding the filter statements.

> See “Operators (, ), AND, OR” on page 374.

8 In the **Filter Statement** dialog box, select the parameter, the operator and the value for the field to form a filter statement and click **OK**.

9 In the **Create Specific Asset Type Filters**, click **Next**.

10 Review the configuration information in the **Summary** panel and click **Finish**.

See “Creating a static asset group” on page 372.

### Creating a static asset group

You create a static asset group for the assets that do not undergo frequent updates. The asset count in the static asset group remains constant unless you edit the group and manually add more assets to the group.

---

**Note:** You can add assets to the asset group only from the folder that contains the asset group or from the folders in the same hierarchy.

---

Consider the following example:

- Under the Asset System folder you have another folder - US-CA.
- You have a static asset group, WindowsServer2003 under the folder US-CA.
- You can add the assets to the asset group WindowsServer2003 from the folder US-CA or from the folders under the US-CA folder.

**To create a static asset group**

1 In the task bar, from the Asset Group Tasks, select **Create Asset Group**.

2 In the **Specify Asset Group Details** panel, specify the following:
Managing assets
Creating asset groups

- Name of the asset group
- Description of the asset group
- Folder path from which to include the assets

3. Select **Static group** in the Asset Group Type section.
4. Click **Next**.
5. In the **Select Asset Type** panel, select the asset type for which you want to create an asset group and click **Next**.
6. In the **Select Assets** panel, navigate to the folder in the asset system hierarchy, select the assets that you want to add to the asset group and click **Add**.
   This is an optional step.
7. Review the configuration information in the Summary panel and click **Finish**.

See “Creating a dynamic asset group” on page 370.

Deleting inactive assets using the asset groups

The Asset System view displays the number of active assets in the top right corner of the table pane. The active assets are the assets that are created or updated during the last six months. The active assets are displayed only for the Windows Machines, the UNIX Machines, and the ESM Agents.

You might want to delete the inactive assets from the asset system. You can use the asset groups feature to form a dynamic group of assets that are not modified for the last six months. You can then delete this group.

**To create an asset group based on the last modified date**

1. In the task bar, from the Asset Group Tasks, select **Create Asset Group**.
2. In the Specify Asset Group Details panel, specify the following:
   - Name of the asset group
   - Description of the asset group
   - Folder path where the asset group should be saved
3. Select **Dynamic group** in the Asset Group Type section.
4. Click **Next**.
5. In the Select Asset Type panel, select the asset type for which you want to create an asset group and click **Next**.
In the Create Common Asset Field Filters panel, specify the value for the common asset field filters and click **Next**.

The Create Common Asset Field Filters panel lets you create a filter that is based on the values of the fields that are common across all the asset types. The panel presents a list of common asset fields. You can specify the values for the selected fields. The asset group is formed based on the values that you specify in this panel.

In the Create Specific Asset Type Filters panel, select **All Asset Types - Asset last modified date** and click **Add Statement**.

You can use the AND and OR operators to specify the filter after adding the filter statements.

See “Operators (, ), AND, OR” on page 374.

In the Filter Statement dialog box, select **Specific Value**.

Select **EqualTo (=)** as the operator and from the Specify value drop-down list select a date.

The assets that were modified till the specified date are included in the asset group.

Review the configuration information in the Summary panel and click **Finish**.

### Operators (, ), AND, OR

In the asset system you can use the opening and closing parentheses, AND, and OR operators to join the filter statements. You need to specify the filters on the basis of which the asset import job or the asset groups is created.

You can use more than one filter and create a combined filter expression with the operators.

Consider the following example:

- You create the following filter statements:
  - A Equal To (=) B
  - C Greater Than or Equal To [<=] D
  - A Equal To (=) B
  - C Equal To (=) F

- You can use opening and closing parentheses, AND, OR operators in the following ways to specify the relation among the given filter statements:
  - A Equal To (=) B and C Greater Than or Equal To [<=] D
The AND operator is the default operator that is used to join the two filter statements.

- **A Equal To (=) B or C Greater Than or Equal To [<=] D**
  You can switch between the AND/OR operators using the same option.

- **(A Equal To (=) B) and (C Greater Than or Equal To [<=] D) or (A Equal To (=) B) and (C Equal To (=) F)**
  With the opening and closing parentheses, you can create more complex filter expressions.

### Performing the tasks in the Asset System view

You can perform the following tasks from the Manage > Assets > Asset System view:

- Creation of asset folders in the tree pane
  See “Creating the asset folders” on page 375.

- Asset group tasks
  See “Performing the asset group tasks” on page 376.

- Global tasks
  See “Performing the global tasks” on page 377.

- Asset tasks
  See “Performing the asset tasks” on page 391.

- Common tasks
  See “Deleting assets or asset groups” on page 393.

- View asset details pane
  See “Viewing asset information in the details pane” on page 394.

- Use Filter by pane
  See “Using the Filter by pane in the Asset System view” on page 402.

### Creating the asset folders

You create folders to store new assets. You use folders to organize the business objects in a hierarchical manner. The organization of the assets in a hierarchical manner is the most crucial step in the asset system. You can model the default hierarchy that is created during the installation of Control Compliance Suite, to suit your organizational requirements. Asset hierarchy can also be created based on the location, the department, the platform, or any other criteria.

See “Asset folder hierarchy” on page 234.
You can effectively administer the permissions on the folders and the objects within the folder if the hierarchy is created properly.

See “Assigning permissions from the Permission Management view” on page 113.

You can use reconciliation rules to help you arrange the assets in a specific hierarchical form.

To create a folder in the tree pane

1. Go to Manage > Asset System.
2. In the Asset System view, in the tree pane, right-click Asset System folder.
4. In the Create new container dialog box, type the name of the container.
5. Click OK.

See “About using special characters in folder and job names” on page 71.

See “Quick start with minimum configuration” on page 76.

Performing the asset group tasks

You can perform the following asset group tasks from the Asset System view:

- Create asset group.
  See “Creating asset groups” on page 369.

- Edit asset group.
  See “Editing an asset group” on page 376.

- Copy and paste asset group.
  See “Copying and pasting an asset group” on page 377.

- Rename Asset Group
  See “Renaming an asset group” on page 377.

Editing an asset group

You can edit the asset groups with the use of the Create or Edit Asset Group Wizard.

To use the Create or Edit Asset Group Wizard

1. In the table pane, select an asset group that you want to edit.
2. From the Common Tasks, select Edit Asset Group.
3. Edit the selections as you want and complete the wizard.
Copying and pasting an asset group

You can copy and paste the asset group to the same folder or any other folder under the Asset System in the tree pane. If you copy the asset group to the same folder, the group is created as Copy of <Name of the original asset group>.

You can also select and copy multiple asset groups from the table pane.

Note: When you copy and paste an asset group, the assets in the asset group are not retained. The filters for the asset group are retained. This is because you can include the assets to the asset group only from the folder where the asset group is present.

To copy and paste the asset group

1. In the table pane, right-click the asset group that you want to copy.
2. Select Copy Asset Group.
3. In the tree pane, right-click the folder in which you want to paste the asset group.
4. Select Paste Asset Group.

Renaming an asset group

To rename the asset group

1. In the tree pane right click the asset group.
2. Select Rename Asset Group.
3. In the Rename Asset Group dialog box, type a new name for the group.
4. Click OK.

Performing the global tasks

You can perform the following global tasks from the Asset System view:

- Mark as control point.
  See “Marking an asset as a control point” on page 378.
- Request exceptions.
  See “Requesting an exception for assets on checks” on page 379.
- Set up data collection.
  See “Setting up a data collection job from the Assets view” on page 380.
- Run evaluation.
See “Running an evaluation job from the Asset System view” on page 383.

- Run collection-evaluation-reporting
  See “Running a collection-evaluation-reporting job from the Asset System view” on page 385.

**Marking an asset as a control point**

An asset that is marked as a control point appears in the Entitlements > Control Points view.

You can mark only the following asset types as control points:

- Windows File
- Windows Directory
- Windows Groups
- UNIX File
- UNIX Group
- SQL Database
- Oracle Database
- ESM Agents

See “Control points” on page 497.

---

**Note:** You cannot mark Windows Machines, UNIX Machines, SQL Servers, and Oracle Servers as control points.

---

**To mark an asset as a control point**

1. Go to Manage > Assets > Asset System.
2. In the table pane, right-click the asset that you want to mark as a control point.
3. Select **Mark as Control Point**.
4. In case you mark an asset that belongs to Oracle, SQL, or ESM platforms as a control point, you must select the entitlement type.
   See “Control point type and entitlement type” on page 500.
5. In the Entitlement Type Selector dialog box, select one or more entitlement types and click **OK**.
6  In the confirmation message box, click OK.

7  Go to Manage > Entitlements > Control Points and verify the control point in the table pane.

See “Unmarking a control point” on page 501.
See “Control points” on page 497.

**Requesting an exception for assets on checks**

A requestor can request an exception on the checks for specific assets in the organization.

**To request an exception**

1  Go to Manage > Exceptions.

2  In the Exceptions view, do either of the following:
   - On the taskbar, click **Request Exception**.
   - In the table pane, right-click anywhere on the grid and select **Request Exception**.

3  In the Request Exception Wizard, in the Specify Exception Details panel, enter the following details and click **Next**:
   - In the Title box, enter the name of the exception.
   - In the Type box, select **Standards**.
     In the Template box, the displayed template is Evaluation Exception.
   - In the Description box, type a description for the exception.
   - In the Attachment box, browse to enter the name of the file that you want to attach.
   - In the Exception Validity group box, in the Effective Date box, select the date on which the exception becomes applicable. In the Expiration Date box, select the date on which the exception becomes invalid. Click **Next**.

4  In the Select Checks and Assets panel, click **Add** to select the standards, sections, or checks.

All the checks within the selected standard or section are displayed.
5 In the Select Standards or Sections or Checks dialog box, expand the Standards folder and select a folder. The standards within the selected folder are displayed in the right pane. Select a standard, section, or check and click Add. Click Add All to select all the standards. To remove one or more standards from the Selected Items list, click Remove or Remove All. Click OK.

All the checks within the selected standard or section are displayed in the Select Checks and Assets Panel.

6 In the Select Checks and Assets panel, click Add to select the assets. In the Select Assets or Asset Groups or Folders dialog box, expand the Assets folder and select a folder. The assets within the selected folder are displayed in the right pane. Select an asset and click Add. Click Add All to select all the assets. To remove one or more assets from the Selected Items list, click Remove or Remove All. Click OK.

7 In the Specify Exception Type Information panel, click Next.

8 In the Specify Requestor Information panel, type or browse to enter the Requestor and the Requestor Group. Enter the Requestor Email ID and Comments.

9 In the Specify Notification Information panel, edit the notification information for the notification type. Select the tab of the notification type. Modify the Subject and the Message. Click Next.

10 In the Summary panel, verify the details that you have entered in the wizard. Click Back to modify any data. Click Finish to exit the wizard.

The exception is created and its state is set to Requested.

Similarly, you can request an exception by launching the Request Exception Wizard from the Standards view, Assets view, and the Evaluation Results dialog box.

See “Launching the Request Exception Wizard” on page 541.

See “About exception states ” on page 533.

**Setting up a data collection job from the Assets view**

You can run a data collection job from the asset management view. You can use the Create or Edit Data Collection Job wizard to create a job to start the process of collecting data for the specified standards.

Ensure that you already have some assets in the asset store before you proceed with the data collection.
To set up a data collection job

1. Go to Manage > Asset System.
2. In the table pane, select the assets or the asset group for which you want to run the data collection job.
3. From the Global Tasks select, **Setup Data Collection**.
4. In the Create or Edit data Collection Job, in the Specify Job Name and Description panel, in the Name field, type the name of the data collection job.
5. In the Description box, type a description for the evaluation job and click **Next**.
6. In the Select Standards panel, navigate through the Standards and select a standard against which you want to set up a data collection.
   - The predefined standards or the custom standards that are relevant to the asset type selected only are available for selection.
7. Click **Add** to add the standard to the data collection job and click **Next**.
In the **Schedule Job** panel, select one of the following options:

- **Run with criteria**: Lets you collect the data for the assets for which the data is older than the specified number of days or is missing.
- **Run now**: Runs the job immediately, only once.
- **Run periodically**: Runs the job periodically based on the specified interval. Lets you specify the date and time to being the periodic schedule on. The **Run Periodically** option presents more options within the schedule.

The following table describes the options under the **Run periodically options**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run once</td>
<td>Runs the job only once based on the date and time that you specify in the <strong>Start On</strong> option.</td>
</tr>
<tr>
<td>Run every # days</td>
<td>Runs the job at regular intervals based on the number of days you specify.</td>
</tr>
<tr>
<td>Sub-schedule for data collection</td>
<td>Lets you specify the number of days after which you want to repeat the job. The option also lets you specify the last day until you want the job to continue running periodically. The sub-schedule is a subset of the period that you specify in the <strong>Run every # days</strong> option.</td>
</tr>
</tbody>
</table>

This schedule collects the data for the assets for which data was never collected for the standards in the job scopes.
9 In the Specify Notification Details panel, select **Send notification** and type the information for sending the notification and click **Next**.

10 In the Summary panel review all the selections that you made and click **Finish**.

You can monitor the status of the job from the Monitor > Jobs view.

See “Running an evaluation job from the Asset System view” on page 383.

### Running an evaluation job from the Asset System view

See “Viewing the evaluation results in the details pane” on page 400.

You run an evaluation job wizard to evaluate the assets in your organizations against specific standards or checks.

See “About evaluation jobs” on page 557.

**To run an evaluation job**

1 Go to Manage > Assets.

2 In the Assets view, do one of the following:
   - In the table pane, right-click and select **Run Evaluation**.
   - From the Global Tasks, select **Run Evaluation**.

3 In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.

4 In the Description box, type a description for the evaluation job and click **Next**.

5 In the Select Standards panel, in the tree pane, select a folder. You can further select from the displayed folder contents.

   The selected standards are displayed in the Selected Items list.

6 After this step, you can configure automatic remediation.

   If you do not want to configure remediation, you can skip the **Select Asset Types for Remediation** panel and click **Next** to reach the **Schedule Job** panel.

   For a detailed procedure of configuring the automatic remediation visit the following link:

   See “To remediate the assets automatically” on page 384.

7 In the Schedule Job panel, select any one of the following:
   - If you want to run the evaluation job after the wizard closes, check **Run Now**.
If you want to run the job at a specified interval, check Run Periodically and enter the following information.
In the Start On box, enter the start date and time to run the job.
Under the Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click Next.

You must set a password in the System Management > User Preferences > Data Collection Password. If you fail to set the password, a warning message appears when you schedule the job. You can click OK in the message box and specify the scheduling details. But you must set the password before the scheduled time for running the job.

8 In the Add Result Viewers panel, add the users or the groups that have the permissions to view the evaluation results and reports.
It is recommended to add the groups as the result viewers.

9 In the Specify Notification Details panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check Send notification, enter the following information and then click Next:

- Enter the subject and message of the notification mail.
- Enter the sender and the receiver email ID.
  Notification can be sent to multiple recipients.

To remediate the assets automatically

1 In the Select Asset Type for Remediation Ticketing panel, check the Enable Automatic Remediation Ticketing option to configure the automatic remediation details.
Select the asset types that correspond to the assets that were evaluated and click Next.

2 In the Specify Remediation Ticketing Criteria panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.
You can select Apply to all standards if you want to apply the specified remediation criteria to all the standards for remediation.
If you do not select Apply to all standards, you must specify the remediation ticketing criteria for each standard.
Click Next.

3 In the Select Remediation Ticket Type panel, select one of the following:
Create an email notification.
This option lets you create an email notification that you want to send for notification.

Create a service desk ticket.
This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.
You can choose the Enable closed-loop verification option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.
See “About closed-loop verification” on page 664.

Click Next.

4 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the Configure Notification Details for Remediation Ticketing panel. Click Next.

If you select Consolidate multiple assets in a single ticket/email, a single notification is sent that includes all the non-compliant assets.

You can check Make this the default Email Notification template if you want to use the same message for all the service desk ticket requests.

5 If you choose to create a service desk ticket as a remediation action, specify the message that you want to send as a service desk request in the Configure Service Desk Ticket panel. Click Next.

If you select Consolidate multiple assets in a single ticket/email, a single service desk ticket is generated that includes all the non-compliant assets.

You can check Make this the default Service Desk Ticket template if you want to use the same message for all the service desk ticket requests.

6 Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel.

Running a collection-evaluation-reporting job from the Asset System view

The collection-evaluation-reporting job lets you create a common job to schedule data collection, evaluation, and report generation. Control Compliance Suite provides different jobs for data collection, evaluation, and report generation tasks. In case of environments where thousands of such jobs are scheduled, a collection-evaluation-reporting job makes it easy to manage all the tasks from a single wizard.

See “About evaluation jobs” on page 557.
To run a collection-evaluation-reporting job

1. Go to Manage > Asset System.

2. In the Asset System view, right-click an asset in the table pane and select Run Collection-Evaluation-Reporting.

3. In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.

4. In the Description box, type a description for the evaluation job and click Next.

5. In the Select Standards panel, from the list of standards that appear in the left section, select the standard against which you want to evaluate the assets.
   Click Add to add the selected standard and click Next.
   Click Add All to add all the standards that appear in the right section and click Next.

6. In the Select Report Templates panel, do one of the following:
   - Select Synchronize evaluation results with reporting database to sync the evaluation results with the reporting database and click Next.
   - Select Generate reports for this evaluation results to select the report template for the evaluation results.
   You can also use the Define Scope and Add Template option to define the scope for the report.

7. After this step, you can configure automatic remediation.

   If you do not want to configure remediation, you can skip the Select Asset Types for Remediation panel and click Next to reach the Schedule Job panel.

   For a detailed procedure of configuring the automatic remediation visit the following link:

   See “To remediate the assets automatically” on page 390.

8. In the Schedule Job panel, select any one of the following:
   - If you want to run the evaluation job after the wizard closes, check Run Now.
   - If you want to run the job at a specified interval, check Run Periodically and enter the following information.
     In the Start On box, enter the start date and time to run the job.
     Under the Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click Next.
You must set a password in the **Home > User Preferences > Schedule Job Credentials**. If you fail to set the password, a warning message appears when you schedule the job. You can click OK in the message box and specify the scheduling details. But you must set the password before the scheduled time for running the job.
9 In the **Schedule Job** panel, select one of the following options:

- **Run with criteria**
  - Lets you collect the data for the assets for which the data is older than the specified number of days or is missing.
  - **Note:** The **Run with criteria** option is applicable only for the data collection job.

- **Run now**
  - Runs the job immediately, only once.

- **Run periodically**
  - Runs the job periodically based on the specified interval.
  - Lets you specify the date and time to being the periodic schedule on.
  - The **Run Periodically** option presents more options within the schedule.

The following table describes the options under the **Run periodically** options:

- **Run once**
  - Runs the job only once based on the date and time that you specify in the **Start On** option.

- **Run every # days**
  - Runs the job at regular intervals based on the number of days you specify.
Sub-schedule for data collection

Let's you specify the number of days after which you want to repeat the job. The option also lets you specify the last day until you want the job to continue running periodically.

The sub-schedule is a subset of the period that you specify in the Run every # days option.

This schedule collects the data for the assets for which data was never collected for the standards in the job scopes.

**Note:** The sub-schedule is applicable only to the data collection job.

10 In the **Add Result Viewers** panel, add the users or the groups that have the permissions to view the evaluation results and reports.

It is recommended to add the groups as the result viewers.

11 In the **Specify Notification Details** panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check **Send notification**, enter the following information and then click **Next**:

- Enter the subject and message of the notification mail.
- Enter the sender and the receiver email ID.

Notification can be sent to multiple recipients.

12 In the **Summary** panel, view the summary and click **Finish**.

The Create or Edit Collection-Evaluation-Reporting wizard also lets you configure the details to remediate the assets that are non-compliant.
To remediate the assets automatically

1. In the **Select Asset Type for Remediation Ticketing** panel, check the **Enable Automatic Remediation Action** option to configure the automatic remediation details.

   Select the asset types that correspond to the assets that were evaluated and click **Next**.

2. In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

   You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

   If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

   Click **Next**.

3. In the **Select Remediation Ticket Type** panel, select one of the following:

   - Create an email notification.
     This option lets you create an email notification that you want to send for notification.

   - Create a service desk ticket.
     This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.

     You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.

     See “**About closed-loop verification**” on page 664.

   Click **Next**.

4. If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

   If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

   You can check **Make this the default Email Notification template** if you want to use the same message for all the service desk ticket requests.
5 If you choose to create a service desk ticket as a remediation action, specify
the message that you want to send as a service desk request in the Configure
Service Desk Ticket panel. Click Next.

If you select Consolidate multiple assets in a single ticket/email, a single
service desk ticket is generated that includes all the non-compliant assets.

You can check Make this the default Service Desk Ticket template if you
want to use the same message for all the service desk ticket requests.

6 Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel.
See “Quick start with minimum configuration” on page 76.

Performing the asset tasks

You can perform the following asset tasks from the Asset System view:

- Import assets.
  See “Importing assets” on page 313.

- Edit assets.
  See “Editing assets” on page 391.

- Move assets.
  See “Moving an asset” on page 392.

- Export CSV headers.
  See “Exporting CSV headers” on page 393.

Editing assets

You can edit the asset field values using the Edit Assets dialog box.

The Edit Assets dialog box lets you edit the mandatory and the optional field
values along with the common fields for the selected asset. You can also add or
remove the tags from the Edit Assets dialog box.

Note: You can edit multiple assets of the same asset type collectively if you want
to specify common field values and tags to all assets.

To edit assets

1 In the table pane, right-click an asset that you want to edit.
   You can also select multiple assets at a time for editing.

2 Select Edit Assets.
3 In the **Edit Assets** dialog box, under the **Properties** tab specify or change the values of the fields.

The **Properties** tab presents the list of the editable fields for the selected asset type. The editable fields include the mandatory fields, the optional fields, and the common fields.

The boxes for all the fields are empty by default. The current value is retained if you do not specify any value for a field.

4 Under the Tags tab, click **Add Tag**.

5 In the Select Tags dialog box, select a tag that you want to apply to the asset and click **Add**.

6 Click **OK** in the Select Tags dialog box.

7 Click **OK**

**Moving an asset**

You use the right-click menu or the menu bar in the Control Compliance Suite Manage > Asset System view to move an asset from one location to another.

**To move an asset**

1 In the table pane, right-click an asset that you want to move.

2 Select **Move**.

3 In the **Move Asset** dialog box, select the destination folder to which you want to move the asset.

4 Click **OK**.

**Applying a tag to the asset**

You can apply one or more tags to a single asset.

**To assign a tag to the assets**

1 In the table pane, select one or more assets to which you want to assign a tag.

2 Right-click the assets and select **Edit Assets**.

3 In the Edit Assets dialog, in the Tags tab click **Add**.

4 In the Apply Tag dialog, select the tag from the Tags folder and click **Add**.

5 Click **OK**.

**Removing a tag from the asset**

You can remove the tag that is associated with the asset.
To remove a tag
1. In the table panel, select the asset for which you want to remove the tag.
2. Right-click the asset and select **Edit Assets**.
3. In the Edit Assets dialog, under the Tags tab select the tag that you want to remove and click **Remove**.
4. Click **OK** in the Edit Assets dialog.

**Exporting CSV headers**
You can export the CSV headers of the asset type for which you want to import the assets through the CSV data collector. With the list of CSV headers, you can create your own CSV files with more accuracy to import the assets of a particular asset type.

You can use the CSV headers to create the CSV file that can be used for importing the assets from the CSV data collector.

**To export the CSV headers**
1. Go to Manage > Assets > Asset System.
2. Select an asset type from the **Display** drop-down list.
3. From the **Asset Tasks** in the taskbar, select **Export CSV Headers**.
4. Select the location where you want to save the CSV file.

See “**Importing asset-specific and common fields using the CSV data collector**” on page 335.

**Performing the common tasks**
You can perform the following common tasks from the Asset System view:
- **View permissions**
  See “**Viewing permissions on the asset folders and asset groups**” on page 394.
- **Delete**
  See “**Deleting assets or asset groups**” on page 393.

**Deleting assets or asset groups**
You can delete one or more assets or asset groups from the Asset System view.

**Note**: You cannot delete an asset that is used as a control point for which the review cycle is progress.
To delete the assets or the asset groups

1. Go to Manage > Assets > Asset System.
2. From the table pane select the assets or the asset groups that you want to delete.
3. From the Common Tasks, click **Delete**.

See “Moving an asset” on page 392.

Viewing permissions on the asset folders and asset groups

You can view the permissions that are associated with the asset folder or an asset group from the Asset System view.

**To view the permissions on the asset folder and asset groups**

1. Go to **Manage > Asset System**.
2. In the asset system view, do one of the following:
   - In the tree pane, right-click the asset folder or the asset group for which you want to view permissions and select **View Permissions**.
   - In the table pane, right-click the asset folder or the asset group for which you want to view the permissions and select **View Permissions**.
   - In the **Permissions** tab of the Details pane, view the permissions on the asset folder or the asset group that is selected in the table pane.
3. In the **View Permissions** dialog box, view the permissions that are displayed in tabular form.
4. Select **View my permissions** to view the permissions that are assigned to the logged-in user on the selected asset folder or asset group.

Viewing asset information in the details pane

You can view the information about the assets in the details pane.

**To view the asset information**

1. In the table pane, select the asset for which you want to view the information.
2. View the information for the selected asset in the details pane.

The details pane displays all the information about the selected asset in the following tabs:

- **General**
  - See “**Asset details pane- General tab**” on page 395.
- **Asset-type Properties**
See “Asset details pane- Asset-type Properties tab” on page 397.

■ Custom Properties
See “Asset details pane- Custom Properties tab” on page 398.

■ Errors
See “Asset details pane- Errors tab” on page 398.

■ Data Collection
See “Asset details pane- Data Collection tab” on page 399.

■ Evaluation
See “Asset details pane- Evaluation tab” on page 399.

■ Tags
See “Asset details pane- Tags tab” on page 400.

■ Exceptions
See “Asset details pane- Exceptions tab” on page 401.

■ Permissions
See “Asset details pane- Permissions tab” on page 401.

**Asset details pane- General tab**

The General tab of the asset details pane provides general information about the selected asset.

The General tab contains the following details about the assets:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset name</td>
<td>Displays the name of the asset.</td>
</tr>
<tr>
<td>Asset type</td>
<td>Displays the asset type.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Displays the date when the asset or the asset group was created.</td>
</tr>
<tr>
<td>Last modified date</td>
<td>Displays the date when the asset or the asset group was last modified.</td>
</tr>
<tr>
<td>Last evaluation date</td>
<td>Displays the date when the asset or the asset group was last evaluated.</td>
</tr>
</tbody>
</table>
Confidentiality Displays one of the following states for confidentiality:

- Not Defined
  This is represented by 0 in the CCS directory.
- Low
  This is represented by 1 in the CCS directory.
- Medium
  This is represented by 2 in the CCS directory.
- High
  This is represented by 3 in the CCS directory.

**Note:** If you specify the value of this field in the CSV file as anything greater than 3, the asset system marks it as NotDefined.

Integrity Displays one of the following states for integrity:

- Not Defined
  This is represented by 0 in the CCS directory.
- Low
  This is represented by 1 in the CCS directory.
- Medium
  This is represented by 2 in the CCS directory.
- High
  This is represented by 3 in the CCS directory.

**Note:** If you specify the value of this field in the CSV file as anything greater than 3, the asset system marks it as NotDefined.

Availability Displays one of the following states for availability:

- Not Defined
  This is represented by 0 in the CCS directory.
- Low
  This is represented by 0 in the CCS directory.
- Medium
  This is represented by 0 in the CCS directory.
- High
  This is represented by 0 in the CCS directory.

**Note:** If you specify the value of this field in the CSV file as anything greater than 3, the asset system marks it as NotDefined.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance score</td>
<td>Displays the overall compliance score of the assets in the asset group that is derived from all the sources.</td>
</tr>
<tr>
<td>Risk Score</td>
<td>Displays the overall risk score of the assets in the asset group that is derived from all the sources.</td>
</tr>
<tr>
<td>Risk Rating</td>
<td>Displays the risk rating. The risk rating is the highest risk score of all the risk scores that are derived from all the sources.</td>
</tr>
</tbody>
</table>

See “Using a Pre rule to set the values of the common fields” on page 309.

See “Asset details pane- General tab” on page 395.

See “Asset details pane- Asset-type Properties tab” on page 397.

See “Asset details pane- Custom Properties tab” on page 398.

See “Asset details pane- Errors tab” on page 398.

See “Asset details pane- Data Collection tab” on page 399.

See “Asset details pane- Evaluation tab” on page 399.

See “Asset details pane- Tags tab” on page 400.

See “Asset details pane- Permissions tab” on page 401.

**Asset details pane- Asset-type Properties tab**

The Asset-type properties tab of the Asset details pane provides information about the asset type.

The Asset-type Properties tab contains the primary, mandatory, and optional fields for the selected asset types.

The Asset-type Properties tab contains the information about the following common fields:

- Asset Custodian
- Asset Department
- Asset Location
- Asset Owner
- Asset Site

You can set the values of the common fields, mandatory fields, and optional fields from the Asset-type Properties tab.

See “Predefined asset types” on page 236.
See “Using a Pre rule to set the values of the common fields” on page 309.
See “Asset details pane- General tab” on page 395.
See “Asset details pane- Custom Properties tab” on page 398.
See “Asset details pane- Errors tab” on page 398.
See “Asset details pane- Data Collection tab” on page 399.
See “Asset details pane- Evaluation tab” on page 399.
See “Asset details pane- Tags tab” on page 400.
See “Asset details pane- Permissions tab” on page 401.

**Asset details pane- Custom Properties tab**

The Custom Properties tab presents the fields that are newly added to the asset type from the Schema Manager.

The Custom Properties tab includes the following fields:

- New external fields that are added to the asset type
- New optional fields that are added to the asset type

See “Extending an existing asset type” on page 451.

See “Using a Pre rule to set the values of the common fields” on page 309.
See “Asset details pane- General tab” on page 395.
See “Asset details pane- Asset-type Properties tab” on page 397.
See “Asset details pane- Errors tab” on page 398.
See “Asset details pane- Data Collection tab” on page 399.
See “Asset details pane- Evaluation tab” on page 399.
See “Asset details pane- Tags tab” on page 400.
See “Asset details pane- Permissions tab” on page 401.

**Asset details pane- Errors tab**

The Errors tab lists the errors that occur while running a job for the selected asset.

See “Using a Pre rule to set the values of the common fields” on page 309.
See “Asset details pane- General tab” on page 395.
See “Asset details pane- Asset-type Properties tab” on page 397.
See “Asset details pane- Custom Properties tab” on page 398.
See “Asset details pane- Data Collection tab” on page 399.
See “Asset details pane- Evaluation tab” on page 399.
See “Asset details pane- Tags tab” on page 400.
See “Asset details pane- Permissions tab” on page 401.

**Asset details pane- Data Collection tab**

The Data Collection tab contains the details of the assets for which the data has been collected.

The Data Collection tab presents a View Details icon. You can view the details of the data collection job run.

See “Using a Pre rule to set the values of the common fields” on page 309.
See “Asset details pane- General tab” on page 395.
See “Asset details pane- Asset-type Properties tab” on page 397.
See “Asset details pane- Custom Properties tab” on page 398.
See “Asset details pane- Errors tab” on page 398.
See “Asset details pane- Evaluation tab” on page 399.
See “Asset details pane- Tags tab” on page 400.
See “Asset details pane- Permissions tab” on page 401.

**Asset details pane- Evaluation tab**

The Evaluations tab contains the list of the evaluations.

You can view the details of the assets that are evaluated against a standard in the Details pane.

The Details pane presents the following information about the evaluation:
- Standard against which the evaluation job was run
- Evaluation date
- Checks evaluated
- Checks not evaluated
- Compliance score
- Risk score

See “Using a Pre rule to set the values of the common fields” on page 309.
See “Asset details pane- General tab” on page 395.
See “Asset details pane- Asset-type Properties tab” on page 397.
See “Asset details pane- Custom Properties tab” on page 398.
See “Asset details pane- Errors tab” on page 398.
See “Asset details pane- Data Collection tab” on page 399.
See “Asset details pane- Tags tab” on page 400.
See “Asset details pane- Permissions tab” on page 401.

Viewing the evaluation results in the details pane

You can view the details of the assets that are evaluated against a standard in the Details pane.

The details pane presents the following information about the evaluation:
- Standard against which the evaluation job was run
- Evaluation date
- Checks evaluated
- Checks not evaluated
- Compliance score
- Risk score

To get the asset based view of the evaluation results

1. Go to Manage > Assets > Asset System.
2. Select the assets for which you have run the evaluation job.
3. In the Details pane, select the Evaluation tab.
4. Click the View Details icon at the top right corner of the Details pane.
5. View the asset-based detailed information about the evaluation.

See “Working with Evaluation Results” on page 653.
See “Running an evaluation job from the Asset System view” on page 383.

Asset details pane- Tags tab

The Tags tab contains the list of all the tags that are associated with the selected asset.

The Tags tab also lets you add a new tag to associate with the selected asset.

You can also remove a tag that is already associated with the asset from the Tags tab.
See “Using a Pre rule to set the values of the common fields” on page 309.
See “Asset details pane- General tab” on page 395.
See “Asset details pane- Asset-type Properties tab” on page 397.
See “Asset details pane- Custom Properties tab” on page 398.
See “Asset details pane- Errors tab” on page 398.
See “Asset details pane- Data Collection tab” on page 399.
See “Asset details pane- Evaluation tab” on page 399.
See “Asset details pane- Permissions tab” on page 401.

**Asset details pane- Permissions tab**

The Permissions tab of the Asset System details pane presents a list of permissions that are associated with the asset folder or the asset group selected in the table pane.

Use the **View my permissions** checkbox if you want to view the permissions that are assigned to the logged-in user on the selected asset folder.

See “Asset details pane- General tab” on page 395.
See “Asset details pane- Asset-type Properties tab” on page 397.
See “Asset details pane- Custom Properties tab” on page 398.
See “Asset details pane- Errors tab” on page 398.
See “Asset details pane- Data Collection tab” on page 399.
See “Asset details pane- Evaluation tab” on page 399.
See “Asset details pane- Tags tab” on page 400.
See “Asset details pane- Exceptions tab” on page 401.

**Asset details pane- Exceptions tab**

The Exceptions tab lists all the exceptions that are applied to the selected asset.

See “Using a Pre rule to set the values of the common fields” on page 309.
See “Asset details pane- General tab” on page 395.
See “Asset details pane- Asset-type Properties tab” on page 397.
See “Asset details pane- Custom Properties tab” on page 398.
See “Asset details pane- Errors tab” on page 398.
See “Asset details pane- Data Collection tab” on page 399.
See “Asset details pane- Evaluation tab” on page 399.
See “Asset details pane- Tags tab” on page 400.
See “Asset details pane- Permissions tab” on page 401.

Using the Filter by pane in the Asset System view

The Filter by pane contains the filters that you can use to display only the required assets.

The Control Compliance Suite provides the following default filters for filtering the assets:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select tags</strong></td>
<td>Lets you filter the assets according to the specified tags. You can browse to add the tags in the Tags list.</td>
</tr>
<tr>
<td></td>
<td>You can select either of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Match any</td>
</tr>
<tr>
<td></td>
<td>Displays the assets that match any one of the listed tags.</td>
</tr>
<tr>
<td></td>
<td>■ Match all</td>
</tr>
<tr>
<td></td>
<td>Displays the assets that match all the listed tags.</td>
</tr>
<tr>
<td></td>
<td>See “Select tags filter” on page 404.</td>
</tr>
<tr>
<td><strong>Risk Ratings</strong></td>
<td>Lets you filter the existing assets according to the specific risk rating that is associated with the assets.</td>
</tr>
<tr>
<td></td>
<td>You can select the rating of Confidentiality, Integrity, and Availability from the drop-down list that is shown at each of the risk types.</td>
</tr>
<tr>
<td></td>
<td>The assets that possess the selected risk rating are displayed in the table pane.</td>
</tr>
<tr>
<td></td>
<td>See “Risk Rating filter” on page 403.</td>
</tr>
<tr>
<td><strong>Created Between</strong></td>
<td>Lets you select the dates to display the assets that are created between the selected dates.</td>
</tr>
<tr>
<td></td>
<td>See “Created Between filter” on page 404.</td>
</tr>
<tr>
<td><strong>Modified Between</strong></td>
<td>Lets you select the dates to display the assets that are updated between the selected dates.</td>
</tr>
<tr>
<td></td>
<td>See “Modified Between filter” on page 404.</td>
</tr>
</tbody>
</table>
If you specify values for more than one filters, all the selected filters are considered when the assets are displayed in the table pane. In case you select more than one values for a single filter only one of the values is considered when the assets are displayed in the table pane.

For example:

If you specify values for the Tags, Risk Ratings, Created Between, and Modified Between filters, all the filters are considered. If you select two tags in the tags filter only one of the tags is considered. If you select values for the Confidentiality, Integrity, and Availability rating, only one of the values is considered.

You can customize the filter options in the Filter by pane.

**To customize the filter options**

1. In the Filter by pane, click the **Customize** icon.

2. In the **Customize Filters** dialog box, from the list box select the filter type to edit.

3. For the selected filter type, you can do any of the following:
   - Select or deselect the Display filter type check box. If you deselect the filter type, the filter type and its options are not displayed in the Filter by pane.
   - Use the arrow icons to move the options between Display and Do not display boxes.
   - Use the Move up and Move Down icons to change the order of the options that is displayed in the Filter by pane.

4. Click **Save Changes**.

See “**Customizing the filter options**” on page 67.

See “**Select tags filter**” on page 404.

See “**Risk Rating filter**” on page 403.

See “**Created Between filter**” on page 404.

See “**Modified Between filter**” on page 404.

**Risk Rating filter**

You can use the Risk rating filter when you want to filter the existing assets according to the specific risk rating that is associated with the assets. You can select the rating of Confidentiality, Integrity, and Availability from the drop-down list that is shown at each of the risk types. The assets that possess the selected risk rating are shown in the table pane.
To edit the filter, click the Customize icon at the top of the Filter by pane.

See “Using the Filter by pane in the Asset System view” on page 402.

See “Customizing the filter options” on page 67.

Select tags filter

You can use the Select tags filter when you want the assets with specific tags to be displayed in the tree pane.

In the Filter by pane, under the Select tags section, you can either choose the options "Match any" or "Match all".

You can also use the Browse option to browse and select specific tags.

You can also edit the filter, with the Customize icon at the top of the Filter by pane.

See “Using the Filter by pane in the Asset System view” on page 402.

See “Customizing the filter options” on page 67.

Created Between filter

The Created Between filter lets you select a time period to display the assets that were created between the specified dates.

See “Using the Filter by pane in the Asset System view” on page 402.

See “Customizing the filter options” on page 67.

Modified Between filter

The Modified Between filter lets you select two dates. The assets that were modified between the specified dates are displayed in the table pane.

See “Using the Filter by pane in the Asset System view” on page 402.

See “Customizing the filter options” on page 67.

Performing the tasks in the Reconciliation Rules view

You can perform the following tasks from the Manage > Assets > Reconciliation Rules view:

■ Create rule.
  See “Creating reconciliation rules” on page 306.

■ Copy and paste rule
  See “Copying and pasting a reconciliation rule” on page 406.
- Delete rule.
  See “Deleting a reconciliation rule” on page 406.
- Move rule
  See “Moving a reconciliation rule” on page 405.
- Edit rule.
  See “Editing a reconciliation rule” on page 405.
- View reconciliation rules details pane.
  See “Viewing rules information in the details pane” on page 406.
- Use Filter by pane.
  See “Using the Filter by pane in the Reconciliation Rules view” on page 407.

**Editing a reconciliation rule**

You can edit only one reconciliation rule at a time. You cannot edit the rule type, the asset type, and the rule folder. You can edit the name of the rule, and the conditions and the actions associated with the rule.

**To edit the reconciliation rule**

1. Use the check box to select a rule from the table pane.
2. Click **Edit Rule** from the menu bar.
3. In the **Edit Reconciliation Rules** wizard, in the Select Rule Type and Name panel, edit the name of the rule.
4. Click **Next**.
5. In the **Select Rule Condition and Action** panel, add or remove the conditions and actions.
6. Click **Next**.
7. Click **Finish** in the Summary panel.

**Moving a reconciliation rule**

You use the right-click menu or the menu bar in the Control Compliance Suite Console to move a rule from one location to another.

**To move a rule**

1. In the table pane, use the check box to select a rule.
2. Select **Move Rules** from the menu bar.
3  In the **Move Rules** dialog box, select the destination folder to which you want to move the rule.

4  Click **OK**.

### Copying and pasting a reconciliation rule

You can copy and paste a reconciliation rule to any other folder under the Reconciliation Rules in the tree pane.

**To copy and paste the reconciliation rule**

1  In the table pane, right-click the rule that you want to copy.
   
   You can select multiple rules to copy.

2  Select **Copy Rule**.

3  In the tree pane, right-click the folder in which you want to paste the rule.

4  Select **Paste Rule**.

### Deleting a reconciliation rule

You delete the reconciliation rules with the Delete Rule option in the task bar.

**To delete a rule**

1  Go to Manage > Assets > Reconciliation Rules.

2  In the table pane, select one or more rules of the same rule type.

3  From the task bar, click **Delete Rule**.

4  Click **OK** on the confirmation message box.

### Viewing rules information in the details pane

You can view the information about the reconciliation rules in the details pane.

**To view the rules information**

1  In the table pane, select the rule for which you want to view the information.

2  View the information for the selected asset in the details pane.

   See “Creating reconciliation rules without manual review” on page 306.

   See “Creating reconciliation rules using the manual review” on page 307.

### Marking a rule as default

You can mark any of the predefined reconciliation rules as default rules.
See “Predefined reconciliation rules” on page 284.

If you mark a rule as default, the asset import job uses the default rule to import the assets. You need not specify the reconciliation rule that must be used in the asset import job in case you mark a rule as default.

To mark a rule as default

1. Go to Manage > Asset System > Reconciliation Rules.
3. In the table pane, select a rule that you want to mark as default.
4. From the Common Tasks, click Mark as Default Rule.

See “Unmarking a rule as default” on page 407.

Unmarking a rule as default

You can unmark any of the predefined reconciliation rules that are already marked as default rules.

See “Predefined reconciliation rules” on page 284.

If you mark a rule as default, the asset import job uses the default rule to import the assets. You need not specify the reconciliation rule that must be used in the asset import job in case you mark a rule as default.

You can unmark the default rule.

To unmark a rule as default

1. Go to Manage > Asset System > Reconciliation Rules.
2. In the table pane, select a rule that you want to unmark as default.
3. From the Common Tasks, click Unmark as Default Rule.

See “Marking a rule as default” on page 406.

Using the Filter by pane in the Reconciliation Rules view

The Filter by pane of the Manage > Assets > Reconciliation Rules view contains the filters that you can use to display only the required reconciliation rules.

The Control Compliance Suite provides the following default filters for filtering the reconciliation rules:
**Asset Types**

Lets you filter the reconciliation rules to display only the rules that are associated with a particular asset type.

See “Asset Type filter” on page 408.

**Rule Types**

Lets you filter the reconciliation rules to display only a particular type of rules.

See “Rule Type filter” on page 408.

You can customize the filter options in the Filter by pane.

**To customize the filter options**

1. In the Filter by pane, click the **Customize** icon.

2. In the **Customize Filters** dialog box, from the list box select the filter type to edit.

3. For the selected filter type, you can do any of the following:
   - Select or deselect the Display filter type check box. If you deselect the filter type, the filter type and its options are not displayed in the Filter by pane.
   - Use the arrow icons to move the options between Display and Do not display boxes.
   - Use the Move up and Move Down icons to change the order of the options that is displayed in the Filter by pane.

4. Click **Save Changes**.

See “Customizing the filter options” on page 67.

**Rule Type filter**

The Rule Type filter lets you select a type of the rule from the Pre, Add, Update, and Post. The rules of the selected type only are displayed in the table pane.

See “Customizing the filter options” on page 67.

See “Using the Filter by pane in the Reconciliation Rules view” on page 407.

**Asset Type filter**

You can use the Asset Type filter when you want to filter the existing assets according to the specific asset types. From the list of asset types, you can select the corresponding check boxes to select the specific asset types. The assets of the selected asset type are shown in the table pane.
To edit the filter, click the Customize icon at the top of the Filter by pane.

See “Using the Filter by pane in the Asset System view” on page 402.

See “Customizing the filter options” on page 67.

See “Using the Filter by pane in the Reconciliation Rules view” on page 407.
Performing the tasks in the Reconciliation Rules view
Importing assets from Altiris

This chapter includes the following topics:

■ About importing assets from Altiris
■ Supported asset types for Altiris
■ Prerequisites for installing Control Compliance Suite Asset Export Task
■ Installing Asset Export Task on Altiris Notification Server
■ Working with the Altiris Asset Export Task solution
■ Creating the Altiris asset import jobs in Control Compliance Suite Console
■ Specifying the asset export settings in the Altiris Symantec Management Console
■ Creating a asset export task in the Altiris Symantec Management Console
■ Scheduling asset export task in the Altiris Symantec Management Console
■ About the CSV files on Altiris Notification Server

About importing assets from Altiris

Control Compliance Suite (CCS) provides the CCS Asset Export Task solution to import certain types of assets from the Altiris Configuration Management Database (CMDB) to the CCS database. Windows and UNIX are the predefined asset types that are supported.

The CCS Asset Export Task solution must be installed on the Altiris Notification Server before you can export the assets.
See “Installing Asset Export Task on Altiris Notification Server” on page 413.

When you install the CCS Asset Export Task solution, it becomes part of the Altiris Symantec Management Console. Most of the functionality appears in the Manage > Jobs and Tasks > Notification Server option.

The Altiris Symantec Management Console is a Web-based user interface that is the primary tool for interacting with Notification Server and installed solutions. The CCS Asset Export Task solution does the following:

- Exports assets from the Altiris CMDB to a CSV file.
- Runs an asset import job on CCS. The asset import job imports assets from the CSV file to the CCS asset system. The assets are imported using a CSV data collector.

If any resource is deleted from the Altiris CMDB, the corresponding asset is not deleted from the CCS asset system.

See “Supported asset types for Altiris” on page 412.

See “Working with the Altiris Asset Export Task solution” on page 414.

**Supported asset types for Altiris**

Only the Windows and UNIX asset types are exported from the Altiris Configuration Management Database (CMDB) database.

If the required attributes for Control Compliance Suite (CCS) are not available in the Altiris CMDB, those assets are not imported.

The following attributes are exported for the Windows computers:

- Domain\workgroup name
- Machine name
- Operating system Major version number
- Operating system Minor version number
- Operating system Type
- Machine Is Server
- Machine Is BDC
- Machine Is PDC
- SourceID
- Source
The following attributes are exported for the UNIX computers:

- Machine name
- IP address
- Operating system
- Operating Distribution Field
- Operating system Version
- SourceID
- Source

See “About importing assets from Altiris” on page 411.

Prerequisites for installing Control Compliance Suite Asset Export Task

You must have the following products to successfully download and install the Control Compliance Suite (CCS) Asset Export Task solution:

- Symantec Install Manager
  You must use the latest Symantec Install Manager to install the CCS solution.

- Altiris Notification Server 7.0
  You must have the Altiris Notification Server 7.0 on which to install the CSS solution.

See “About importing assets from Altiris” on page 411.

Installing Asset Export Task on Altiris Notification Server

You use Symantec Installation Manager to install the Control Compliance Suite (CCS) Asset Export Task solution.

You must install the solution on Altiris Notification Server 7.0.

To install the CCS Asset Export Task

1. Start Symantec Installation Manager.
2. On the Installed Products page, click Install new products.
3. On the Install New Products page, check CCSAssetExport, and then click Review selected products.
4 On the **Selected Products and Features** page, verify that you selected the correct product, and then click **Next**.

5 On the **End User License Agreement** page, check **I accept the terms in the license agreements**, and then click **Next**.

6 On the **Contact Information** page, type the required information, and then click **Next**.

7 On the **Computers to Manage** page, click **Begin install** to begin the installation.

8 On the **Installation Complete** page, click **Finish**.

You can now launch the Symantec Management Console to access the CCS Asset Export Task solution.

See “**Working with the Altiris Asset Export Task solution**” on page 414.

See “**About importing assets from Altiris**” on page 411.

---

**Working with the Altiris Asset Export Task solution**

You must perform certain tasks on Control Compliance Suite (CCS) and Altiris Notification Server to import assets successfully from the Altiris CMDB.

In the CCS console, perform the following tasks:

- Configure a CSV data collector to import assets from the CSV file on Altiris Notification Server.
  
  See “**Configuring the CSV data collector**” on page 156.

- Create asset import jobs for Windows and UNIX asset types.
  
  See “**Creating the Altiris asset import jobs in Control Compliance Suite Console**” on page 415.

In the **Altiris Symantec Management Console**, perform the following tasks:

- Provide the Web Service URL to import assets into the CCS asset system.
  
  See “**Specifying the asset export settings in the Altiris Symantec Management Console**” on page 416.

- Create a CCS asset export task.
  
  See “**Creating a asset export task in the Altiris Symantec Management Console**” on page 417.

- Schedule the CCS asset export task.
  
  See “**Scheduling asset export task in the Altiris Symantec Management Console**” on page 418.

See “**About importing assets from Altiris**” on page 411.
Creating the Altiris asset import jobs in Control Compliance Suite Console

The CSV data collector is used to import the assets from the Altiris CMDB database to the Control Compliance Suite (CCS) asset system. You must configure the CSV settings for the Windows and UNIX platforms to import the assets.

See “Configuring the CSV data collector” on page 156.

To create an Altiris asset import job

1. In the CCS console, go to Manage > Assets > Asset System.
2. On the taskbar, from the Asset Tasks select Import Assets.
3. In the Specify Name and Description panel, in the Name box, type the name for the import job.

   You can optionally type the description for the import job and click Next.
4. In the Select Platform, Asset Type, and Data Collector panel, do the following:
   - Select the platform and the asset type for which to import the assets. Windows and UNIX are the predefined asset types that are supported.
   - From the Data collector drop-down list, select CSV Data Collector and click Next.
5. In the Select Asset Import Scope panel, do the following:
   - Click the browse ... icon to select the scope for the asset type.
     Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.
     See “About scopes in asset import” on page 349.
   - In the Limit Asset Import Scope dialog box, select the additional scope from the list of the supported scopes and click OK.
   - In the Select Asset Import Scope dialog box, in the left pane, browse through the assets hierarchy and select a folder to add the assets from. In the right pane, select the folder, asset group, or asset and then click Add to add it as a scope. Click Next.
6. In the Add Reconciliation Rules panel, you can add, delete, and move the order of the reconciliation rules.

To add rules, do the following:
   - Click Add Rules.
In the Select Reconciliation Rules panel, browse through the Reconciliation Rules folder and use the Add option to add the existing reconciliation rules to the import job. Click OK.

In the Add Reconciliation Rules panel, click Next.

7 In the Specify Asset Field Filters panel, you can configure the asset field filters. The fields in this panel are specific to the asset type that you want to import. You can select a field that should be used as a filter for the selected asset type and create a filter statement.

To add a filter, do the following:
- Select a statement from the drop-down list, and click Add Statement.
- In the Create Filter Statement dialog box, use the parameter type and the conditions to create a filter statement and click OK. See “Examples of asset filters” on page 292.
  See “Filter statement operators” on page 293.
- After you add the filters, click Next.

8 In the Schedule panel, select any one of the schedule options.

9 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:
- Type the subject and message of the notification mail.
- Type the email ID of the sender and the receiver.

10 In the Summary panel, review the configurations for the import job and click Finish.

You can go to the Monitor > Jobs view to monitor the current status of the job.

See “About importing assets from Altiris” on page 411.

Specifying the asset export settings in the Altiris Symantec Management Console

You must specify the Control Compliance Suite (CCS) asset export task settings to run the CCS asset import jobs.

The asset import job in CCS is run using a CCS Web Service. You must provide the URL to the Web Service to import the assets into the CCS asset system.
To specify the settings

1. In the Altiris Notification Server Management Console, in the Settings menu, click Notification Server > CCS Asset Export Task Setting.

2. Type the Web Service URL. If SSL is enabled, use https://.
   `http://<webservicehostname>/CCS_WebServices/AssetImportService.asmx`

3. Type the number of days that you want to retain a CSV file. Any CSV files that are older than the number of days entered is deleted from the folder.

4. Click OK to save.

See “About importing assets from Altiris” on page 411.

Creating a asset export task in the Altiris Symantec Management Console

The Control Compliance Suite (CCS) Asset Export Task must be installed on Notification Server before you can run the task.

See “Installing Asset Export Task on Altiris Notification Server” on page 413.

When you create a new task, there may be a time delay to store the credentials. Therefore, if you schedule to run a job immediately after you create a new task, the job might fail. You may have to reschedule the job.

To create a CCS asset export task

1. In the Altiris Notification Server Management Console, in the Manage menu, click Jobs and Tasks.

2. In the left pane, expand Jobs and Tasks > System Jobs and Tasks > Notification Server.

3. Right-click Notification Server and select New > Job or Task.
On the **Create New Task** page, type the following information:

**Specify export location**
Type the location where the CSV files are stored.
See “About the CSV files on Altiris Notification Server” on page 419.

**Specify credentials**
Type the user name and the password that is required to access the CSV file and run the asset import job on CCS.

**Specify import job to run**
Select the asset import job.
The listed asset import jobs are created in CCS.
See “Creating the Altiris asset import jobs in Control Compliance Suite Console” on page 415.

1. Click **Apply**.
2. Select the computers for which you want to run the asset import job.
3. Click **OK**.

After you create an export task, you must set up the schedule to run the task.

See “Scheduling asset export task in the Altiris Symantec Management Console” on page 418.

See “About importing assets from Altiris” on page 411.

---

**Scheduling asset export task in the Altiris Symantec Management Console**

After you create a Control Compliance Suite (CCS) asset export task, you must schedule the task to export the assets to a CSV file. The assets are then imported into the CCS asset system from the CSV file.

When you create a new task, there may be a time delay to store the credentials. Therefore, if you schedule to run a job immediately after you create a new task, the job might fail. You may have to reschedule the job.

**To schedule the CCS asset export task**

1. In the Altiris Notification Server Management Console, in the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Notification Server**.
3 In the left pane, under **Notification Server**, select the task to schedule.

4 In the **New Schedule** page, provide the following information:
   - **Now** Select this option if you want to run the job immediately.
   - **Schedule** Select this option if you want to run the job at a specified time.

5 Click **Schedule**.
   You can now go to the CCS console's **Monitor > Jobs** view to monitor the status of the job.

See “Creating a asset export task in the Altiris Symantec Management Console” on page 417.

See “About importing assets from Altiris” on page 411.

### About the CSV files on Altiris Notification Server

When the scheduled Control Compliance Suite asset export task runs, the resources from the Altiris Configuration Management Database (CMDB) are exported to a CSV file. The resources that are exported depends on the type of asset import job that is selected in the task. A CSV file is created per asset type. The CSV files are purged according to the settings in the CCS Asset Export Task Setting page.

See “Specifying the asset export settings in the Altiris Symantec Management Console” on page 416.

On the Notification Server, the CSV files are created with the following syntax:

```
CCS_<AssetType>_<DateTime>_<GUID>.csv
```

See “About importing assets from Altiris” on page 411.

See “Creating a asset export task in the Altiris Symantec Management Console” on page 417.
Importing incident data from Symantec Data Loss Prevention

This chapter includes the following topics:

- About importing incident data from Symantec Data Loss Prevention
- Configuring the Symantec Data Loss Prevention Connector
- About rules-based action execution
- Managing controls for Symantec Data Loss Prevention Connector
- About Symantec Data Loss Prevention Connector logging
- Using the Symantec Data Loss Prevention Connector Credentials Removal utility
- Using the Symantec CSM Connector Executor utility

About importing incident data from Symantec Data Loss Prevention

Symantec Data Loss Prevention (DLP) lets you discover and protect the confidential data that is stored in files, in databases, and on endpoints. DLP raises an incident when it detects a violation in a policy. DLP stores the incident records in the database. DLP uses reports to query the database for incidents. Each report is assigned a unique ID within DLP.
The Symantec Data Loss Prevention Connector lets you import this incident data into the Control Compliance Suite (CCS). You can incorporate incident data into reports and dashboards in CCS. You can also use the incident data to trigger rule-based actions on the CCS assets.

Before you can import the Symantec DLP incident data into CCS, you must configure the DLP Connector. You must also enable and configure DLP Web Services.

Symantec Data Loss Prevention Connector requires Symantec Data Loss Prevention 10.0 or later.

See “About the Symantec Data Loss Prevention Connector” on page 422.

See “Configuring the Symantec Data Loss Prevention Connector” on page 423.

About the Symantec Data Loss Prevention Connector

The Symantec Data Loss Prevention Connector is an interface between your deployments of the Symantec Data Loss Prevention (DLP) and the Control Compliance Suite (CCS). The DLP Connector lets you import the incident data from the Symantec DLP and use CCS to generate reports and dashboards.

The DLP Connector uses the DLP Web service reporting API to connect to the Symantec DLP Enforce Server. The Web service reporting API is exposed on the Symantec DLP Enforce Server.

The DLP Connector does the following:

- Gathers the incident data from the reports that are created on the Symantec DLP Enforce Server.
- Stores the incident data in the extended evidence system database.
- Optionally performs the rule-based actions on the CCS assets.

See “About rules-based action execution” on page 432.

See “About the extended evidence sources system” on page 809.

Roles and permissions for the Symantec Data Loss Prevention Connector

The Symantec Data Loss Prevention Connector runs as service on your local computer. You must assign the account that you use for the DLP Connector service to one or more Control Compliance Suite (CCS) roles.

The roles must grant the account permission to do the following:

- View assets.
View asset reconciliation rules.
Manage evidence definitions.
Import assets.
Manage assets and asset groups.

The user account must also have permissions on the CCS asset system to successfully execute asset resolution tasks.

See “Configuring roles and permissions” on page 95.
See “Adding users and groups to a role” on page 107.
See “Assigning permissions from the Roles view” on page 109.
See “Assigning permissions from the Permission Management view” on page 113.

Configuring the Symantec Data Loss Prevention Connector

You must configure the Symantec Data Loss Prevention Connector (DLP) to import the Symantec DLP incident data into Control Compliance Suite (CCS) extended evidence sources. The CCS infrastructure can use the Symantec DLP incident data to generate reports and dashboards.

You must have a dedicated Symantec DLP Enforce Server user account for each DLP Connector. The user account that you configure for running the connector must have the Reporting API Web Service access permission.

Use the Symantec Data Loss Prevention Connector Configuration Wizard to configure the DLP Connector.

When you configure the DLP Connector, you do the following:

- Specify the address and credentials the connector uses to contact the DLP Enforce Server.
- Specify the DLP reports to collect incident data from.
- Map the DLP Status to the appropriate CCS result.
- Map the DLP Severity to the appropriate CCS Severity.
- Specify the CCS Application Server to use.
- Configure email notification.
- Schedule the connector to run automatically.
After you configure the DLP Connector, a new evidence source appears in the **Extended Evidence Sources** workspace. The new evidence source is named the **Symantec Data Loss Prevention Connector Source**.

**Note:** You must configure the DLP Connector in the context of a Symantec Data Loss Prevention Connector Service user.

See “About Symantec Data Loss Prevention and Control Compliance Suite result mapping” on page 430.

**To configure the DLP Connector**

1. From the Windows taskbar, go to **Start > All Programs > Symantec Corporation > Symantec Control Compliance Suite > DLP Connector Configuration Wizard**.

2. In the **Specify the Symantec Data Loss Prevention Enforce Server Connection** panel, enter the following information, and then click **Next**:

   - **Computer name**: Type the name of the computer that hosts the Symantec DLP Enforce Server.
   - **Port**: Type the port number that the Web service uses on the Symantec DLP Enforce Server host.
     - The default port number is 443.
   - **User name**: Type the user name that the DLP Connector uses to connect to the Symantec DLP Enforce Server.
     - The user account that you use must have the **Reporting API Web Service** access permission to successfully connect to the Symantec DLP Enforce Server.
   - **Password**: Type the password that the DLP Connector uses to authenticate the user account.
   - **Confirm password**: Re-type the password.

   The DLP Connector verifies the connection to the DLP Web services. An error message appears if the connection is not available.

3. If the certificate the DLP Connector uses is not installed, an error message appears. If the message appears, click **OK** to dismiss the message, then install the certificate.

   See “**Installing a certificate for the Symantec Data Loss Prevention Connector**” on page 427.
4 In the **Specify the Symantec Data Loss Prevention Saved Reports for Incident Collection** panel, do one of the following, and then click **Next**:

- **Add**
  
  Click **Add** to open the **Add Report Details** dialog box. You use the **Add Report Details** dialog box to add a new saved DLP report ID. The report ID uniquely identifies the report with DLP.

  In the **Add Reports Details** dialog box, enter the DLP report ID that the connector uses to collect incident data from the Symantec DLP Enforce Server. You can also enter a description of the report.

  If you specify an ID that already exists in the DLP Connector, an error message appears.

- **Modify**
  
  Click an existing saved report then click **Modify** to open the **Modify Report Details** dialog box. You use the **Modify Report Details** dialog to modify an existing saved report ID.

  You can change the report ID or the brief description about the saved report if required.

- **Remove**
  
  Click an existing saved report then click **Remove** to delete an existing saved report ID.

  You can find the Saved Report ID in the Symantec DLP Web console. The Saved Report ID is displayed in the status bar of the Web browser when you move the cursor over the Saved Report name.

5 In the **Specify the DLP Status to CCS Status Mapping** panel, do one of the following and then click **Next**:

- **Add**
  
  Click **Add** to open the **Add Status Mapping** dialog box. You can use the **Add Status Mapping** dialog box to map the DLP Status ID to an appropriate CCS result.

  The numeric value of the DLP Status ID appears in the DLP console status bar when the cursor is over the incident status attribute value.

- **Modify**
  
  Click an existing saved status mapping then click **Modify** to open the **Modify Status Mapping** dialog. The **Modify Status Mapping** dialog box you modify an existing status mapping.

- **Remove**
  
  Click an existing saved status mapping then click **Remove** to delete an existing status mapping.
6 In the Specify the DLP Severity to CCS Severity Mapping panel, select a row and click Modify to modify the default severity mapping.

In the Modify Severity Mapping dialog box, use the CCS Severity drop-down list to modify the severity mapping.

In the Specify the DLP Severity to CCS Severity Mapping, when you are satisfied with the severity mappings, click Next.

7 In the Specify the computer name and port for the Symantec Application Server Service panel, specify the following information:

- **Computer name**: Enter the name of the computer that hosts the CCS Application Server.
- **Port**: Type the port number the Application Server uses on the host. The default port is 1431.
- **Enable Symantec Data Loss Prevention Connector Rules Execution**: When the option is checked, the DLP Connector can use the rules-based action execution component.

Click Next. When you click Next, the wizard verifies the connection to the Application Server.

See “About rules-based action execution” on page 432.
8 In the Specify the Symantec Data Loss Prevention Email Notification Configuration panel, check Enable Email Notification to use email notifications.

When you use email notifications, users are sent a notification when the connector finishes collecting incident data collection.

If you click Enable Email Notification, you must enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server name</td>
<td>The name of the SMTP server to use for email notifications.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number to contact the SMTP server on.</td>
</tr>
<tr>
<td>From (Email ID)</td>
<td>The email address that appears in the From: line of the email notification.</td>
</tr>
<tr>
<td>To (Email IDs)</td>
<td>The email addresses the email notifications should be sent to.</td>
</tr>
</tbody>
</table>

You can type multiple email IDs. When you send to multiple addresses, separate the addresses with a comma (,).

See “About Symantec Data Loss Prevention Connector email notification configurations and logging” on page 428.

9 In the Specify the Symantec Data Loss Prevention Connector Schedule panel, click Modify to schedule the incident data collection. The DLP Connector uses the Windows Scheduler to trigger data collection.

When you have configured the schedule, click Next.

See “Scheduled task configurations for Symantec Data Loss Prevention Connector incident data collection” on page 430.

10 In the Summary panel, click Finish.

Installing a certificate for the Symantec Data Loss Prevention Connector

You must install the Symantec DLP Enforce Server certificate on the computer that hosts the DLP Connector. You use the Certificate Import Wizard to install the certificate.

**Note:** You must install a certificate under the context of a Symantec Data Loss Prevention Connector Service user.
To install a certificate

1. Browse to the following location on your local computer:

   #<user local application data store>\Symantec\Symantec Data Loss Prevention Connector


   The Symantec DLP Enforce Server certificate is stored in your local application data folder. The Symantec Data Loss Prevention.cer file is stored when the connection with the Symantec DLP Enforce Server is verified.

3. In the Certificate dialog box, click Install Certificate.

4. In the Welcome panel of the Certificate Import Wizard, click Next.

5. In the Certificate Store panel, do the following and then click Next.
   - Click Place all the certificates in the following store and then click Browse.
   - In the Select Certificate Store dialog box, select Trusted Root Certificate Authorities.
   - Click OK to close the Select Certificate Store dialog box.

6. In the Security Warning dialog, click Yes to install the certificate.

7. In the Completing the Certificate Import Wizard panel, click Finish.

8. In the successful certificate import message, click OK.

9. In the Certificate dialog box, click OK to close.

About Symantec Data Loss Prevention Connector email notification configurations and logging

When you configure email notifications, a notification is sent to the users when the connector finishes collecting incident data. Whenever an email notification is sent to the user, the email summary is recorded in the log file. The log file is on the computer that hosts the DLP Connector in the following location:

C:\Documents and Settings\All Users\Application Data\Symantec.CSM\Logs\ThirdPartyConnectors

The email summary is recorded in the log file along with a certain log level.

Table 7-1 contains the probable scenarios for email notifications and the corresponding log levels.
### Table 7-1
DLP Connector email notification configurations and the corresponding log levels

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Log level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any of the DLP Connector components encounters an error during execution.</td>
<td>The email summary is recorded in the log file with the Error Logging level.</td>
</tr>
<tr>
<td>The DLP Connector executes successfully and email notification feature is enabled. However, the email notification fails due to some reason.</td>
<td>The email summary is recorded in the log file with the Error Logging level.</td>
</tr>
<tr>
<td>If DLP Connector executes successfully and you have the email notification feature disabled.</td>
<td>If you have customized the log level in the ConnectorService.config file, the email summary is recorded in the log file with the Informational logging level. If the ConnectorService.config file is in the default configuration the email summary is not logged. <strong>Note:</strong> The default log level is Warning. If you want to see the logged email summary after a successful execution, then change the log level to Information.</td>
</tr>
</tbody>
</table>

See “Configuring the Symantec Data Loss Prevention Connector” on page 423. See “About Symantec Data Loss Prevention Connector logging” on page 440.

### Symantec Data Loss Prevention Connector incident data batch size

You can configure the number of incidents that you want Symantec Data Loss Prevention Connector to process in one batch. The default batch size value is 100. You can modify the default batch size in the DLPIncidentsConfiguration.xml file. The file is installed in the DLP Connector installation directory, which is normally:

```
#Symantec\CCS\Reporting and Analytics\Third Party Integration\Symantec Data Loss Prevention Connector
```

In the DLPIncidentsConfiguration.xml file, enter the value for the batch size in the following parameter:

```
<dlpIncidents batchSize=<input value>>
```
Note: You must restart the Symantec Data Loss Prevention Connector Service before you use the latest configuration.

See “Configuring the Symantec Data Loss Prevention Connector” on page 423.

Scheduled task configurations for Symantec Data Loss Prevention Connector incident data collection

When you schedule an incident data collection, the Symantec Data Loss Prevention Connector creates a new task in the Windows Scheduled tasks. The task is named Symantec Data Loss Prevention Connector task. You use this task to schedule the incident data collection.

The scheduled task is disabled by default. The incident data collection is scheduled at midnight every day by default. You should enable the schedule and provide the credentials of a user account for the task. The account you supply must have local admin privileges on the computer that hosts the DLP Connector.

You should configure your schedule according to the report configuration in Symantec Data Loss Prevention.

See “Configuring the Symantec Data Loss Prevention Connector” on page 423.

About Symantec Data Loss Prevention and Control Compliance Suite result mapping

Symantec Data Loss Prevention (DLP) triggers an incident when it detects a policy violation. The process of handling incidents goes through several stages from discovery to resolution. You may use various status attributes to identify an incident at various stages of the incident, such as “New”, “Investigation”, “Resolved” and so on. The default status attribute that DLP contains is “New”. Each status attribute contains a unique status ID.

The status ID displays in the DLP console status bar when you place the cursor over the incident status attribute value.

You map the DLP incident status attribute value to the Control Compliance Suite (CCS) result when you configure the DLP Connector. You must map the DLP status attribute to the CCS result before you collect incident data.

If the status mappings are not set, the DLP Connector generates an error and the incident data is ignored. These incidents are added to the error log file, which is located in the following location:

C:\Documents and Settings\All Users\Application Data\Symantec.CSM\Logs\ThirdPartyConnectors
You must ensure that the Symantec DLP status IDs that you use are appropriately mapped to the corresponding CCS result. CCS uses the following results:

- Pass.
- Fail.
- Neutral.
- Unknown.

Each DLP incident status attribute value has a numeric value that is assigned to it. As a CCS user, you must map the numeric value for the DLP incident status attribute value to the CCS result.

By default, the DLP incident status “New” that has the status ID “1” is mapped to “Failed” in CCS.

See “About the Symantec Data Loss Prevention Connector incident and Control Compliance Suite asset mapping” on page 431.

About the Symantec Data Loss Prevention Connector incident and Control Compliance Suite asset mapping

When the Symantec Data Loss Prevention Connector collects incident data, it resolves the IP addresses or the Hostnames in the incident data. The DLP Connector resolves the data to the corresponding Control Compliance Suite (CCS) assets. After a successful asset resolution, the DLP Connector adds an asset ID against each resolved incident data in the extended evidence sources.

Table 7-2 lists the Symantec Data Loss Prevention (DLP) incident types and the corresponding CCS asset type that the DLP Connector resolves the incident to.

<table>
<thead>
<tr>
<th>Incident type</th>
<th>Corresponding CCS asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint prevent</td>
<td>▪ Windows machine</td>
</tr>
<tr>
<td></td>
<td>▪ ESM agents</td>
</tr>
<tr>
<td>Discover file system</td>
<td>▪ Windows machine</td>
</tr>
<tr>
<td></td>
<td>▪ ESM agents</td>
</tr>
<tr>
<td>Discover endpoint file system</td>
<td>▪ Windows machine</td>
</tr>
<tr>
<td></td>
<td>▪ ESM agents</td>
</tr>
<tr>
<td>Discover file system scanner</td>
<td>▪ Windows machine</td>
</tr>
<tr>
<td></td>
<td>▪ ESM agents</td>
</tr>
<tr>
<td></td>
<td>▪ UNIX machine</td>
</tr>
</tbody>
</table>
Table 7-2  DLP incident type and the CCS asset mapping (continued)

<table>
<thead>
<tr>
<th>Incident type</th>
<th>Corresponding CCS asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover SQL database</td>
<td>■ SQL databases</td>
</tr>
<tr>
<td></td>
<td>■ SQL server</td>
</tr>
<tr>
<td></td>
<td>■ Oracle configured databases</td>
</tr>
<tr>
<td></td>
<td>■ Oracle configured servers</td>
</tr>
</tbody>
</table>

For Discover SQL Database incident data, the DLP Connector tries to perform asset resolution for the database first and then the server. For example, if a particular incident data concerns a SQL database and a SQL server, the DLP Connector tries to resolve the database first. If the SQL database asset is not present in the CCS asset system, then the DLP Connector tries to resolve the SQL server. The asset resolution is successful only if the asset that is involved in the incident is present in the CCS asset system.

**Note:** The DLP Connector does not perform any asset resolution for the remaining incidents types.

See “About Symantec Data Loss Prevention and Control Compliance Suite result mapping” on page 430.

**About rules-based action execution**

The Rules-based Actions Execution component lets you configure the actions that you want to execute automatically when collected incident data matches a particular condition. For example, if the incident data contains the policy name “PCI,” then you can tag the resolved asset as “PCI.”

By default, the Symantec Data Loss Prevention Connector can perform the following actions on resolved assets:

- Tag an asset using the existing tags in the CCS
- Untag an asset

Before you configure the rules-based actions, you must create the tags and the categories in CCS.

See “Creating a new tag category” on page 678.

See “Creating a new tag” on page 678.
Note: To be able to configure rules-based actions, you must check **Enable Symantec Data Loss Prevention Connector Rules Execution** during the connector configuration.

You can use the following rules XML files for rules-based action execution:

- ApplyTagsToAssets.xml
- RemoveTagsFromAssets.xml

The Rules XMLs are present at the following location:

#Symantec\CCS\Reporting and Analytics\Third Party Integration\Symantec Data Loss Prevention Connector\Rules\RulesXmls


### About predefined rules-based actions

The predefined xml rules files are located in the `<Install Directory>\ Third Party Integration\Symantec Data Loss Prevention Connector\Rules\RulesXmls`. The Rules Xml files let you perform rules-based actions.

The Rules XMLs contain the predefined conditions and the actions that you can use for tagging and untagging an asset.

The directory includes the following files:

- **ApplyTagsToAssets.xml**
  Applies tags you specify to the assets that match the specified conditions.

- **RemoveTagsFromAssets.xml**
  Removes the tags you specify from the assets that match the specified conditions.

You must provide the following information in the Rules Xml file:

- **Policy ID**
  The Policy ID displays on the status bar of the DLP console when you place the cursor on the policy name.

- **Status ID**
  The Status ID of the incident appears in the DLP console status bar when you place the cursor on the incident status attribute value.
tagName
The CCS tag name that you want to apply on the resolved assets.
tagCategory
The category of the tag that you specify in the tag name.

The table Table 7-3 provides information about the parameters in the Rules Xml file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Name&gt;Apply tags to assets&lt;/Name&gt;</td>
<td>Rule name. The name of the rule which appears in the log file.</td>
</tr>
<tr>
<td>&lt;Description&gt;Rule for applying tags to assets.</td>
<td>Rule description. A small description of what the rule is meant to accomplish. This description only appears in this XML file.</td>
</tr>
<tr>
<td>&lt;Order&gt;0&lt;/Order&gt;</td>
<td>Rule order. Rules are executed in numerical order. You should enter a non-negative integer in this field. (&gt;=0) The rule with the lowest number is executed first.</td>
</tr>
<tr>
<td>&lt;Conditions LogicalOperator=&quot;AND&quot;&gt;</td>
<td>Rule Condition. You can specify a logical AND or OR. All conditions are linked with the operator you specify.</td>
</tr>
<tr>
<td>&lt;Id&gt;GetProperty&lt;/Id&gt;</td>
<td>Attribute Data Type. The data type depends on the attribute you specify. The data type you specify must match all other data type entries in this condition. The topic &quot;About custom rules-based actions&quot; in the Control Compliance Suite help lists the supported data types and matching attributes.</td>
</tr>
<tr>
<td>&lt;IsProtoType&gt;false&lt;/IsProtoType&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;IsMandatory&gt;false&lt;/IsMandatory&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;Unary&gt;false&lt;/Unary&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;ValueType&gt;System.Int32&lt;/ValueType&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Table 7-3 Parameters and their descriptions (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Name&gt;PolicyID&lt;/Name&gt;</code></td>
<td>Attribute. The topic &quot;About custom rules-based actions&quot; in the Control Compliance Suite help lists the supported data types and matching attributes.</td>
</tr>
<tr>
<td><code>&lt;Id&gt;ValueOperand&lt;/Id&gt;</code></td>
<td>Attribute Data Type. The data type depends on the attribute you specify. The data type you specify must match all other data type entries in this condition. The topic &quot;About custom rules-based actions&quot; in the Control Compliance Suite help lists the supported data types and matching attributes.</td>
</tr>
<tr>
<td><code>&lt;IsProtoType&gt;false&lt;/IsProtoType&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;IsMandatory&gt;false&lt;/IsMandatory&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;Unary&gt;false&lt;/Unary&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;ValueType&gt;System.Int32&lt;/ValueType&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;ParameterValue&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;Value Type=&quot;System.Int32&quot;&gt;0&lt;/Value&gt;</code></td>
<td>Attribute Data Type. The data type depends on the attribute you specify. The data type you specify must match all other data type entries in this condition. The topic &quot;About custom rules-based actions&quot; in the Control Compliance Suite help lists the supported data types and matching attributes. Replace zero with the actual value.</td>
</tr>
<tr>
<td><code>&lt;RelationalOperator&gt;IsEqual&lt;/RelationalOperator&gt;</code></td>
<td>Relational operator. The relational operator connects the left and right operands in this condition. The topic &quot;About custom rules-based actions&quot; in the Control Compliance Suite help lists the supported relational operators for each data type.</td>
</tr>
</tbody>
</table>
Table 7-3  Parameters and their descriptions (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;TagName&gt;&lt;![CDATA[ tagName]]&gt; &lt;/TagName&gt;</code></td>
<td>Control Compliance Suite Tag name. Replace &quot;tagName&quot; to Specify the Control Compliance Suite tag to apply.</td>
</tr>
<tr>
<td><code>&lt;TagCategory&gt;&lt;![CDATA[categoryName]]&gt; &lt;/TagCategory&gt;</code></td>
<td>Control Compliance Suite category name. Replace &quot;categoryName&quot; to Specify the Control Compliance Suite tag category.</td>
</tr>
</tbody>
</table>

See “About custom rules-based actions” on page 436.

The DLP Connector logs all the incidents when a condition that you specify in a rule is satisfied and an action is executed. The log file is stored in the following location on the computer that hosts the DLP Connector:

C:\Documents and Settings\All Users\Application Data\Symantec.CSM \Logs\ThirdPartyConnectors

See “About rules-based action execution” on page 432.

About custom rules-based actions

Custom rules-based actions let you create your own action execution rules to execute when the incident data matches a particular condition. Custom rules-based actions let you specify your own parameters. You can specify a logical operator to use for the conditions or you can use the policy name instead of the policy ID. You can use multiple conditions in the custom rule. You can specify multiple tags or conditions to apply or to remove.

Before you configure the custom rules-based actions, you must create the tags and the categories in Control Compliance Suite (CCS).

Both predefined rules files and custom rules files are stored in the same directory. You must store all rules files in the `<Installation Directory>\CCS\Reporting and Analytics\Third Party Integration\Symantec Data Loss Prevention Connector\Rules\RulesXmls`.

You configure the custom rules xml file to suit your needs.

Table 7-4 lists the items you must configure in the file. In the file, the items you must configure are enclosed in XML tags. You must edit the values between the tags.
Table 7-4 Custom rule files

<table>
<thead>
<tr>
<th>Items to customize</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule name</td>
<td>You must use a unique name for the rule.</td>
</tr>
<tr>
<td>rule description</td>
<td>A description of the rule purpose and actions. The rule is only visible in the XML file itself, not the CCS Console.</td>
</tr>
<tr>
<td>rule order</td>
<td>You must specify a unique non-negative integer. Rules are executed in the order that you specify from smallest to largest.</td>
</tr>
<tr>
<td>rule conditions</td>
<td>If you specify multiple conditions, you can use logical operators to link them. You can use the <strong>AND</strong> and <strong>OR</strong> operators to link conditions. The same operator is used to link all conditions. That is, the <strong>AND</strong> or <strong>OR</strong> operator links all of the conditions.</td>
</tr>
<tr>
<td>data type</td>
<td>The data type you specify depends on the attribute you specify. You must specify the data type that matches the attribute. You specify the data type in 4 lines in each condition. You must specify the same data type in each line in a given condition.</td>
</tr>
<tr>
<td>attribute</td>
<td>The attribute you specify determines the data type you specify. You must specify the data type that matches the attribute. You specify the attribute in 2 lines in each condition. You must specify the same attribute in each line in a given condition.</td>
</tr>
<tr>
<td>relational operator</td>
<td>The relational operator connects the left operand and the right operand in the condition. The supported operators depend on the data type. You specify the relational operator in 1 line in each condition.</td>
</tr>
<tr>
<td>Items to customize</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------</td>
</tr>
<tr>
<td>values</td>
<td>The values block lets you specify the CCS tags and categories to apply to or remove from the affected assets. You can insert multiple copies of the values block. Each copy of the value block has a unique tag and category. In the values block, you assign the CCS tag name to apply or remove. You also specify the name of the CCS category the tag is assigned to.</td>
</tr>
</tbody>
</table>

Table 7-5  
**Attribute data types**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>detectionserver</td>
<td>System.String</td>
</tr>
<tr>
<td>policyName</td>
<td>System.String</td>
</tr>
<tr>
<td>PolicyVersion</td>
<td>System.Int32</td>
</tr>
<tr>
<td>severity</td>
<td>System.String</td>
</tr>
<tr>
<td>status</td>
<td>System.String</td>
</tr>
<tr>
<td>policyId</td>
<td>System.Int32</td>
</tr>
<tr>
<td>statusId</td>
<td>System.Int32</td>
</tr>
</tbody>
</table>
Table 7-6  Supported relational operators

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Supported relational operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>System.String</td>
<td>IsEqual</td>
</tr>
<tr>
<td></td>
<td>IsNotEqual</td>
</tr>
<tr>
<td></td>
<td>IsGreaterThan</td>
</tr>
<tr>
<td></td>
<td>IsGreaterThanOrEqual</td>
</tr>
<tr>
<td></td>
<td>IsLessThan</td>
</tr>
<tr>
<td></td>
<td>IsLessThanOrEqual</td>
</tr>
<tr>
<td></td>
<td>DoesNotContain</td>
</tr>
<tr>
<td></td>
<td>BeginsWith</td>
</tr>
<tr>
<td></td>
<td>DoesNotBeginWith</td>
</tr>
<tr>
<td></td>
<td>EndsWith</td>
</tr>
<tr>
<td></td>
<td>DoesNotEndWith</td>
</tr>
<tr>
<td>System.Int32</td>
<td>IsEqual</td>
</tr>
<tr>
<td></td>
<td>IsNotEqual</td>
</tr>
<tr>
<td></td>
<td>IsGreaterThan</td>
</tr>
<tr>
<td></td>
<td>IsGreaterThanOrEqual</td>
</tr>
<tr>
<td></td>
<td>IsLessThan</td>
</tr>
<tr>
<td></td>
<td>IsLessThanOrEqual</td>
</tr>
</tbody>
</table>

See “Creating a new tag category” on page 678.

See “Creating a new tag” on page 678.

When you create your own rules, you must do the following:

■ Make a duplicate copy of an existing rule xml file with a new name.

■ Open the copied file in any text editor.

■ Edit the required elements of the xml file.

■ Save and close the edited file.

You can make a duplicate copy of the Rules XML, enter the custom parameters, and save the duplicate copies with a new name. However, you must save the custom Rules XMLs at the same location as the predefined rules XMLs.

All rules xml files are stored in the following directory on the computer that hosts the DLP Connector:
You must restart the Symantec Data Loss Prevention Connector Service before the new rules take effect.

See “About rules-based action execution” on page 432.

See “About predefined rules-based actions” on page 433.

Managing controls for Symantec Data Loss Prevention Connector

The Symantec Data Loss Prevention Connector imports Symantec Data Loss Prevention (DLP) incidents into the Control Compliance Suite (CCS). As it does so, it creates a control for each violated DLP policy. The controls are stored in the extended evidence sources and have the same name as the DLP policy that was violated.

You can view the DLP controls and the mapped control statements in the Extended Controls Statement Mappings page in the Symantec Content Studio.

See “Working with extended controls” on page 825.

See “Editing an extended control” on page 831.

See “Deleting an extended control” on page 831.

About Symantec Data Loss Prevention Connector logging

The Symantec Data Loss Prevention Connector adds a new entry into the log file for each new operation that the DLP Connector performs. The type of log entry that the application adds to the log depends on the configurations in the ConnectorService.config file.

You can enter the following in the ConnectorService.config file for DLP Connector logging:

- **Log directory** Specify the location for the log file if you do not want the log file to be in the default location.

  The default location of the log file is:

  `C:\Documents and Settings\All Users\Application Data\Symantec.CSM\Logs\ThirdPartyConnectors`
Severity

Specify the severity of the log levels.

See “About log levels” on page 206.

The level of details that the DLP Connector logs depends on the CCS log configurations.

Note: You must restart the Symantec Data Loss Prevention Connector Service before you use the latest configuration.

See “About Symantec Data Loss Prevention Connector email notification configurations and logging” on page 428.

Using the Symantec Data Loss Prevention Connector Credentials Removal utility

The DLP Enforce Server credentials are stored in the context of the Symantec Data Loss Prevention Connector service account where the service account is created. When you use a new Symantec Data Loss Prevention Connector service account, the previously used DLP Enforce Server credentials still remain in the secure store. The Remove Symantec DLP Connector Credentials.exe utility lets you purge the service account credentials. The Remove Symantec DLP Connector Credentials.exe is located in the following location:

#Symantec\CCS\Reporting and Analytics\Third Party Integration\Symantec Data Loss Prevention Connector

Note: Symantec recommends that you run the utility before you change the Symantec Data Loss Prevention Connector service account.

To run the DLP Connector Credentials Removal utility

1. Navigate to the install directory on your local computer.
2. Double-click Remove Symantec DLP Connector Credentials.exe.
3. Click Yes on the message prompt that appears.

The Enforce Server account credentials are purged from the local secure store of your computer.

See “Configuring the Symantec Data Loss Prevention Connector” on page 423.
Using the Symantec CSM Connector Executor utility

The Symantec CSM Connector Executor.exe lets you collect incident data for specified saved reports immediately. You can use the utility to collect incident data at any time, without regard for the schedule that you have configured for incident data collection.

The utility uses the settings you configured for the Symantec Data Loss Prevention Connector.

You can run the Symantec CSM Connector Executor utility from the installation folder on your local computer or from the command line.

If you specify one or more report IDs when you run the utility from the command line, data is only collected for the specified reports. If you do not specify any saved report ID in the command line, the utility collects the incident data for all the configured reports. You separate multiple report IDs with a space.

The Symantec CSM Connector Executor.exe is located in the following location:

#Symantec\CCS\Reporting and Analytics\Third Party Integration\Symantec Data Loss Prevention Connector

To run the Symantec CSM Connector Executor utility from the command line

1. At the command prompt, navigate to <Install Directory>\Symantec\CCS \Reporting and Analytics\Third Party Integration\Symantec Data Loss Prevention Connector.

2. Type the following:

   Symantec CSM Connector Executor <report ID_1> <report ID_2> ... <report ID_n>

   The utility collects the data for the report IDs you specify.

See “Configuring the Symantec Data Loss Prevention Connector” on page 423.
Managing custom schema

This chapter includes the following topics:

- About the custom schema
- Working with custom asset types
- Working with custom entity
- Working with custom target type
- Working with custom schema scenarios

About the custom schema

Control Compliance Suite provides certain predefined asset types that you can use to import the assets into the asset system. Asset types let you import the asset data for a collection of fields that belong to a specific entity. In the process of managing the assets in the system, you might need to create your custom asset types to manage the assets that are outside the scope of the predefined asset types.

Control Compliance Suite lets you create your own schema for the asset types and the entities. In addition, you can also extend the schema for the predefined asset types and extend the custom entity schema. You can also create new target types and edit the newly created target types.

In addition, you can also edit the existing asset type and existing entity schema. The Schema Manager gives you the option to switch the CSV or ODBC data collectors for the custom and common platforms.

You can create and edit the following types of schema

- Asset type schema
  See “About the asset type schema” on page 444.
- Entity schema
See “About the entity schema” on page 445.

- Target type schema
  See “About the target type schema” on page 445.

See “Working with custom schema scenarios” on page 468.
See “Working with custom asset types” on page 446.
See “Working with custom entity” on page 456.
See “Working with custom target type” on page 466.

**About the Schema Manager view**

The Schema Manager view lets you create or extend the asset type schema and the entity schema. The view also lets you create a new target type or edit an existing target type.

You can access the Schema Manager view from Settings > Schema Manager.

You can do the following from the Schema Manager view:

- See “About the asset type schema” on page 444.
- See “About the entity schema” on page 445.
- See “About the target type schema” on page 445.

**About the asset type schema**

The assets are stored in the asset store in the CCS directory. Each asset type in the CCS directory has its own schema. Control Compliance Suite supports some predefined asset types.

See “Predefined asset types” on page 236.

The assets schema includes the following types of schema:

- **Asset type schema**
  Each asset type is a separate entity and has no relation with the other asset types. Each asset type has some primary fields. The primary fields are used to uniquely identify the asset in the CCS directory.

- **Asset base schema**
  The asset base schema represents the asset fields that are common across all the asset types. The common fields of the asset type include, Integrity, Confidentiality, Availability, Tags, Asset Custodian, Asset Department, Asset Owner, Asset Location, and Asset Site.

Control Compliance Suite lets you create your own asset type schema and extend the existing asset type schema to manage your assets.
About the entity schema

An entity schema in Control Compliance Suite is the blueprint that contains the asset information, which is used to create an asset type. Once the asset type is defined, the registered data collectors import the assets into the infrastructure based on the defined schema. The data collectors of Control Compliance Suite also collect data from the imported assets.

An entity schema interprets data only if the data is defined in a specific format. For every asset, data must be defined in a format that contains attributes such as platform, entity, and fields. The entity schema is a set of XML definitions, which represent the defined attributes.

In Control Compliance Suite, you can define an entity schema for any custom application for which you want to collect data. Data for the application must be imported to a comma-separated value (CSV) file and arranged in a specific format for the entity schema. The CSV data collector of Control Compliance Suite collects data from the CSV file.

You can also define an entity schema for any custom application and collect data for the asset using the ODBC data collector.

See “About the ODBC data collector” on page 159.

The entity schema drives the data collectors to collect data from the queried assets. In the entity schema, every asset is associated with an unique identifier called the primary key. The primary keys are fields, which are used to identify an asset. For all the predefined platforms of Control Compliance Suite you must know the primary keys of all the predefined entities.

See “About the predefined platforms and the primary entities” on page 454.

You can create a new entity schema or extend an existing entity schema using the appropriate tools from Settings > Schema Manager view of the console.

See “Creating a new entity schema” on page 461.

See “Editing an existing entity schema” on page 465.

About the target type schema

You select a target type to evaluate a set of assets against a standard. The standards are based on the asset types. You cannot evaluate an asset of the type Oracle Configured Database against an ESM standard.
Control Compliance Suite lets you create your own target types to filter the assets of a particular asset type for evaluation.

Consider the following example:

Windows machines is a predefined asset type. If you want to evaluate a standard only for the Windows XP machines, the Windows XP machines can be your target type.

See “Creating a new target type” on page 466.
See “Editing a target type” on page 467.

Working with custom asset types

Control Compliance Suite lets you create custom asset types from the custom platforms and custom entities that you can create from the Schema Manager view.

See “About the entity schema” on page 445.

You can import the assets from the custom asset types in the same way as you import the assets from the predefined or probable asset types.

Asset types are based on the entities of the platform. In Control Compliance Suite, a platform is defined as the category to which a group of entities belong. A group of fields that define the common functions of the network element form an entity.

See “About platforms” on page 456.
See “About entities” on page 457.

When you create your own platform and defined fields for the platform to create an entity, you can define an asset type also. The custom asset type imports the data of the fields that are defined in the custom entity.

You can create the custom asset types from the Schema Manager view. Go to Settings > Schema Manager > Add new asset type to get started with the creation of a custom asset type.

See “Creating a new asset type” on page 446.
See “Extending an existing asset type” on page 451.

Creating a new asset type

Control Compliance Suite lets you create a custom asset type that you can use for importing assets.

The creation of a new asset type involves the following steps:

■ Choose your own platform and the primary entity to create the asset type.
See “Asset types” on page 235.

- Specify the fields that should be included in the newly created asset type. You can specify the fields for the referenced entity also. See “About referenced entity fields” on page 454.

- Mark the fields as mandatory or optional. See “About the primary, mandatory, and optional fields” on page 454.

- Add a new field that has no reference to the entity schema. See “About separators in name fields” on page 455.

- Add asset name fields. See “About separators in name fields” on page 455.

- Close the Control Compliance Suite Console, Restart the Symantec Application Server Service, and re-launch the Console.

**Note:** Before creating a new asset type you must know that an asset type once created or a field once added to the asset type cannot be deprecated.

**To create a new asset type**

1. Go to Settings > Schema Manager.

2. Select **Add new asset type**.

3. In the Specify Asset Type Details panel, do the following:
   - Type the name of the asset type that you want to create in the Name field. The asset type name should not include spaces and should not exceed 10 characters.
   - Type the display name and the description for the asset type in the Display name and Description fields and click **Next**.

4. In the Select Platform and Primary Entity panel, do the following:
   - From the Platform drop-down list, select a platform for which you want to create an asset type. The list of platforms includes the predefined platforms and any custom platform that you have already created.
   - From the Primary entity drop-down list, select a primary entity for the selected platform and click **Next**.
   See “About the predefined platforms and the primary entities” on page 454.
In the Specify Fields panel, select the fields from the Available fields list and add the fields in the Selected fields list with the Add icon. By default, the primary fields for the primary entity are listed in the Available fields list.

Select **Include referenced entities** if you want to add the fields for the referenced entities and click **Next**. If you select this option, the referenced entities appear in the Entity drop-down list. You can then select a referenced entity and add the fields for the referenced entities. See “About referenced entity fields” on page 454.

In the Customize Field Attributes panel, you can mark the fields as mandatory or optional and click **Next**. You mark the fields as mandatory or optional that are not primary fields. You can also specify if the field is a part of the asset import and if the field is editable. See “About the primary, mandatory, and optional fields” on page 454.

In the Add External Fields panel, click **Add** to add an external field. See “Creating an external field to add to the asset type” on page 453.

In the Specify Asset Name Fields, select the fields from the Available fields list. Use the Add icon to add to add the fields to the Selected fields list. Click **Next**. You can use the separators to add multiple asset name fields and to specify the relation among the multiple fields. See “About separators in name fields” on page 455.

In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.

Restart the Symantec Application Server service and relaunch the Console. See “Viewing the custom asset type and the custom fields in the asset system” on page 450.

See “Extending an existing asset type” on page 451.

### Registering a platform

The **Settings > Schema Manager** view lets you register a platform to enable the import of the asset types.
Note: The registration of platform is a mandatory step to perform the asset type import.

See “Importing an asset type” on page 449.

To register a platform

1. Go to Settings > Schema Manager.
2. From the menu bar, click Register Platform.
3. In the Register Platform dialog box, browse and select the XML for the platform that you want to register.

   You must copy the Platform and the Entity XMLs to the Reporting and Analytics, the Application Server, and the DPS folders. Restart the Symantec Application Server service and the Symantec Data Processing service for all the configured Data Processing Servers. Relaunch the Control Compliance Suite Console.
4. Click Register.

Importing an asset type

The import asset type functionality lets you access a custom asset type that another user has created. The user from whom you want to import the asset type must export the asset type.

See “Exporting an asset type” on page 450.

You must first register the platform of the primary entity of the asset type that you want to import.

See “Registering a platform” on page 448.

To import an asset type

1. Go to Settings > Schema Manager.
2. From the menu bar, click Import Asset Type.
3 In the **Import Asset Type** dialog box, browse and select the asset type XML to import.

You must have already registered the platform for the primary entity of this asset type.

---

**Note:** You must manually copy the custom entity schema and platform XMLs for the primary entity of the asset type that you want to import.

---

4 Click **Import**.

### Exporting an asset type

The export asset type functionality lets you export an asset type that you want to share with another user.

---

**Note:** You can export only the custom asset types. The predefined asset types cannot be exported.

---

**To export an asset type**

1 Go to **Settings > Schema Manager**.

2 From the menu bar, click **Export Asset Type**.

3 In the **Export Asset Type** dialog box, select the primary entity of the asset type that you want to export from the **Asset Type** list.

4 Browse and select the XML that you want to export.

5 Click **Export**.

See “**Registering a platform**” on page 448.

See “**Importing an asset type**” on page 449.

### Viewing the custom asset type and the custom fields in the asset system

You can view the custom asset type in the asset system after you create an asset type from the Create new Asset Type wizard.
To view the custom asset type in the asset system

1. Go to Start > Run and type `services.msc`.

2. In the Services console, right-click the Symantec Application Server Service and select **Restart**.

3. Close the Control Compliance Suite Console and relaunch the console after waiting for two minutes.

4. Go to Manage > Assets > Asset System.

5. Check if the newly created asset type appears in the Display drop-down list that appears in the taskbar.

You can view the newly added mandatory, optional, or external fields after you import the assets from the custom asset type.

To view the custom fields in the asset system:

1. Go to Manage > Assets > Asset System.

2. Select the asset type for which you imported the assets.

3. Select an asset for which you want to view the custom field information.

4. In the details pane, go to Custom Properties tab.

   The newly added fields appear.

See “Creating a new asset type” on page 446.

Extending an existing asset type

Control Compliance Suite lets you extend the existing asset types by modification of the default fields and addition of the optional fields to the asset types.

**Note:** Before extending an existing asset type you must know that a field once added to the asset type cannot be deprecated.

To extend an existing asset type

1. Go to Settings > Schema Manager.

2. Select **Extend existing asset type**.

3. In the Select Asset Type panel, select an asset type that you want to extend and click **Next**.

   The primary, mandatory, and optional fields for the selected asset type are displayed.
4 In the Select Optional Fields panel, select the fields from the Available fields list and add the fields in the Selected fields list with the Add icon.

5 Select **Include referenced entities** if you want to add the fields for the referenced entities and click **Next**.

   If you select this option, the referenced entities appear in the Entity drop-down list. You can then select a referenced entity and add the fields for the referenced entities.

   See “About referenced entity fields” on page 454.

6 In the Customize Field Attributes panel, you can choose to include the fields in the data collection job and mark them editable.

   When you extend an existing asset type, you can only add the optional fields. The optional fields are not required for data collection. You can explicitly mark the field to include in the data collection job.

   Click **Next**.

7 In the Add External Fields panel, click **Add** to add an external field.

   See “Creating an external field to add to the asset type” on page 453.

8 In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.

   See “Creating a new asset type” on page 446.

---

**Editing an existing asset type**

You can edit an existing asset type from the **Settings > Schema Manager > Edit existing asset type** option.

The **Edit existing asset type** option lets you edit the attributes of the custom fields for an existing asset type.

**To edit the existing asset type**

1 Go to **Settings > Schema Manager > Edit existing asset type**.

2 In the **Edit Asset Type Details** panel, select the asset type that you want to edit from the **Asset Type** list.

3 Specify the new display name and the description for the asset type and click **Next**.
4 In the **Edit Attributes** panel, edit the following asset type attributes and click **Next**.

- **Display Name**: This field is editable. You can edit the display name of the attribute from this panel.
- **Description**: This field is editable. You can edit the description of the attribute from this panel.
- **Data Type**: This field it not editable.
- **Field Type**: This field is not editable.
- **Allow Editing of Field?**: This field lets you choose if you want to make the field editable.

5 In the **Summary** panel, review the information that you entered in the wizard. Click **Back** to make any modifications or click **Finish** to exit the wizard.

Creating an external field to add to the asset type

Control Compliance Suite gives you a flexibility to create external fields that have no reference to the entity schema. The data for the external fields cannot be imported from the data collectors. You can manually specify values for the external fields from the details pane or use the pre reconciliation rules to set the value.

**To create an external field to add to the asset type**

1 From the Add External Fields panel in the Create New Asset Type wizard, click **Add**.
2 In the Add New Field dialog box, type the name of the new field in the Field name box.
3 Type the display name and the description for the field.
4 Select the type of the field from the following options:
   - String
   - Integer
   - Boolean
   - DateTime
5 Check **Allow editing of field** to mark the field as editable.
About the predefined platforms and the primary entities

The Control Compliance Suite provides certain primary entities for the predefined platforms as predefined asset types.

See “Predefined asset types” on page 236.

In addition to the predefined asset types, the Control Compliance Suite also defines certain primary entities that you can use to create custom asset types.

See “Probable asset types” on page 273.

Control Compliance Suite provides the following primary entities for the predefined platforms to create asset types:

See “Creating a new asset type” on page 446.
See “Creating a new entity schema” on page 461.

About the primary, mandatory, and optional fields

The primary fields are the identifier fields. The primary fields are used to identify the asset type exclusively.

The mandatory fields are the fields that are required for data collection and evaluation. Without the presence of the mandatory fields, the asset is not imported into the asset system.

The optional fields are the fields that are not required for asset import, data collection, or evaluation. The new fields that you can add to the custom asset type are optional fields. They have no reference to the entity schema.

See “Creating a new asset type” on page 446.
See “Creating a new entity schema” on page 461.

About referenced entity fields

A referenced entity is a parent entity. You can choose to include the fields of the referenced entity along with the fields of the primary entity in the custom schema. Consider the following example:

- You select Windows File as the primary entity to create a new asset type.
You choose to include the referenced entity fields also in the new asset type. The parent or referenced entities for the Windows File are Domain, Machine, and Group.

You create a new asset type. When you run a job that is based on the new asset type, the job also collects the information about the referenced fields.

If the data for the Windows File asset type contains information about the Domain, the import job also returns the data for the domain.

See “Creating a new asset type” on page 446.

See “Creating a new entity schema” on page 461.

About separators in name fields

You use the separators to set the format to display the asset name on the Control Compliance Suite console.

For the assets that belong to the predefined asset types, the default format to display the asset name is as follows:

```
domain name\machine name\file name with full path
```

For example, CMCT\2k3-105-133\c:\boot.ini

The backslash mark (\) is a separator that is used to display the asset name. The domain name, the machine name, and the file name are the name fields that are used to form the asset name.

When you create a custom asset type, you can use one or more available asset name fields and use a separator from the given list. The asset name for the custom asset type that you create is displayed in the format that you specify.

Consider the following selections:

<table>
<thead>
<tr>
<th>Platform</th>
<th>SQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary entity</td>
<td>Database</td>
</tr>
<tr>
<td>Asset name fields</td>
<td>Database name, Host name (node), and Server name (instance)</td>
</tr>
<tr>
<td>Separator</td>
<td>#</td>
</tr>
</tbody>
</table>

In case of the selections that are specified, the asset name format should be as follows:

```
Database name#Host name(node)#Server name(instance)
```
Note: You cannot edit the naming convention once you create an asset type with the convention.

See “Creating a new asset type” on page 446.
See “Extending an existing asset type” on page 451.

Working with custom entity

A custom entity comprises a group of fields.

See “About entities” on page 457.

In Control Compliance Suite, entities are defined for a platform and contain fields that comprise the entity. You can define a custom entity only through an entity schema in Control Compliance Suite. An entity schema is a set of XML definitions that is interpreted by the infrastructure to drive the data collectors for data collection. You can configure either a CSV or an ODBC data collector for collecting data that is defined for the custom entity. The data of the custom entity is defined either in a CSV file or in the ODBC database tables.

The entity schema can be created using the Create new entity schema tool of the Schema Manager. The Schema Manager can be accessed through the Settings > Schema Manager option of the console.

A custom entity must have unique identifiers known as primary keys, which are defined in the entity schema. Control Compliance Suite lets you extend an already created custom entity through the Extend entity schema tool of the Schema Manager.

See “Creating a new entity schema” on page 461.
See “Editing an existing entity schema” on page 465.

About platforms

In Control Compliance Suite, a platform is defined as the category to which a group of entities belong. For example, SQL can be a platform, which contains entities that define the SQL application.

See “About entities” on page 457.

The Control Compliance Suite supports certain predefined platforms that are recognized by the infrastructure for data collection. For every predefined platform, a default data collector of Control Compliance Suite performs the data collection. An entity schema contains the blueprint of a data collector and drives the data collector for data collection.
The predefined platforms of Control Compliance Suite are as follows:

- Windows
- UNIX
- SQL
- Oracle
- Exchange
- NDS
- NetWare
- ESM

You can define a platform for any custom application for which you want to collect data through a CSV file or through an ODBC database table.

See “Creating a CSV file for custom application” on page 357.
See “Creating an ODBC database table for custom application” on page 365.

About entities

An entity is formed by a group of fields that define the common functions of the network element. The entity encapsulates the properties of an asset type, based on which an asset type can be created.

For example, for a Windows platform, you can define an entity such as Machines, which contains fields that define the entity. Fields such as machine name, IP address, netmask, and CPU usage, and so on can define the Machine entity.

See “About platforms” on page 456.
See “About fields of an entity ” on page 457.

About fields of an entity

A field contains definitions of a network element. A network element can be a router, directory, server, desktop, or any entity that functions on set parameters.

For example, in Windows server computer, the directories can be the entities. The directories can be defined by parameters such as the disk-occupied size in bytes, directory location in the computer, and user privileges to access. The fields such as disk space, location, and users can be used to define the directory parameters.

Fields are an integral part of the entity schema for defining an asset type. In an entity schema, fields are defined for an entity. An entity can contain as many
fields as are required to define the asset type. A configured data collector collects data for the fields that are specified in the entity schema.

See “About the entity schema” on page 445.

See “About platforms” on page 456.

See “About entities” on page 457.

About setting tasks to roles for entity schema

To create an entity schema through the Control Compliance Suite console, you must have permission to execute specific tasks. The tasks are associated with the role that is assigned to you.

You must have the following tasks associated with your role to create an entity schema:

- Manage Configuration Settings
- Manage Schema

By default, the role, CCS_Administrator is provided permission for all the tasks to create an entity schema. If you are not assigned the CCS_Administrator role, then create a custom role through the Settings > Role view of the console.

See “Creating a custom role” on page 110.

See “Creating a new entity schema” on page 461.

About relationships between the predefined entities

In Control Compliance Suite, there is defined relationship between the predefined entities of the predefined platforms. The relationship is between the fields of the predefined entities. Such relationships between the predefined entities facilitate broader scope of collecting data for a custom entity. The scope of collecting data broadens whenever a custom entity extends a predefined entity.

You must know the relation between the predefined entities of all the predefined platforms. You can use the relationship between the predefined entities to reference the custom entity. The Create new entity schema wizard is used to reference a custom entity during creation.

See “Creating a new entity schema” on page 461.

Table 8-1 relationship details of the predefined entities for the Oracle platform

<table>
<thead>
<tr>
<th>Predefined entity</th>
<th>Relation entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGUREDDATABASES</td>
<td>CONFIGUREDSERVERS of the Oracle platform</td>
</tr>
</tbody>
</table>
Table 8-1  relationship details of the predefined entities for the Oracle platform (continued)

<table>
<thead>
<tr>
<th>Predefined entity</th>
<th>Relation entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGUREDSERVERS</td>
<td>The CONFIGUREDSERVERS entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine entity of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Machine entity of the UNIX platform</td>
</tr>
</tbody>
</table>

Table 8-2  relationship details of the predefined entities for the SQL platform

<table>
<thead>
<tr>
<th>Predefined entity</th>
<th>Relation entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Server of the SQL platform</td>
</tr>
<tr>
<td>Server</td>
<td>Machine of the Windows platform</td>
</tr>
<tr>
<td>Stored Procedure</td>
<td>The Stored Procedure entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Database of the SQL platform</td>
</tr>
<tr>
<td></td>
<td>■ Server of the SQL platform</td>
</tr>
<tr>
<td>User</td>
<td>The User entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Database of the SQL platform</td>
</tr>
<tr>
<td></td>
<td>■ Server of the SQL platform</td>
</tr>
</tbody>
</table>

Table 8-3  relationship details of the predefined entities for the UNIX platform

<table>
<thead>
<tr>
<th>Predefined entity</th>
<th>Relation entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Machine of the UNIX platform</td>
</tr>
<tr>
<td>Group</td>
<td>Machine of the UNIX platform</td>
</tr>
<tr>
<td>Machine</td>
<td>No defined relationship</td>
</tr>
<tr>
<td>User</td>
<td>Machine of the UNIX platform</td>
</tr>
</tbody>
</table>
Table 8-4  relationship details of the predefined entities for the Windows platform

<table>
<thead>
<tr>
<th>Predefined entity</th>
<th>Relation entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>The Directory entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Domain of the Windows platform</td>
</tr>
<tr>
<td>Domain</td>
<td>No defined relationship</td>
</tr>
<tr>
<td>File</td>
<td>The File entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Domain of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Directory of the Windows platform</td>
</tr>
<tr>
<td>Group</td>
<td>The Group entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Domain of the Windows platform</td>
</tr>
<tr>
<td>IISVirtualDirectories</td>
<td>The IISVirtualDirectories entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Domain of the Windows platform</td>
</tr>
<tr>
<td>IISWebSite</td>
<td>The IISWebSite entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Domain of the Windows platform</td>
</tr>
<tr>
<td>Machine</td>
<td>Domain of the Windows platform</td>
</tr>
<tr>
<td>Registry</td>
<td>The Registry entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Domain of the Windows platform</td>
</tr>
<tr>
<td>Service</td>
<td>The Service entity is referenced to the following predefined entities:</td>
</tr>
<tr>
<td></td>
<td>■ Machine of the Windows platform</td>
</tr>
<tr>
<td></td>
<td>■ Domain of the Windows platform</td>
</tr>
</tbody>
</table>
Creating a new entity schema

You can create a new entity schema for a custom application through the Schema Manager of the Control Compliance Suite Console. The entity schema defines the platform, entities, and fields of an asset for which data is to be collected. You can create a new entity schema only when you do not want to use any of the predefined platforms for data collection.

**Note:** Before you create a new entity schema you must know that the entities and platforms cannot be deprecated.

See “About platforms” on page 456.

For a custom platform of a custom application, you must create and define the entities through the Create New Entity Schema wizard. You can collect data for the custom application either through a CSV data collector or through an ODBC data collector.

Difference between a CSV data collector and an ODBC data collector in collecting data are as follows:

- A CSV data collector interprets data that is contained in a CSV file and arranged as per the defined CSV file format. The CSV file format requires headers, which are defined based on the entity schema that you create.

- An ODBC data collector interprets data that is stored in the ODBC databases and the table and column names are mapped appropriately. The table names must map to the entities and table column names must map to the field names that are defined in the entity schema.

  See “Format to create ODBC compliant database tables” on page 363.

After you create an entity, you must create the custom asset types, which are later imported into Control Compliance Suite using the Asset Import wizard.

See “Creating a new asset type” on page 446.

**Note:** Every custom asset type that you create from a custom entity can scope to Site and the asset type itself when importing assets. The assets are imported using the Asset Import wizard.

**To create a new entity schema**

1. Go to Settings > Schema Manager.
2. Select **Create new entity schema** to launch the **Create New Entity Schema** wizard.
3 In the **Select or Create New Platform** panel, select either option and click **Next**.

Specify the values for the following fields:
- Create new platform
- Use existing platform

4 In the **Specify Entity Details** panel, enter the values for the fields and click **Next**.

Specify the values for the following fields:
- Name
- Display name
- Description
- Extend an existing entity
- Folder path

5 In the **Add Fields** panel, click **Add** to add new fields for the entity.

6 In the **Create New Field** dialog box, enter the values for the fields and click **OK**.

Specify the values for the following fields:
- Field name
- Display name
- Description
- Type
- Is case sensitive
- Is array

The added field details are displayed in the **Add Fields** panel. You must check the option, **Is primary key** if you want to declare the field as a primary key. Unchecking the option makes the added fields optional.

If you have extended a predefined entity (in the **Specify Entity Details** panel), then you must ensure that the number of primary keys for the creating entity is same as that of the extended entity.

7 In the **Add Fields** panel, click **Next**.
In the Specify Entity Name Fields panel, select the primary fields that are listed in the Available fields column and use the Add icon to add them to the Selected fields column.

The fields that are selected constitute the name of the assets that are created for the entity, which in turn defines the asset type.

Click Next.
9 In the **Specify References** panel, associate the fields of the entity with a parent entity and click **Next**.

Select the Platform, Parent entity, and fields from the drop-down boxes for associating the created entity as a child entity and click **Add**.

The panel lets you create relationship between the new entity and an entity of the predefined platform. A parent-child relationship is created between the entity of the predefined platform and the new entity that you are creating. You can associate the primary fields of the new entity with the primary fields of the parent entity to create a parent-child relationship. The parent-child relationship lets you collect data for the parent entity along with the child entity.

When you extend an entity, you must create a reference with the extended entity. You can also create a reference with the entity with which the extended entity shares a relationship. The relationship between the predefined entities are defined in Control Compliance Suite.

See “**About relationships between the predefined entities**” on page 458.
10 In the Summary panel, review the details of the created entity and click **Finish**.

The entity schema creates three XML files for the new platform, new entity, and the common platform respectively. You must put the XML files in the specific directories of every computer on which a CCS component is installed and restart the services.

The directories where the XML files are to be placed are as follows:

- **Installation directory of the Reporting and Analytics**
  
  \<install directory>\Symantec\CCS\Reporting And Analytics
  
  For example, C:\Program Files\Symantec\CCS\Reporting And Analytics

- **Installation directory of the Application Server**
  
  \<install directory>\Symantec\CCS\Reporting And Analytics\Application Server
  
  For example, C:\Program Files\Symantec\CCS\Reporting And Analytics\Application Server

- **Installation directory of the Data Processing Service (DPS)**
  
  \<install directory>\Symantec\CCS\Reporting And Analytics\DPS
  
  For example, C:\Program Files\Symantec\CCS\Reporting And Analytics\DPS

  **Note:** For a distributed setup mode, if you have more than one DPS, then copy all the schema XML files to the computers on which DPS is installed.

See “Editing an existing entity schema” on page 465.

**Editing an existing entity schema**

Control Compliance Suite lets you extend an existing entity schema to add new fields. You can extend a schema that you have earlier created.

**Note:** Before you edit the existing entity schema you must know that the entities once edited cannot be deprecated.
To extend an existing schema

1. Go to Settings > Schema Manager.
2. Select **Extend existing entity schema** to launch the Extend Entity Schema wizard.
3. In the Select Entity panel, select an existing platform and provide details for the entity that is to be extended.
   
   Click **Next**.
4. In the Select Fields panel, click **Add** to add new fields for the entity.
   
   The added fields are optional for the entity.
5. Click **Next**.
6. In the Summary panel, review the details of the fields and click **Finish**.

See “Creating a new entity schema” on page 461.

Working with custom target type

A target type is used to filter the assets during the data collection and the evaluation process.

See “About target types” on page 558.

A custom target type must be created when you want to collect data and run an evaluation for the custom asset type.

See “Creating a new asset type” on page 446.

See “Working with custom asset types” on page 446.

You can create a target type from the Schema Manager view.

The Schema Manager view lets you perform the following tasks that are related to target types:

- Create a new target type
  See “Creating a new target type” on page 466.

- Edit a target type
  See “Editing a target type” on page 467.

Creating a new target type

You need to create a custom target type to be able to collect data and run an evaluation for the custom asset type. You can create a new target type for both predefined as well as custom asset types.
To create a target type

1. Go to Settings > Schema Manager.
2. Click **Create New Target Type**.
3. In the Specify Name and Description for Target Type panel, type the name and description for the new target type. Click **Next**.
4. In the Select Platform and Asset Type panel, select an asset platform in the Platform list. Select an asset type in the Asset Type list.
   The custom platform, the custom asset types, and the predefined asset types are available for selection in the drop-down list.
5. In the Create Asset Type filters panel, click **Add Statement** to add a filter statement.
6. In the Filter Statement dialog box, select an operator and in the Specify Value box, type a value. Click **OK**.
7. In the Create Asset Type filters panel, click **Next**.
8. In the Summary panel, review the information that you have entered in the wizard. Click **Back** to make any modifications or click **Finish** to exit the wizard.

   Go to Manage > Standards. The new target type is available for selection in the Specify Name and Target Type panel of the Create Check wizard.

Editing a target type

You can edit only the custom target types. You cannot edit a predefined target type.

To edit a target type

1. In the **Select Target Type** panel, select the relevant asset platform and the asset type.
2. In the **Target Type** box, check the target type that you want to edit. Click **Next**.
3. In the **Specify Name and Description for Target Type** panel, you can edit the name and the description of the target type. Click **Next**.
4. In the **Edit Asset Type** filters panel, you can do either of the following:
   - To edit a filter statement, select the statement and click **Edit**.
   - To delete a filter statement, select the statement and click **Delete**.
5. To add a filter statement, click **Add Statement**.
6. In the **Filter Statement** dialog box, select an operator and in the Specify Value box, type a value. Click **OK**.

7. In the **Edit Platform and Asset Type** panel, click **Next**.

8. In the **Summary** panel, review the information that you have entered in the wizard. Click **Back** to make any modifications or click **Finish** to exit the wizard.

---

### Working with custom schema scenarios

You use the Schema Manager to create or extend the entity schema, asset type, and the target type.

Go through the following scenarios and perform the tasks in the given order to understand the application of the custom schema functionality in the process of managing assets.

<table>
<thead>
<tr>
<th>Table 8-5</th>
<th>Custom schema scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scenario</strong></td>
<td><strong>How to achieve?</strong></td>
</tr>
</tbody>
</table>
| You want to create a custom asset type, Windows Service. | Use the Add new asset type option on the Schema Manager view.  
For a detailed procedure of how to create a custom asset type, Windows Service, click on the link:  
See “Creating a custom asset type - Windows Service” on page 469. |
| You want to add a new field, TCP/IP Address to the Windows Machine asset type. | Use the Extend existing asset type option on the Schema Manager view.  
For a detailed procedure of how to add TCP/IP Address to the Windows Machine, click on the link:  
See “Extending the predefined asset type - Windows Machine” on page 471. |
<table>
<thead>
<tr>
<th>Scenario</th>
<th>How to achieve?</th>
</tr>
</thead>
</table>
| You want to extend the Windows Machine asset type to manage the inventory information. | - Use the Create new entity schema option on the Schema Manager view.  
- Create a new entity Inventory with relevant fields that are required to manage the inventory.  
- Use the Extend existing asset type option.  
- Add the inventory fields to the Windows Machine asset type.  
For a detailed procedure click on the link:  
See “Extending Windows Machine to manage inventory and vendor data information” on page 472. |
| You want to create custom asset types printers, scanners, monitors, and so on to manage the physical devices in the enterprise. | - Use the Create new entity schema option on the Schema Manager view,  
- Create a new platform Devices and a new entity Printer.  
- Use the Add new asset type option on the Schema Manager view.  
- Create a new asset type, Printer based on the custom platform, Devices.  
For a detailed procedure click on the link:  
See “Creating a custom asset type-Printer based on the custom platform-Devices” on page 477. |

### Creating a custom asset type - Windows Service

In the scenario, create a custom asset type, Windows Service. You must use the Add new asset type option in the Schema Manager view to create the custom asset type.

Windows is one of the predefined platforms that the Control Compliance Suite supports.
See “Predefined platforms” on page 235.

Service is one of the primary entities that is not supported as a predefined asset type. Service can be a probable asset type.

See “Probable asset types” on page 273.

**To create a Windows Service asset type**

1. Go to Settings > Schema Manager.
2. Select **Add new asset type**.
3. In the Specify Asset Type Details panel of the Create New Asset Type wizard, type **WindowsService** in the Name field.
4. In the Select Platform and Primary Entity panel, do the following:
   - From the Platform drop-down list, select **Windows**.
   - From the Primary entity drop-down list, select **Service**.
     By default, the primary fields are listed in the Primary fields list. The primary fields for the Windows Service are as follows:
     - Domain/Workgroup Name
     - Machine Name
     - Service Name
     Click **Next**
5. In the Specify Fields panel, add the following fields from the Available fields list:
   - **Startup type**
     This field returns the method by which the service is started (automatic or manual)
   - **Owner**
     This field returns the name of the account that currently owns the Service.
   - **Status**
     This field returns the current status of the service process.
   - **Service Type**
     This field returns the internal type of the service process. Valid values are Shared Process and Own Process.
6 In the Customize Field Attributes panel, mark, **Owner** as the mandatory field and mark **startup type, service type,** and **status** as the optional fields and click **Next**.

See “**About the primary, mandatory, and optional fields**” on page 454.

7 In the Add External Fields panel, click **Next**.

8 In the Specify Asset Name Fields, select all the fields from the Available fields list and use the Add icon to add the fields to the Selected fields list.

Click **Next**.

From the Separator drop-down list, select **#**.

See “**About separators in name fields**” on page 455.

9 In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.


11 Launch the Control Compliance Suite Console and go to Manage > Assets > Asset System.

In the table pane, from the Display drop-down list, view the Windows Service asset type.

**Extending the predefined asset type - Windows Machine**

In the scenario, add the field TCP/IP Address to the predefined asset type, Windows Machine. You must use the Extend Asset Type wizard to add the field to the existing asset.

Control Compliance Suite lets you extend the existing asset types by modification of the default fields and addition of the optional fields to the asset types.

You can extend the predefined asset types and the custom asset types also.

**To extend an existing asset type**

1 Go to Settings > Schema Manager.

2 Select **Extend existing asset type** and click **Next**.

3 In the Select Asset Type panel of the Extend Asset Type wizard, from the Asset Type drop-down list, select **Windows Machine** and click **Next**.

The primary, mandatory, and optional fields for Windows Machine are displayed.
4 In the Select Optional Fields panel, select **TCP/IP Address (First)** from the Available fields list and add to the Selected fields list with the Add icon.

5 In the Customize Field Attributes panel, check the options **Is field part of job** and **Allow editing of field**.

When you extend an existing asset type, you can only add the optional fields. The optional fields are not required for data collection. You can explicitly mark the field to include in the data collection job.

Click **Next**.

6 In the Add External Fields panel, click **Next** without adding any external field.

7 In the Summary panel, review the selections that you made for the custom asset type.

Make sure that the field TCP/IP Address is available under the heading New Optional Fields and click **Finish**.

8 Close the Control Compliance Suite Console and restart the Symantec Application Server Service.

9 Launch the Control Compliance Suite Console and go to Manage > Assets > Asset System.

10 Select the Windows Machine asset type.

If you already have the assets for the Windows Machine, select an asset. In the details pane, under the Custom Properties tab, view the newly added field TCP/IP Address.

To import the values of the newly added field TCP/IP Address, go to Monitor > Jobs view and re-run the asset import job for Windows Machine.

---

**Extending Windows Machine to manage inventory and vendor data information**

Assume that you want to use the predefined asset type Windows Machine to manage the inventory and the vendor data.

Perform the following tasks:

- Create a new custom entity, Inventory using the Create new entity schema option from the Schema Manager view.
  
  Click on the link to create a new entity, Inventory.
  
  See “Create a custom entity- Inventory” on page 473.

- Extend the Windows Machine asset type to include the fields from the custom entity, Inventory, using the Extend asset type option from the Schema Manager view.
Click on the link to extend Windows Machine to include the fields from Inventory.
See “Extending Windows Machine to include the fields from Inventory” on page 475.

Create a custom entity - Inventory

The entity schema defines the platform, entities, and fields of an asset for which the data collector collects data. You can create a new entity schema only when you do not want to use any of the predefined platforms for data collection.

To create a custom entity - Inventory

1. Go to Settings > Schema Manager.
2. Select Create new entity schema to launch the Create New Entity Schema wizard.
3. In the Select or Create New Platform panel, select Create a new platform. In the Name box, type Custom and click Next.
   This platform name is used to create headers in the CSV file and table or view names in the ODBC database.
   See “Format to create ODBC compliant database tables” on page 363.
4. In the Specify Entity Details panel, in the Name box, type Inventory as the name of the entity.
5. In the Specify Entity Details pane, select Extend an existing entity. From the platform drop-down list, select Windows. From the entity drop-down list, select Machine. Select the folder path where you want to create the entity schema xml files and click Next.
6. In the Add Fields panel, click Add to add new fields for the entity.
7 In the Create New Field dialog box, create four fields as follows.

The number of primary fields for the new entity, Inventory must match the number of primary fields of Windows Machine. The objective to create the custom entity is to include the fields to the Windows Machine asset type. You must add the primary fields of Windows Machine as the primary fields of the entity, Inventory.

Let us add the four fields with the following details:

- Domain/Workgroup Name - Primary String data type
- Machine Name - Primary String data type
- Vendor Name String data type
- Address of the Vendor String data type
- Date/Time of Contract Expiry DateTime

Click Next.

8 In the Specify Entity Name Fields panel, select Domain/Workgroup Name and Machine Name from the Available fields list and add them to the Selected fields list.

The added primary fields form the name of the new entity.

From the list of Separators, select # and click Next.

9 In the Specify References panel, from platform list, select Windows and in the Parent entity list, select Machine.

Associate the fields of the <Windows>.<Machine> with the fields of the <Custom>.<Inventory> as follows:

- Domain/Workgroup Name Domain/Workgroup Name
- Machine Name Machine Name

The panel lets you create relation between the new entity and an entity of the predefined platform. A parent-child relation is created between the entity of the predefined platform and the new entity that you are creating. You can associate the primary fields of the new entity with the primary fields of the parent entity to create a parent-child relation. The parent-child relation lets you collect data for the parent entity along with the child entity.

See “About referenced entity fields” on page 454.

10 In the Summary panel, review the details of the created entity and click Finish.
11 Close the Control Compliance Suite Console.

12 Copy the XMLs at the following paths:
   ■ \<installdir>\Symantec\CCS\Reporting and Analytics
   ■ \<installdir>\Symantec\CCS\Reporting and Analytics\Application Server
   ■ \<installdir>\Symantec\CCS\Reporting and Analytics\DPS

13 Restart the Symantec Application Server Service and the Symantec Data Processing Service and launch the Control Compliance Suite Console again.

Now that you have a custom entity Inventory that extends from Windows Machine, you can include the newly added fields to the Windows Machine.

See “Extending Windows Machine to include the fields from Inventory” on page 475.

Extending Windows Machine to include the fields from Inventory

After you create the entity Inventory and extend it from the Windows Machine asset type, you must now include the Inventory fields to the Windows Machine asset type.

Use the Extend existing asset type option on the Schema Manager view to include the Inventory fields to the Windows Machine.

To extend the Windows Machine to include the fields from Inventory

1 Go to Settings > Schema Manager.

2 Select Extend existing asset type.

3 In the Select Asset Type panel, select Windows Machine and click Next.
   The primary, mandatory, and optional fields for the selected asset type are displayed.

4 In the Select Optional Fields panel, Select Include referenced entities and select Inventory from the list of entities.

5 Select Vendor Name, Address of Vendor, and Date/Time of Contract Expiry from the Available fields column. Use the Add icon to add the fields to the Selected fields column.
   Click Next.

See “About referenced entity fields” on page 454.
In the Customize Field Attributes panel, check **Is field part of job** for all the three fields and mark them editable.

When you extend an existing asset type, you can only add the optional fields. The optional fields are not required for data collection. You can explicitly mark the field to include in the data collection job.

Click **Next**.

In the Add External Fields panel, click **Next**.

In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.

Close the Control Compliance Suite Console, restart the Symantec Application Server Service and relaunch the Control Compliance Suite Console.

Now you have the predefined asset type, Windows Machine with the new fields from the entity, Inventory. You can use the default data collector, CSV data collector, or ODBC data collector to import the information about the Inventory fields. The extended Windows Machine asset type can be used like any other predefined asset type for asset import.

To import data from the CSV file for the newly added fields, create a CSV file with the following format:

```plaintext
Custom.Inventory.DomainName,
Custom.Inventory.MachineName,
Custom.Inventory.VendorName,
Custom.Inventory.VendorAddress,
Custom.Inventory.Date-TimeofContractExpiry
```

After you create a CSV file, share the file, and specify the share path for the CSV settings. After you create a CSV file, share the file and specify the share path in the CSV settings. You can then perform an asset import for the new fields.

To import data from an ODBC database for the newly added fields, create a database table or view with name as CustomInventory. Create table column names that are same as the field names such as, DomainName, MachineName, VendorName and so on. After you create the ODBC database tables, specify the database connection string in the ODBC settings. You can then perform an asset import for the new fields.

See “Configuring the CSV data collector” on page 156.

See “Configuring the ODBC data collector” on page 158.

See “Importing assets” on page 313.
Creating a custom asset type- Printer based on the custom platform- Devices

Assume that you want to manage the physical devices assets such as, printers, scanners, monitors, keyboards and so on. The predefined asset types cannot manage these assets. The predefined platforms and the data collectors cannot help you gather data about these assets. Now, you must create custom asset types for printers, scanners and so on. You must first create a new platform and a custom entity based on which the custom asset types can be created.

Perform the following tasks:

- Create a new platform, Devices and a new entity, Printer
  See “Creating a custom platform- Devices and the custom entity- Printer” on page 477.
- Create a new asset type, Printer
  See “Creating a custom asset type- Printer” on page 479.

Creating a custom platform- Devices and the custom entity- Printer

Let us use the Create new entity schema option and create an entirely new platform and entity for managing the physical assets or devices in the enterprise. You can create a new platform, Devices and create multiple entities that are based on the platform as Printer, Scanner, Monitors, Keyboard and so on. You can then create asset types based on each of the entities and use the asset types to import the data for the entities.

You must use the Create new entity schema option from the Schema Manager view to create a new platform and an entity.

To create a custom platform- Devices and the custom entity- Printer

1. Go to Settings > Schema Manager.
2. Select Create new entity schema to launch the Create New Entity Schema wizard.
3. In the Select or Create New Platform panel, select Create a new platform.
   In the Name box, type Devices.
   Enter the name of the platform. This platform name is used to create headers in the CSV file and table or view names in the ODBC database.
   See “Format to create ODBC compliant database tables” on page 363.
   In the Display Name box, type Devices and click Next.
4 In the Specify Entity Details panel, in the Name box, type **Printer** as the name of the entity.

In the Display Name box, type **Printer** and click **Next**.

The display name of the entity appears in the evaluation report that is generated for the collected data of the asset.

5 In the Add Fields panel, click **Add** to add new fields for the entity.

6 In the Create New Field dialog box, create fields with the following details:

   - **Name:** String data type
     - **Printer Name**
     - **Name:** String data type
       - **Printer Type**
   - **Name:** Boolean data type
     - **Is double sided?**

In the Add Fields panel, click **Next**.

7 In the Specify Entity Name Fields panel, **PrinterName** from the Available fields list and add them to the Selected fields list.

   Click **Next**.

8 In the Specify References panel, click **Next**.

   Let us not specify any field from the existing entities as the reference fields for `<Devices><Printer>`.

   You can alternatively specify a field from the existing entity and establish a relation between the two fields. In this case, the field from the parent entity becomes the primary asset type if you want to import the assets from the Printer asset type.

   See “**Primary and secondary assets**” on page 275.

   See “**About referenced entity fields**” on page 454.

9 In the Summary panel, review the details of the created entity and click **Finish**.

10 Close the Control Compliance Suite Console.

11 Copy the XMLs at the following paths:
   - `<installdir>\Symantec\CCS\Reporting and Analytics`
   - `<installdir>\Symantec\CCS\Reporting and Analytics\Application Server`
12  Go to Start > Run, type services.msc, restart the Symantec Application Server Service and re-launch the Console after two minutes.

Creating a custom asset type- Printer

Let us create a custom asset type, Printer that is based on the custom platform, Devices and the custom entity, Printer that you created in

To create a Windows Service asset type
1  Go to Settings > Schema Manager.
2  Select Add new asset type.
3  In the Specify Asset Type Details panel of the Create New Asset Type wizard, type Printer in the Name field and in the Display name field and click Next.
4  In the Select Platform and Primary Entity panel, do the following:
   ▪  From the Platform drop-down list, select Devices.
   ▪  From the Primary entity drop-down list, select Printer and click Next.
5  In the Specify Fields panel, add the following fields from the Available fields list to the Selected fields list and click Next.
   ▪  Type of the printer
   ▪  Is double sided?
6  In the Customize Field Attributes panel, mark the field Type of the printer as Mandatory and the field Is double sided? as Optional
   Select Is field part of job for both the fields and click Next.
   See “About the primary, mandatory, and optional fields” on page 454.
7  In the Add External Fields panel, click Add.
8  In the Add New Field dialog box, type Location and select String as the data type.
9  In the Specify Asset Name Fields, select Name of the printer from the Available fields list and add it to the Selected fields list.
   Click Next.
10 In the Summary panel, review the selections that you made for the custom asset type and click Finish.
11 Close the Control Compliance Suite Console and restart the Symantec Application Service.

12 Launch the Control Compliance Suite Console and go to Manage > Assets > Asset System.

   In the table pane, from the Display drop-down list, view the Printer as the new asset type.

Now you have the new asset type, Printer that is based on the new platform, Custom and the new entity Printer. Configure either a CSV data collector or an ODBC data collector to import assets of the asset type, Printer.

To import the data for the Printer fields using a CSV data collector, create a CSV file with the following format:

   Devices.Printer.Printername,
   Devices.Printer.PrinterType,
   Devices.Printer.IsdoubleSided,

To import data for the Printer fields from an ODBC database for the newly added fields, create a database table or view with name as DevicesPrinter. Create table column names that are same as the field names such as, PrinterName, PrinterType, IsdoubleSided and so on. After you create the ODBC database tables, specify the database connection string in the ODBC settings. You can then perform an asset import for the new fields.

To learn the procedure to import the assets for the asset type, printer click on the following links:

   See “Importing the specific and common fields for custom asset using the CSV data collector” on page 338.

   See “Configuring the ODBC data collector” on page 158.

   See “Creating a target type for the asset type - Printer” on page 480.

Creating a target type for the asset type - Printer

   After you import the assets for the custom asset type, Printer you might want to collect the data for the Printer.

   See “Setting up a data collection job from the Assets view” on page 380.

To evaluate the assets for the Printer, you must create custom checks and build a standard. To create custom checks for the custom asset type, Printer you must create a target type.
You can create a target type that is based on the fields of the asset type, Printer. PrinterName is the primary field and the PrinterType and Is DoubleSided are the other fields of the Printer asset type.

Let us create a target type that is based on the field, PrinterType.

To create a target type for the asset type - Printer

1. Go to Settings > Schema Manager.
2. Click Create New Target Type.
3. In the Specify Name and Description for Target Type panel, type DotNet and click Next.
4. In the Select Platform and Asset Type panel, select Devices as the platform and Printer as the asset type.
5. In the Create Asset Type filters panel, select PrinterType from the drop-down list and click Add Statement to add a filter statement.
6. In the Filter Statement dialog box, select Specific Value as the parameter type.
   Select EqualTo (=) as the operator and type DotNet in the Specify Value box.
   Click OK.
7. In the Create Asset Type filters panel, click Next.
8. In the Summary panel, review the information that you have entered in the wizard. Click Back to make any modifications or click Finish to exit the wizard.
   Go to Manage > Standards and create the custom checks that are based on the newly created target type.
   See “Creating a new check” on page 633.
Managing custom schema

Working with custom schema scenarios
Managing entitlements

This chapter includes the following topics:

- About entitlements
- Concepts in entitlements
- Working with control points
- Working with entitlements import
- Working with approval
- Working with notifications
- About the entitlements filters
- Viewing the control points information in the details pane

About entitlements

The Entitlements view in Control Compliance Suite facilitates the monitoring of access rights in the organization. The Entitlements view provides the means to efficiently gather the permissions data from the various platforms and enables the user to generate reports.

In a typical environment, IT compliance is confined to configuration management, the firewall, the antivirus systems, and the vulnerability assessment. However, there is a difference between managing security configurations and vulnerabilities and managing access controls and data entitlements. The IT department can implement processes for managing and auditing entitlements. The decision about who has access to what data lies with the business owner of that data. Incidents can occur when a valid user can have access to the data that the user should not access. The Entitlements view identifies these false entitlements. The Entitlements...
view lets you define the data that user X is entitled to access. The Entitlements view also monitors whether the system adheres to the defined access controls.

The Entitlements view lets you configure the control points and assign the review periods. The view also ensures the frequent approvals of the control points by the respective data owners. To know where an individual user and groups have rights is critical to safeguard the data. Merely the documentation of those rights is insufficient to safeguard the data. This information must correspond to the internal business processes and must be directly linked to data ownership. The ability to confirm the entitlements at regular intervals gives additional support to the organizations for demonstrating good stewardship. This confirmation ability includes internal and external data security, confidentiality, integrity, and availability.

See “Creating a review cycle setting” on page 503.

See “Problems in managing entitlements” on page 484.

Reasons for managing entitlements

User and group entitlements is one of the most significant and the most difficult aspects of IT security. In an organization, the protection of data is highly important, not only from external exploitation but also from internal misuse. A person in an organization who has illegal access to sensitive data can lead to undesirable effects. To determine who should have access to which data can be difficult, especially in large companies with a number of users. Large companies maintain many identity management roles and also maintain multiple databases that contain sensitive information. The concern that arises is to how entitlements should be determined.

See “Problems in managing entitlements” on page 484.

Problems in managing entitlements

Many companies maintain an Access Control List (ACL). This approach might serve the purpose of restricting access to sensitive information to a limited number of users. Equally important is to ensure that the authentic users have access to all the relevant data. This type of management requires extensive effort to gather information about users, to look at the data flows, and to conduct frequent analyses.

The following questions must be answered while monitoring entitlements in an organization:
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where does user X have access in the network?</td>
<td>When an employee leaves the company or is terminated for serious reasons, it becomes important to identify the risk exposure that the employee contributes.</td>
</tr>
<tr>
<td>Where in the network do the members of group X have access?</td>
<td>When a user is added to the group, the user inherits all the permissions that are assigned to that group. These inherited permissions should be audited diligently.</td>
</tr>
<tr>
<td>Who has access to the data X?</td>
<td>When all the access grants are finalized, the review of the complete list of read, write, and execute permissions on a regular basis is important.</td>
</tr>
<tr>
<td>Who validates that the access grants are appropriate?</td>
<td>Apart from a strong security model for the network, the proof of an ongoing review process is also needed to comply with various government regulations. To serve this purpose, organizations must be able to associate critical data with appropriate business data owners who can validate the access grants.</td>
</tr>
</tbody>
</table>

The approval of the entitlements on a periodic basis is in the core of the entitlements system.

See "Creating a review cycle setting" on page 503.

### About the entitlements system workflow

To understand the workflow of the entitlements system, you must review the concepts that are related to the entitlements system.

See "Concepts in entitlements" on page 496.

The workflow of the entitlements system starts with marking an asset as a control point and ends with the generation of the entitlements reports.

The entitlements reports include the Control Point Effective Permissions, the Control Point Simple Permissions, the Entitlement Changes, the Control Point Permissions by Trustee, and the Entitlement Change Requests.

See "About the control point status" on page 489.
The users in the role of an entitlement administrator and the entitlements data owner perform the tasks in the entitlements system.

See “Predefined roles” on page 97.

The tasks in the entitlements system can be divided as follows:

<table>
<thead>
<tr>
<th>Manual tasks</th>
<th>System tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Performed by the user</td>
<td>■ System tasks</td>
</tr>
<tr>
<td>■ Require user input and user action.</td>
<td>■ Require no user input and user action.</td>
</tr>
</tbody>
</table>

You can perform the following manual tasks in the entitlements system based on your role:

- **Mark an asset as a control point**
  See “Marking an asset as a control point” on page 378.

- **Create a review cycle setting**
  See “Creating a review cycle setting” on page 503.

- **Assign the role of data owner to a trustee**
  See “Adding users and groups to a role” on page 107.
Configure the control point

See “Configuring control points” on page 501.

You configure a control point to assign a data owner or an approver, the tags, and the review cycle to the control point.

The entitlements administrator can configure the control points from the Manage > Entitlements > Control Points view.

The control points status changes to Review Start Awaited when the control point is configured with a review cycle.

When you configure the control point with a review cycle the entitlements system transitions the control points in various states. The states are based on the review cycle status.

The control point status changes from Review Start Awaited to Review Started when the review cycle starts. The system starts the review cycle on the start date that is specified in the review cycle setting.

The system then changes the control point status from Review Started to Entitlement Import Required. The Entitlement Import Required status is set according to the number of days specified for importing the entitlements before the approval starts.

Import entitlements

See “Importing the entitlements manually” on page 511.

See “Configuring the automatic entitlements import” on page 510.

The entitlements administrator must import the entitlements before the approval starts. The entitlements are then available for the data owner to approve.

If the automatic entitlements import is not configured, then the entitlements administrator must import the entitlements manually.

The control point status changes from Entitlement Import Required state to Entitlement Import Pending when the entitlements import is in progress.

When the entitlement import is complete the system changes the control point status to Approval Start Awaited.
The control points status changes from Approval Start Awaited to Request for Approval when the approval period starts. The approval period starts on the approval start date that is specified in the review cycle setting.

<table>
<thead>
<tr>
<th>Request for Approval</th>
<th>The entitlement administrator requests the approval of entitlements when the approval period starts. After the entitlement administrator requests for approval, the data owner can either approve the entitlements or request changes in the entitlements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve the control points</td>
<td>The data owner can view the entitlements for the control points and approve the control points from the My Control Points view. The alternative approver can also approve the control points if the alternative approver is enabled. After the approval, the control point status changes to Approved.</td>
</tr>
<tr>
<td>Request changes in entitlements</td>
<td>The data owner can request changes in the entitlements of the control points. The control points status changes to Request for Change.</td>
</tr>
<tr>
<td>Request for Approval</td>
<td>The entitlement administrator can request for approval again when the IT department implements the change requests of the data owner. The entitlement administrator must import the entitlements again. When the entitlement administrator requests for approval of the control points for which a change is requested, the status changes to Entitlement Import Required.</td>
</tr>
</tbody>
</table>

See “Requesting approval of entitlements” on page 513.

See “Approving the entitlements” on page 514.

See “Alternative approver” on page 498.
Import entitlements

The entitlement administrator must import the entitlements before the approval starts. The entitlements are then available for the data owner for approval.

If the automatic entitlement import is not configured, the entitlement administrator must import the entitlements manually.

The control point status changes from Entitlement Import Required state to Entitlement Import Pending when the entitlements import is in progress.

When the entitlement import is complete the system changes the control point status to Request for Approval.

The data owner can now approve if the entitlements are as expected or again request for change if the entitlements are not as expected.

About the control point status

In the process of the approval of the entitlements, a control point moves through various states.

At any given time, a control point can be in any of the following states in the entitlements system:

- **No Review Configured**: Indicates that the control point has no review cycle that is associated with it.
  - No Review Configured is the default status of the control point, when an asset is marked as the control point.
  - A control point cannot be monitored for its entitlements in the approval workflow unless a review cycle is associated with it.

- **Review Start Awaited**: Indicates that the review cycle is associated with a control point and the review start date is awaited.
  - The review cycle start depends on the date that you indicate in the review cycle settings.
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Started</td>
<td>Indicates that the review cycle for the control point has started.</td>
</tr>
<tr>
<td></td>
<td>The review cycle starts after the daily approval job runs on the review cycle start date.</td>
</tr>
<tr>
<td></td>
<td>Status changes from Review Start Awaited to Review Started when the review cycle starts.</td>
</tr>
<tr>
<td>Entitlement Import Required</td>
<td>Indicates that the entitlements should be imported before the approval period begins.</td>
</tr>
<tr>
<td></td>
<td>The control point status changes to the Entitlement Import Required in the following cases:</td>
</tr>
<tr>
<td></td>
<td>• The status changes from Review Started to Entitlement Import Required according to the review cycle setting. In the review cycle setting, you mention the number of days before the approval start when you want to import the entitlements.</td>
</tr>
<tr>
<td></td>
<td>• The status changes from Request For Change to Entitlement Import Required when the entitlements administrator requests for the approval of control point after the entitlements are changed according to the change requests.</td>
</tr>
<tr>
<td>Entitlement Import Pending</td>
<td>Indicates that the entitlement import is in progress.</td>
</tr>
<tr>
<td></td>
<td>Status changes from Entitlement Import Required to Entitlement Import Pending.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Sometimes, in case of system failure during the entitlement import, control points are left in the Entitlement Import Pending status even after the system is up. You must revert the status to the Entitlement Import Required status to re-import the entitlements of these control points. To revert the status to the Entitlement Import Required status, go to Settings &gt; General &gt; Entitlements &gt; Revert Import Pending Control Point Status. You cannot revert the status if another entitlement import job is running.</td>
</tr>
<tr>
<td>Approval Start Awaited</td>
<td>Indicates that the approval period for the control points is yet to start after Entitlement Import.</td>
</tr>
</tbody>
</table>
Indicates that the request for approval is sent to the data owner of the control points.

The control point status changes to the Request for Approval in the following cases:

- The status changes from Approval Start Awaited to Request for Approval when the approval starts.
- The status changes from Entitlement Import Required to Request for Approval when the entitlement import is complete. This is in case of the re-importing of entitlements after the implementation of the change requests.

Indicates that the data owner has requested changes in the entitlements of the control points.

Status changes from Request for Approval to Request for Change.

Indicates that the data owner has approved the entitlements of the control points.

See “Working with control points” on page 500.

About the Control Points view

The Control Points view lets you manage the control points in the Control Compliance Suite.

You can access the Control Points view from Manage > Entitlements > Control Points.

The Control Points view contains the following panes:

- Tree pane
  This pane appears on the left side of the console window under the navigation bar.
  This pane displays the asset folders and asset groups under the Asset System node.

- Filter by pane
  This pane appears in the lower left side of the console window under the tree pane.
  You can use the following filters in the Control Points view:
  - Control point status
  - Select tags
The My Control Points view lets the data owner manage the control points that require the data owner's approval.

You can access the My Control Points view from Manage > Entitlements > My Control Points.

The My Control Points view contains the following panes:
About the Import Settings view

You can refine the entitlements import process from the network with the help of rules that are called import settings.

The Import Settings view lets you configure the analysis options for the following entitlement types:
- Windows File or Directory
- ESM File or Folder
- ESM User Group

You use the analysis options to narrow down the scope of the job when you import the entitlements.
**Note:** The import settings are applicable to all the entitlement import jobs for the selected control point type. For example, if you specify the import settings for Windows File and Directory, the settings are considered every time when the entitlements for the Windows File or Directory are imported.

You can set the following analysis options for the Windows File / Directory:

<table>
<thead>
<tr>
<th>Analysis types</th>
<th>You can select one of the following analysis types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Local and network analysis</td>
<td>Performs the full analysis of effective permissions whether they are obtained by logging on locally or by accessing the file system object through a share. This option executes a local analysis and a network analysis and combines the results.</td>
</tr>
<tr>
<td>■ Security descriptor only</td>
<td>Calculates the effective permissions to the file system object by analyzing only the security descriptor.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Analysis options</th>
<th>You can select any one or all the following analysis options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Report groups</td>
<td>Includes the Groups in the entitlement import</td>
</tr>
<tr>
<td>■ Report users</td>
<td>Includes only the users in the entitlement import</td>
</tr>
<tr>
<td>■ Skip logon workstations</td>
<td></td>
</tr>
</tbody>
</table>
Group analysis

You can select one of the following group analysis options:

- Report members of all groups
  Reports the members of all the groups that are contained in the scope of the entitlement import
- Do not report members of these groups
  Lets you type the names of the groups separated by semicolon. The members of the specified groups are not reported on in the entitlement import job.

You can set the following analysis options for ESM File, Folder entitlements and User Group entitlements:

Policy name

Lets you enter the ESM policy name.

The policy name that you specify is case sensitive.

See “Configuring the import settings” on page 508.

About the Browse Notifications view

The Notifications view lets you enable or disable notifications to be sent to the data owners. The notifications are sent to the data owners at certain time intervals during the review cycle.

You can access the Notifications view from Manage > Entitlements > Notifications.

You can configure the following types of notification:

- Review End
- Approval Start
- Approval End
- Approval Requested
- Review Start
- Data Owner Change
- Alternative Approver Changed

The Notifications view also lets you configure and customize the notifications.

See “Configuring entitlements notifications” on page 520.
About the Review Cycle Settings View

The Review Cycle Settings view lets you create review cycle settings. The review cycles that you create in this view, are used when you configure the control points. You can only assign a review cycle that is already created in the view.

See “Creating a review cycle setting” on page 503.

The Review Cycle Settings view contains the following panes:

Table pane
This pane appears under the taskbar.
This pane displays all the review cycle settings that you create.

Details pane
This pane appears in the lower right side of the console window under the table pane.
This pane displays the control points that are associated with the review cycle setting that is selected in the table pane.

Concepts in entitlements

To understand the workflow for managing the entitlements in Control Compliance Suite, you must first understand the concepts in the entitlements.

The following are the concepts in the Entitlements view:

- Control points
  See “Control points” on page 497.

- Data owners
  See “Data owners” on page 498.

- Alternative approver
  See “Alternative approver” on page 498.

- Review cycle setting
  See “Review cycle setting” on page 498.

- Approval period
  See “Approval period” on page 499.

- Tagging
  See “Tagging” on page 499.
Control points

A control point is the data location in the system at which the access permissions are granted and approved. You can mark an asset that is imported into the Control Compliance Suite system as a control point.

Consider the following directory structure:

C:\
C:\Data
C:\Data\Accounting
C:\Data\Accounting\Site 01
C:\Data\Accounting\Site 02
C:\Data\Accounting\Site 03

In the directory structure, the permissions for the Accounting folder are assigned at the data location, C:\Data\Accounting. The rights that are assigned at this point in the directory are also assigned down to any file or folder that exists under this directory. You can assign additional rights lower in this directory for a specific file or a folder. The file is the lowest level of control point.

You can also define a control point for a group. A group of users can have the same type of permissions for a certain directory or a file.

Note: You cannot mark Windows Machines or UNIX Machines as control points.

The entitlements system supports certain predefined asset types as control point types. In addition to the supported asset types, the entitlements cannot be imported for any custom asset type that you create. But, the entitlements system supports an extended predefined asset type that is supported as a control point type.

The entitlements system lets you mark the following asset types as control points:

- Oracle Configured Databases
- SQL Databases
- UNIX File
- UNIX Group
- Windows File
- Windows Group
- Windows Directory
- ESM Agents
The entitlements system supports the following entitlement types:

- ESM Agents
  - ESM File, Folder entitlements
  - ESM User Group entitlements
- Oracle Configured Databases
  - Stored procedure entitlements
  - Table entitlements
  - View entitlements
- SQL
  - Database entitlements
  - Stored procedure entitlements
  - Table entitlements
  - View entitlements

See “Working with control points” on page 500.

Data owners

Data owners are the business owners of the data.

Control Compliance Suite assumes that a person who is theoretically the business owner of the data- also owns the data in the system. The data owner has the responsibility to approve or decline permissions on the control points.

See “Configuring control points” on page 501.

Alternative approver

Control Compliance Suite lets you configure an alternative approver for the control points. The alternative approver performs the role of the data owner to approve the entitlements, in case the data owner is not available.

See “Configuring the alternative approver” on page 515.

Review cycle setting

The review cycle setting is the time frame for which the entitlements are validated. The entitlement administrator can define different review cycle settings for different types of data.
For example, an organization might want to validate the entitlements of the financial data two times in a year. However, the HR data might be validated only one time in a year.

The definition of the review cycle setting can be based on the organizational policies of approving entitlements.

A review cycle setting can be set as recurrent or non-recurrent. If you mark a review cycle setting as recurrent, the same review cycle setting repeats after the end of the review cycle setting. For example, if you define a review cycle setting for three months and mark it as recurrent, then the cycle is repeated every three months. Each review cycle setting that is completed becomes a review cycle instance.

See “Creating a review cycle setting” on page 503.

Approval period

The approval period of a control point is a subset of the review period.

The data owner should approve or request a change in the entitlements within the specified approval period. For example, consider that the review period for a set of control points is from January 1 to March 31. The approval period may be between February 1 and February 28.

See “Working with approval” on page 513.

Tagging

The assets that are marked as control points must be defined with reference to some context. You can define the control points according to their sensitivity, confidentiality, and value to the organization. The purpose of defining control points is such that the data owner understands the relevance of the control points. Each organization may have its own ways to classify the data. Control Compliance Suite lets you tag the control points. Tags are used to categorize data so that uniform permissions can be assigned to the data in the same category. This categorization is important for the most effective and the most efficient use of the data.

Tags can be based on the critical value of the data such as confidential, public, or classified. Tags can be also based on how often the data needs to be accessed. You can define the tags according to the department, such as human resources, finance, and marketing. Well-planned tags make the essential data easy to find. The tags can be of particular importance in risk management, legal discovery, and compliance with government regulations.
The Entitlements view lets you assign tags to the control points and categorize the control points as required. You can assign multiple tags to a control point. The tagging of a control point is not mandatory.

## Working with control points

In Control Compliance Suite, you mark an asset as a control point to monitor the entitlements on that control point.

In the entitlement system, you perform the following tasks with the control points:

- Mark an asset as a control point
  See “Marking an asset as a control point” on page 378.

- Unmark a control point
  See “Unmarking a control point” on page 501.

- Configure a control point
  See “Configuring control points” on page 501.

- Create review cycle settings
  See “Creating a review cycle setting” on page 503.

## Control point type and entitlement type

The entitlements system supports certain predefined asset types as control point types. In addition to the supported asset types, the entitlements cannot be imported for any custom asset type that you create. But, the entitlements system supports an extended predefined asset type that is supported as a control point type.

The entitlements system supports the following control point types and entitlement types:

- ESM Agents
  - ESM File, Folder entitlements
  - ESM User Group entitlements

- Oracle Configured Databases
  - Stored Procedure entitlements
  - Table entitlements
  - View entitlements

- SQL
  - Database entitlements
Unmarking a control point

You can unmark a control point from the entitlements management view. To unmark a control point, you must be the entitlements administrator.

To unmark a control point

1. Go to Manage > Entitlements > Control Points.
2. In the table panel, right-click a control point and select **Unmark as control point**.

See “Marking an asset as a control point” on page 378.

See “Control points” on page 497.

Configuring control points

You can configure the control points to make them available for monitoring in the approval workflow. The configuration of the control points associates the control points with the data owner, the alternative approver, the tags, and the review cycle.

**Note:** You can associate the review cycle setting to the control point only if the date of entitlements import before the approval start is yet to arrive.

Make sure that you have at least one review cycle setting created before you configure a control point.
See “Creating a review cycle setting” on page 503.

To launch the Configure Control Points wizard
1  Go to Manage > Entitlements > Control Points.
2  From the table pane, right-click a control point and select Configure Control Point.

To configure the data owners
1  In the Configure Data Owners panel, type a description.
   The description is optional.
2  Under the Data owner details section, click Browse and select a data owner to associate with the control points.
   You can use the Clear option to remove the associated data owner.
   The user that you select as a data owner is a primary data owner.
3  Select Enable Alternative Approver to allow the secondary data owner to approve the control points in the absence of the primary data owner.
   The assignment of the alternative approver is an optional step.
4  Under the Alternative approver details section, click Browse and select a user as an alternative approver.
5  Click Next.

To assign tags to the control points
1  In the Assign Tags panel, click Add.
2  In the Select Tags dialog, select a tag from the Tags node and click Add.
3  Click OK.
4  In the Assign Tags panel, click Next.
To configure a review cycle
1 In the Specify Review Cycle Details panel, select one of the following:

- No Review Required: Lets you choose not to associate the control point with any review cycle. The selected control points do not follow the approval-based reviews.
- Retain Existing Review Cycle: Lets you retain the existing review cycle. This option is enabled only if the control points have the previous review cycles configured.
- Assign a New Review Cycle: Lets you select a review cycle from the existing review cycles.

2 Click Next.

To assign a new review cycle
1 In the Assign a Review Cycle panel, select a review cycle setting from the existing review cycles to associate with the control points.

2 Click Next.

3 In the Summary panel, click Finish.

See “Marking an asset as a control point” on page 378.
See “Unmarking a control point” on page 501.
See “Control points” on page 497.

Creating a review cycle setting
Only the entitlement administrator can configure a review cycle setting.
The review cycle setting is a time period during which you want to monitor the entitlements of a set of control points.

See “Review cycle setting” on page 498.

To create a review cycle setting
1 Go to Manage > Entitlements > Review Cycle Setting.

2 In the taskbar, click Create.

3 In the Create Review Cycle Setting dialog box, specify the following information and click OK.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you type a name for the review cycle.</td>
</tr>
<tr>
<td>Duration</td>
<td>Lets you select a duration for the review cycle.</td>
</tr>
<tr>
<td></td>
<td>You can select the duration from the following options:</td>
</tr>
<tr>
<td></td>
<td>■ 1 Week</td>
</tr>
<tr>
<td></td>
<td>■ 2 Weeks</td>
</tr>
<tr>
<td></td>
<td>■ 1 Month</td>
</tr>
<tr>
<td></td>
<td>■ 3 Months</td>
</tr>
<tr>
<td></td>
<td>■ 6 Months</td>
</tr>
<tr>
<td></td>
<td>■ 1 year</td>
</tr>
<tr>
<td>Next Review Start Date</td>
<td>Lets you choose a date from when the review cycle should start.</td>
</tr>
<tr>
<td>Approval Start</td>
<td>Lets you select a period before the review end date to start the approval.</td>
</tr>
<tr>
<td></td>
<td>Approval start indicates that the data owner has to approve the control points within the specified limit before the review ends.</td>
</tr>
<tr>
<td></td>
<td>You can select from the following options:</td>
</tr>
<tr>
<td></td>
<td>■ 1 Week</td>
</tr>
<tr>
<td></td>
<td>■ 2 Weeks</td>
</tr>
<tr>
<td></td>
<td>■ 1 Month</td>
</tr>
<tr>
<td></td>
<td>■ 3 Months</td>
</tr>
<tr>
<td></td>
<td>■ 6 Months</td>
</tr>
<tr>
<td></td>
<td>■ 1 year</td>
</tr>
<tr>
<td>Approval Duration</td>
<td>Lets you select a duration for the approval period.</td>
</tr>
<tr>
<td></td>
<td>You can select from the following options:</td>
</tr>
<tr>
<td></td>
<td>■ 1 Week</td>
</tr>
<tr>
<td></td>
<td>■ 2 Weeks</td>
</tr>
<tr>
<td></td>
<td>■ 1 Month</td>
</tr>
<tr>
<td></td>
<td>■ 3 Months</td>
</tr>
<tr>
<td></td>
<td>■ 6 Months</td>
</tr>
<tr>
<td></td>
<td>■ 1 year</td>
</tr>
<tr>
<td>Is Recurring?</td>
<td>Lets you select a True or False value to make the review cycle recurring.</td>
</tr>
</tbody>
</table>
Import Entitlements before # days of Approval Start

Lets you select the number of days before the approval start date, to import the entitlements.

You can choose to import the entitlements from 0 to 150 days before the approval start.

See “Deleting a review cycle setting” on page 505.

Deleting a review cycle setting

The entitlement administrator can delete the review cycle setting from the Review Cycle Settings view.

Note: You can delete the review cycle setting if the control points are not associated with the review cycle. In case of non-recurring review cycles, you can delete the review cycle setting after the end of the review cycle even if the control points are associated with it.

To delete a review cycle setting

2. Select a review cycle setting that you want to delete.
3. From the taskbar, click Delete.
4. In the message box, click Yes if you want to delete the review cycle setting and click No if you want to retain the review cycle setting.

See “Creating a review cycle setting” on page 503.

Comparing entitlements

You can compare the entitlements of a control point, only if the control point is approved at least once.

The current entitlements are compared with the latest approved entitlements.

To compare the entitlements

1. Go to > Manage > Entitlements > Control Points.
2. In the table pane, select a control point that you want to compare and select Compare Entitlements.
3. The Compare Entitlements dialog box presents the following details.
Control Point Details

Presents the following details about the control points:
- Asset type
- Domain/Workgroup name
- Machine name
- Directory name

Entitlement Comparison

Lets you select the entitlement type that you want to compare.

Summary

Displays a record of the change in entitlements in the form of rows added, removed, changed, and unchanged.

View Rows

Lets you select a filter from the drop-down list. You can choose to view only the rows that were added, removed, changed, or unchanged.

4 Click **OK** to close the dialog box.

Viewing control point details

You can view the details of the control point from the **Manage > Entitlements > Control Points** view.

To view the control point details

1 Go to **Manage > Entitlements > Control Points**.
2 In the table pane, select a control point.
3 In the task bar, select **View Details**.
4 View the control points details in the following tabs:
   - General
     See “Control point details pane- General tab” on page 525.
   - Entitlements
     See “Control point details pane- Entitlements tab” on page 526.
   - Review Cycle
     See “Control point details pane- Review Cycle tab” on page 526.
   - Entitlement Import Details
Working with entitlements import

In the entitlements system workflow, you import the entitlements of the control points in any of the following states:

- Before the approval period begins the entitlement administrator imports the entitlements of the control points.
- After the entitlements are changed according to the change request by the data owner, the entitlement administrator imports the entitlements of the control points.

See “About the control point status” on page 489.

In the entitlement system, you perform the following tasks with the entitlement import:

- Configure the import settings.
  See “Configuring the import settings” on page 508.
- Configure the automatic entitlements import.
  See “Configuring the automatic entitlements import” on page 510.
- Import the entitlements manually.
  See “Importing the entitlements manually” on page 511.

About entitlements import

Only the entitlement administrator can perform the task of entitlement import.

In the entitlements system workflow, you import the entitlements of the control points in any of the following states:

- Before the approval period begins
- After the entitlements are changed according to the change request by the data owner

To get the latest entitlements of the control points that await the entitlements import, you can also manually create an entitlement import job. You can manually import the entitlements of the control points in any state.

The manual and automatic entitlements import work as follows:
To manually import the entitlements of the control points, you create an entitlements import job. You can run the entitlements import job immediately or schedule the job to run when the approval period of the control points is about to begin. See “Importing the entitlements manually” on page 511.

To automatically import the entitlements of the control points, you configure the automatic entitlements import job. The automatic entitlement import job runs daily at a specified time. The job imports entitlements for all the control points that display the status as Entitlements Import Required. See “Configuring the automatic entitlements import” on page 510.

Configuring the import settings

You can refine the entitlements import process with the help of the rules that are called as the import settings.

The Import Settings view is divided into the following tabs:

- Windows File or Directory
- ESM File or Folder
- ESM User Group

**Note:** The import settings are applicable to all the entitlement import jobs for the selected control point type. For example, if you specify the import settings for Windows File and Directory, the settings are considered every time when the entitlements for the Windows File or Directory are imported.
To configure the import settings

1. Go to Manage > Entitlements > Import Settings.

2. To specify the import settings for the Windows File or Directory, use the following options and click **Save**.

<table>
<thead>
<tr>
<th>Analysis types</th>
<th>You can select one of the following analysis types:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Local and network analysis. Performs the full analysis of effective permissions whether they are obtained by logging on locally or by accessing the file system object through a share. This option executes a local analysis and a network analysis and combines the results.</td>
</tr>
<tr>
<td></td>
<td>■ Security descriptor only. Calculates the effective permissions to the file system object by analyzing only the security descriptor.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Analysis options</th>
<th>You can select any one or all the following analysis options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Report groups. Includes the Groups in the entitlement import</td>
</tr>
<tr>
<td></td>
<td>■ Report users. Includes only the users in the entitlement import</td>
</tr>
<tr>
<td></td>
<td>■ Skip logon workstations.</td>
</tr>
</tbody>
</table>
Group analysis

You can select one of the following group analysis options:

- Report members of all groups.
  Reports the members of all the groups that are contained in the scope of the entitlement import
- Do not report members of these groups.
  Lets you type the names of the groups in the separated by a semicolon. The members of the specified groups are not reported on in the entitlement import job.

3 To specify the import settings for ESM- File, Folder Entitlements and ESM-User Group Entitlements, type the policy name and click Save.

The policy name that you type is case-sensitive. The policy name that you type is used when you import the entitlements for the ESM Agents control points.

Configuring the automatic entitlements import

You configure the automatic entitlements import to get the latest entitlements of the control points on daily basis.

The automatic entitlement import job imports the entitlements for the control points that are in the Entitlement Import Required state.

Consider the following case:

- You have a control point that is in the Entitlements Import Required state.
- The automatic entitlement import job is scheduled to run at 12 midnight.
- You import the entitlements of the control points manually at 8 PM before the automatic entitlement import job runs.
- The automatic entitlement import does not fetch any entitlements as the control point is not in the state of Entitlement Import Required.
**Note:** In case of importing the entitlements for ESM Agents, it is recommended that you customize the templates to limit the entitlement import only for specific objects. The entitlement import for ESM Agents may generate a large amount of data unless you restrict it to a specific scope. The results are stored in the production database (CSM_DB) which may lead to the increase in the size of the database.

See “About entitlements import” on page 507.

**To configure the automatic entitlements import**

1. Go to Settings > General > Application Configuration > Entitlements.
2. Under the Automatic import settings, check Automatically import entitlements.
3. In the Automatic import job run time, specify the time when you want the daily entitlement job to run.

See “Importing the entitlements manually” on page 511.

**Importing the entitlements manually**

You can import the entitlements for the control points using the Create or Edit Entitlements Import Job wizard. The import of entitlements with the wizard is manual import.

You can also configure an automatic entitlement import job to run on a periodic basis. The automatic import job imports the entitlements of the control points that are in the Entitlement Import Required state.

See “Configuring the automatic entitlements import” on page 510.

Consider the following case:

- You have a control point that is in the Entitlements Import Required state.
- The automatic entitlement import job is scheduled to run at 12 midnight.
- You import the entitlements of the control points manually at 8 PM before the automatic entitlement import job runs.
- The automatic entitlement import does not fetch any entitlements as the control point is not in the state of Entitlement Import Required.

**To import the entitlements manually**

1. Go to Manage > Entitlements > Control Points.
2. Right-click in the table pane and select Import Entitlements.
3 In the Specify Job Name and Description panel, type the name for the import job in the Name box and click **Next**.

You can alternatively type the description for the import job.

4 In the Select Platform, Asset Type, and Entitlement Type panel, select the platform, the control point type, and the entitlement type to import.

Click **Next**.

See “Control point type and entitlement type” on page 500.

5 In the Add Asset Scope panel, select the control points by navigating through the asset hierarchy.

Click **Add** to add the selected control points to the import job and click **Next**.

In case of importing the entitlements for ESM Agents, it is recommended that you customize the templates to limit the entitlement import only for specific objects. The entitlement import for ESM Agents may generate a large amount of data unless you restrict it to a specific scope. The results are stored in the production database (CSM_DB) which may lead to the increase in the size of the database.

6 In the Specify Filters panel, under the Data Owners click **Add** and select a data owner.

Only the control points with the selected data owner are included in the imported job. You can select the **Consider Alternate Approver** option if you want to filter on the alternative approver.

7 Under the Tags click **Add** and select the tags.

Only the control points with the selected tags are included in the import job. If you select more than one tag, you can also select the **Include only if all tags assigned** option. The selection of this option includes the control points only if all the tags that are added are assigned to the control point. If you do not select the **Include only if all tags assigned** option, the import job includes the control points with any selected tags.

8 In the Specify Filters panel, click **Next**.

9 In the Schedule panel, select any one of the following:

- If you want to run the job after the wizard closes, check **Run now**.

- If you want to run the job at a specified interval, check **Run periodically** and enter the following information:
  - In the Start On box, enter the start date and time to run the job.
  - Under the Run Periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific
days, select the number of days in the Run Every Day list box. Click Next.

10 In the Specify Notification Details panel, enter the job completion notification details.

Check **Send notification** and enter the following information:

- Enter the subject and message of the notification mail.
- Enter the sender's and the receiver's email ID.
  Notification can be sent to multiple recipients.

11 Click **Next**.

12 In the Summary panel, review the configurations that you made for the import job and click **Finish**.

See “Configuring the automatic entitlements import” on page 510.

## Working with approval

The approval-related tasks of the control point include the following:

- Request approval
  See “Requesting approval of entitlements” on page 513.

- Request change
  See “Requesting changes in entitlements” on page 514.

- Approve
  See “Approving the entitlements” on page 514.

- Configure alternative approver
  See “Configuring the alternative approver” on page 515.

### Requesting approval of entitlements

Only the entitlements administrator can perform the task of sending an approval request.

You, as an entitlement administrator can send an approval request to the data owner, when the entitlements for control point in status Request for Change are modified as per the change request. The control points change their status to Entitlement Import Required. After the entitlement import is complete for these control points, the status changes to Request for Approval.
To request approval of entitlements

1. Go to Manage > Entitlements > Control Points.
2. In the table pane, right-click a control point with the Request for Change status and select **Request Approval**.

See “Requesting changes in entitlements” on page 514.

See “Approving the entitlements” on page 514.

Requesting changes in entitlements

Only the data owner or the alternative approver can request changes in entitlements.

You, as an entitlements data owner, can request changes in the entitlements of the control points, if you are in the role of the entitlements data owner for those control points. The control points status changes to Request for Change.

**To request changes in entitlements**

1. Log on as an entitlements data owner.
2. Go to Manage > Entitlements > My Control Points.
3. In the table pane, select the control point with the status Request for Approval.
4. In the details pane, under the Entitlements tab, review the entitlements of the selected control point.
5. In the table pane, right-click the control point for which changes should be requested and select **Request Change**.
6. In the Request Change for Control Points dialog box, type the change request in the Comments field and click **Request Change**.

See “Approving the entitlements” on page 514.

Approving the entitlements

Only the data owner or the alternative approver approves the entitlements of the control points, depending on who is the active approver.

You as a data owner, approve the entitlements of the control points, if you are in the role of the entitlements data owner for those control points. The control points status changes to Approved after the control points are approved.

**To approve the entitlements**

1. Log on as an entitlements data owner.
2. Go to Manage > Entitlements > My Control Points.
3 In the table pane, select the control point with the status Request for Approval.

4 In the details pane, under the Entitlements tab, review the entitlements of the selected control point.

5 In the table pane, right-click the control point for which changes should be requested and select Approve.

6 In the Approve Control Points dialog box, type the comments and click Approve.

See “Requesting changes in entitlements” on page 514.

Configuring the alternative approver

The data owner can configure an alternative approver for the control point. You can choose to configure an alternative trustee who can perform the role of the data owner to approve the entitlements in case the data owner is not available.

An entitlement administrator can configure and enable an alternative approver when the control point is configured.

See “Configuring control points” on page 501.

An entitlement data owner can also configure an alternative approver for the control points that the data owner owns.

To configure the alternative approver

1 Log on as an entitlement data owner.

2 Go to Manage > Entitlements > My Control Points.

3 Right-click the control point for which you want to configure an alternative approver and select Configure Alternative Approver.

4 In the Assign Alternative Approver dialog box, select a user from the Available Users list and click Add.

5 Check Enable alternative approver if you want the alternative approver to review the entitlements and approve or request for change in the entitlements.

6 Click OK

See “Alternative approver” on page 498.

About the daily approval job

The daily approval job is a hidden system job that runs daily at a specified time. You can specify the time for the daily approval job to run daily in the Entitlement Global Settings.
See “Configuring the entitlements settings” on page 171.

The daily approval job is responsible for the state transitions of the control points in a review cycle.

The notifications about the control point status are sent to the responsible owner after the daily approval job runs.

## Working with notifications

Only the entitlement administrator can configure the notification events.

The data owners get the notifications about the important state transitions of the control points that need the attention of the data owner.

In the entitlements system, the control point acquires its status based on where the control point lies in the entitlements workflow. The entitlements system lets you configure the notifications that are sent to the data owners who own the control points. The notifications are sent as an email to the data owner.

See “About the notification events” on page 516.

See “Configuring entitlements notifications” on page 520.

### About the notification events

In the entitlements system, the control point acquires its status that is based on where it lies in the entitlements workflow. The entitlements system lets you configure the notifications that are sent to the data owners who own the control points. The notifications are meant to inform the data owner about the status of the control point. The notifications are sent as an email to the data owner.

You can configure the following types of notifications:
Review Cycle Start

This notification event is generated at the beginning of the review cycle for the set of control points.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See “Configuring entitlements notifications” on page 520.

Approval Period Start

This notification is generated at the beginning of the approval period.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See “Configuring entitlements notifications” on page 520.
Approval Period End

This notification is generated at the end of the approval period.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See “Configuring entitlements notifications” on page 520.

Review Cycle End

This notification is generated at the end of the review cycle.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See “Configuring entitlements notifications” on page 520.
Approval Requested

This notification is generated when the status of the control point changes to Request for Approval.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See “Configuring entitlements notifications” on page 520.

Change in Data Owner or Alternative Approver Configuration

This notification is generated when the data owner or the alternative approver is assigned to a control point, or the data owner or the alternative approver changes.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.
Approver Activated

This notification is sent to the user who is mentioned in the To field of the notification.

This notification can be sent in any of the following cases:

- When the entitlement administrator configures a data owner.
- When the data owner configures an alternative approver for the control point and enables the alternative approver.

This notification is sent to the user that is mentioned in the To field. You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation.

The notifications for all the control points that belong to the same review cycle are consolidated and sent within an hour.

See “Configuring entitlements notifications” on page 520.

Configuring entitlements notifications

You configure the email notifications from the Manage > Entitlements > Browse Notification Events view.

**Note:** The notifications are sent to the data owner email addresses that are specified as tokens in the email configuration. The token for the email address reads the email address from the User Management view. Ensure that the User Management view reflects the updated email address of the user to whom the notification should be sent.
To configure notifications

1. Go to Manage > Entitlements > Browse Notification Events.

2. Right-click the notification event that you want to configure and click **Edit Notification**.

3. In the Edit Notification Events dialog box, in the Send notification option, do one of the following:
   - **Immediately**
     Sends the notification immediately after the daily approval job runs on the event date.
     For example, if the approval period for a control point starts today at 12 PM, the notification is sent immediately when the daily approval job runs after 12 PM. In this case, if another nine control points belong to the same review cycle, then separate notification is sent for each control point for the same event.
   - **After consolidation**
     Consolidates the notifications of all the control points that belong to the same review cycle.
     For example, if the approval period for ten control points that belong to the same review cycle starts today at 12 PM a consolidated notification is sent within an hour after the daily approval job runs.

4. Select **Disable notification for this event** if you want to disable the notification for this event.

5. In the **Send reminder notification # days before event date** option, select the number of days. The reminder notification is sent before the specified number of days of the event date.

6. Create a notification text with the tokens.
   See “**About notification tokens**” on page 521.

7. To preview the notification, click **Preview** and then click **OK**.

**About notification tokens**

You use tokens to configure the notification text in the entitlement system. You can customize the notifications that are sent to the data owners when the control point status changes. To create a standard text that should be sent to the data owner, you use the tokens.

Tokens are similar to variables. The actual value replaces the tokens when the notification is sent.

The token with their descriptions are as follows:
<table>
<thead>
<tr>
<th>Token Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataOwnerMailAddress</td>
<td>Address token that is used in the To field.</td>
</tr>
<tr>
<td></td>
<td>The email ID of the data owner replaces the token.</td>
</tr>
<tr>
<td>AlternateApproverMailAddress</td>
<td>Address token that is used in the To field.</td>
</tr>
<tr>
<td></td>
<td>The email ID of the alternative approver replaces the token.</td>
</tr>
<tr>
<td>DataOwnerName</td>
<td>Body or Subject token that can either be used in the subject line or the message body.</td>
</tr>
<tr>
<td></td>
<td>The name of the data owner replaces the token.</td>
</tr>
<tr>
<td>AlternateApproverName</td>
<td>Body or Subject token that can be used either in the subject line or in the message body.</td>
</tr>
<tr>
<td></td>
<td>The name of the alternative approver replaces the token.</td>
</tr>
<tr>
<td>ReviewCycleName</td>
<td>Body or Subject token that can be used either in the subject line or in the message body.</td>
</tr>
<tr>
<td></td>
<td>The name of the review cycle replaces the token.</td>
</tr>
<tr>
<td>ReviewCycleStartDate</td>
<td>Body or Subject token that can be used either in the subject line or in the message body.</td>
</tr>
<tr>
<td></td>
<td>The review cycle start date replaces the token.</td>
</tr>
<tr>
<td>ApprovalStartDate</td>
<td>Body or Subject token that can either be used in the subject line or the message body.</td>
</tr>
<tr>
<td></td>
<td>The approval period start date replaces the token.</td>
</tr>
<tr>
<td>ApprovalEndDate</td>
<td>Body or Subject token that can be used either in the subject line or in the message body.</td>
</tr>
<tr>
<td></td>
<td>The approval period end date replaces the token.</td>
</tr>
<tr>
<td>Token Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ReviewCycleEndDate</td>
<td>Body or Subject token that can be used either in the subject line or in the message body. The review cycle end date replaces the token.</td>
</tr>
<tr>
<td>AutomaticImportRequiredDate</td>
<td>Body or Subject token that can be used either in the subject line or in the message body. The date when the control point status changes to Entitlement Import Required replaces the token.</td>
</tr>
<tr>
<td>ReviewCycleSettingsDetails</td>
<td>Body or Subject token that can be used either in the subject line or in the message body. The details of the review cycle settings replace the token.</td>
</tr>
<tr>
<td>ReviewCycleDates</td>
<td>Body or Subject token that can be used either in the subject line or in the message body. The dates that are applicable in case of the review cycle replace the token. This includes the approval start, approval end, review start, review end, and the import required dates.</td>
</tr>
<tr>
<td>ControlPointIdentifier</td>
<td>Body token that can be used in the message body. The name of the control point replaces the token.</td>
</tr>
<tr>
<td>ApproverName</td>
<td>Body or Subject token that can be used either in the subject line or in the message body. The name of the alternative approver replaces the token.</td>
</tr>
<tr>
<td>ApproverMailAddress</td>
<td>Body or Subject token that can be used either in the subject line or in the message body. The email ID of the alternative approver replaces the token.</td>
</tr>
</tbody>
</table>
About the entitlements filters

The Filter pane shows the filters that you can use to display only the required control points.

Control Compliance Suite provides the following default filters for filtering the control points:

- Control point status
  See “Control Point Status filter” on page 524.

- Tags
  See “Tag filter” on page 524.

Control Point Status filter

During the entitlements workflow a control point can display a different status at a different point of time. You can use the Control Point Status filter to filter the control points that display a particular status.

You can select from any of the following control point states to filter the control points of your choice:

- Request for Change
- Request for Approval
- Approved
- No Review Configured
- Review Start Awaited
- Approval Start Awaited
- Entitlement Import Required
- Entitlement Import Pending
- Review Started

Tag filter

You can use the Tag filter when you want to filter the existing control points that display a specific tag. From the list of tags, you can select the corresponding check boxes to select the specific tags. The control points that display the selected tag are shown in the table pane.

To edit the filter, you click on the Customize icon at the top of the Filter by pane.
You can view the information about the control points through the details pane.

To view the control point information
1. In the table pane, select the control point for which you want to view the information.
2. View the information for the selected control point in the details pane.

The details pane displays all the information about the selected control point in the following tabs:

- **General**
  See “Control point details pane- General tab” on page 525.

- **Entitlements**
  See “Control point details pane- Entitlements tab” on page 526.

- **Review Cycle**
  See “Control point details pane- Review Cycle tab” on page 526.

- **Entitlement Import Details**
  See “Control points details pane- Entitlement Import Details tab” on page 527.

- **Review Cycle Dates**
  See “Control points details pane- Review Cycle Dates tab” on page 527.

- **Tags**
  See “Control point details pane- Tags tab” on page 527.

- **Exceptions**
  See “Control point details pane- Exceptions tab” on page 527.

- **Workflow Trails**
  See “Control point details pane- Workflow Trails tab” on page 528.

### Control point details pane- General tab

The General tab of the control point details pane provides the general information about the selected control point.

The General tab contains the following details about the control points:

| Description | Displays the description of the control point that you provide while you configure the control point. |
Control point details pane- Entitlements tab

The Entitlements tab of the control points details pane presents the entitlements in case the entitlements are imported for the control point.

You can select the entitlement type in case of the Oracle, the SQL, and the ESM control points. You can view the entitlement details of the selected entitlement type.

You can also choose to view the simple or the effective permissions.

Control point details pane- Review Cycle tab

The Review Cycle tab presents all the details of the review cycle that are associated with the selected control point.
The details include the following:
- Name
- Review duration
- Next review start date
- Approval start
- Approval duration
- Import entitlements # days before the approval start
- Is recurring (Yes or No)

See “Creating a review cycle setting” on page 503.

Control points details pane- Entitlement Import Details tab

The Entitlement Import Details tab of the control point details pane provides information about the entitlements that are imported for the selected control point.

The Entitlement Import Details tab provides the following information:
- Entitlement type
- Last import date
- Last approved date

Control points details pane- Review Cycle Dates tab

The Review Cycle Dates tab of the control points details pane provides the information about the review cycle dates for the selected control point.

Control point details pane- Tags tab

The Tags tab of the control point details pane contains a list of all the tags that are associated with the selected asset.

The Tags tab also lets you add a new tag to associate with the selected asset.

You can also remove a tag that is already associated with the asset from the Tags tab.

Control point details pane- Exceptions tab

The Exceptions tab lists all the exceptions that are applied to the selected control point.
Control point details pane- Workflow Trails tab

The Workflow Trails tab of the control point details pane provides information about the control point status changes.

The Workflow Trails tab presents a tabular view that contains the date and the time details about the control point status transition.
Managing exceptions

This chapter includes the following topics:

- Concepts in exception
- About the Exceptions view
- Working with exceptions

Concepts in exception

Before you begin to perform the exception-related tasks, you should review the following concepts in exceptions:

- Exception Management System
  See “About the exception management system” on page 530.

- Exceptions
  See “About exceptions” on page 530.

- Exception validity
  See “About exception validity” on page 531.

- Exception templates
  See “About exception templates” on page 532.

- Exception states
  See “About exception states” on page 533.

- Exception filters
  See “About the exception filters” on page 534.
About exceptions

Exceptions are the temporary permissions that exempt an asset from following an organizational policy for a specific time period. Make an exception for a valid business reason.

For example, consider a check that verifies whether the latest Microsoft patch is installed on Windows Server 2003. The mailing server administrator may only be able to apply the patch over the weekend. Because applying the patch requires the computer to be restarted, which can have an effect on the mailing infrastructure of the company. Under such a situation, the mailing administrator can request an exception to be made.

The exception management system creates and tracks exceptions in Control Compliance Suite.

Before creating exceptions, complete the settings available in the Settings > General Settings > Exceptions.

The following permissions must be assigned while creating exceptions:

- Exception for asset on check or an exception for check on asset: View Asset and View Standard
- Exception for control points: View Asset
- Exception for policy on asset or an exception for asset on policy: View Asset and View Policies

Certain predefined roles are required for exceptions.

See “Predefined roles” on page 97.

See “About the exception management system” on page 530.

About the exception management system

Exception management is a well-defined system that is used to create, manage, track, and report the exceptions in the Control Compliance Suite.

The exception management system provides a central place for handling exceptions of different modules in Control Compliance Suite.

At the present time, the following modules are permitted the use of exceptions:

- Standards
- Entitlements
- Policies
About exception validity

Exceptions are applicable only for a specific time period. This time period is specified when the exception is requested. You can modify the time period when you edit the exception.

The exception validity time period consists of the following terms:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective date</strong></td>
<td>The start date when the exception is applied to the specified objects.</td>
</tr>
<tr>
<td></td>
<td>When you modify an exception, you can only postpone the effective date.</td>
</tr>
<tr>
<td></td>
<td>For example, if the validity period is 24th Aug to 26th Aug, you can change</td>
</tr>
<tr>
<td></td>
<td>the effective date to 25th or 26th Aug. You cannot change the date to 23rd</td>
</tr>
<tr>
<td></td>
<td>Aug.</td>
</tr>
<tr>
<td><strong>Effective time</strong></td>
<td>The local time at which the exception validity period begins. The exception is</td>
</tr>
<tr>
<td></td>
<td>applied to the specified objects at this time on the specified effective</td>
</tr>
<tr>
<td></td>
<td>date.</td>
</tr>
<tr>
<td></td>
<td>When an exception is created or modified, the effective time by default is</td>
</tr>
<tr>
<td></td>
<td>12:00 a.m. local time.</td>
</tr>
<tr>
<td><strong>Expiration date</strong></td>
<td>The end date when the exception no longer remains valid. From this date</td>
</tr>
<tr>
<td></td>
<td>onward, the exception is not applied to the specified objects.</td>
</tr>
<tr>
<td></td>
<td>The expiration date must be equal to or greater than the effective date.</td>
</tr>
<tr>
<td></td>
<td>You can change this date when you modify an exception.</td>
</tr>
<tr>
<td></td>
<td>When the current date exceeds the expiration date, the exceptions are marked</td>
</tr>
<tr>
<td></td>
<td>as expired automatically.</td>
</tr>
</tbody>
</table>
Expiration time

The local time at which the exception validity period ends. The exception becomes invalid at this time on the specified expiration date.

When an exception is created or modified, the expiration time by default is 11:59 p.m. local time.

An internal system job runs at 12 a.m. by default to mark all the exceptions due for expiration as **Expired**.

Ensure that your scheduled jobs such as an Evaluation job, Collection-Evaluation-Reporting job and so on do not clash with the scheduled time of the system job.

The system job is internal and is not visible in the Jobs view. However, you can change the scheduled time of the system job.

### About exception templates

Each module that registers with the exceptions management system has a template. A template governs the kind of information that is stored in the exception. The template specifies the objects that are exempted from following the normal organizational process. A module can have more than one template.

**Table 10-1**  

<table>
<thead>
<tr>
<th>Module</th>
<th>Template</th>
<th>Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>Evaluation Exception</td>
<td>The objects are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Sections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Checks</td>
</tr>
<tr>
<td>Entitlements</td>
<td>Entitlement Exception</td>
<td>The objects can be associated with assets, asset groups, and asset containers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Control Points</td>
</tr>
</tbody>
</table>
Object Template Module

Policies

The objects can be associated with assets, asset groups, and asset containers.

Policy Exception Policies

The exception workflow with reference to the exception states can be explained as follows:

- A requestor requests an exception for a particular object. An exception request is created and the initial state is set to Requested.
- An approver must then review the requested exception. The approver can go through the exception details and act in one of the following ways:
  - The approver can set the exception state to In Review to show that the exception is under consideration.
  - The approver may want more information regarding the exception. The Approver can then set the exception state to Request Clarification.
  - The approver can review the exception details and approve the exception. The exception state is set to Approved.
  - If the approver does not want to approve the exception request, the approver can set the exception state to Deny.
  - If the approver takes no action on the exception request until the specified effective date, then the system sets the state to Approval Overdue.
  - If the expiration date of the exception is reached, then the system sets the exception state to Expired. A requestor can also set the state to Expired if the exception is no longer required. An approver cannot set the exception state to Expired.

An exception can be in one of the following states:

### Table 10-2 Exception states

<table>
<thead>
<tr>
<th>Exception State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested</td>
<td>This state indicates that a requestor has requested or modified an exception.</td>
</tr>
<tr>
<td>Approved</td>
<td>This state indicates that an approver has approved the exception.</td>
</tr>
</tbody>
</table>
Table 10-2 Exception states (continued)

<table>
<thead>
<tr>
<th>Exception State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Clarification</td>
<td>This state indicates that the approver requires additional information about the exception.</td>
</tr>
<tr>
<td>In Review</td>
<td>This state indicates that the approver has the exception under consideration.</td>
</tr>
<tr>
<td>Deny</td>
<td>This state indicates that the approver has rejected the exception request.</td>
</tr>
<tr>
<td>Approval Overdue</td>
<td>This state indicates that the approver has performed no action on the exception request until the effective date of the exception.</td>
</tr>
<tr>
<td>Expired</td>
<td>This state indicates that the exception is now invalid.</td>
</tr>
<tr>
<td></td>
<td>The system sets the status of an exception as expired when the current date has exceeded the expiration date of the exception.</td>
</tr>
<tr>
<td></td>
<td>A requestor can set the status of an exception as expired at any time.</td>
</tr>
</tbody>
</table>

About the exception filters

The Filter by pane contains the filters that you can use to display only the required exceptions.

The Control Compliance Suite provides the following default filters for filtering the exceptions:

- **Exception Types**: Lets you filter the exceptions according to the type of module for which the exception is created.
- **Exception States**: Lets you filter the exceptions according to the specified exception state.
- **Others**: Lets you filter the exceptions according to the specified requestors.
- **Select Tags**: Lets you filter the exceptions according to the specified tags.
  - **Match Any**: Select the Match Any option to display the exceptions that match any one of the listed tags.
  - **Match All**: Select the Match All option to display the exceptions that match all the listed tags.
About the Exceptions view

The exception management view is used to manage and track all the exceptions in the Control Compliance Suite.

You can access the exception management view from Manage > Exceptions.

The exception management view lets you perform the following tasks:

- Request an exception for specific objects.
- Approve an exception request.
- Edit an exception.
- Change the exception state.

Working with exceptions

You can perform the following tasks using exceptions:

- View exception information in the details pane
  See “Viewing exception information in the details pane” on page 535.
- Request an exception
  See “Requesting an exception” on page 538.
- Approve an exception
  See “Approving an exception” on page 542.
- Set the exception state to In Review
  See “Setting the exception state to In Review” on page 545.
- Set the exception state to Request Clarification
  See “Setting the exception state to Request Clarification” on page 545.
- Set the exception state to Deny
  See “Setting the exception state to Deny” on page 546.

Viewing exception information in the details pane

You can view the information about an exception through the details pane.

**To view the exception information**

1. In the table pane of the Exceptions view, select the exception for which you want to display the information.
2. View the information for the selected exception in the details pane.

The exception details are contained in the following tabs:
General
See “Exceptions details pane - General tab” on page 536.

Associations
See “Exceptions details pane - Associations tab” on page 537.

Notifications
See “Exceptions details pane - Notifications tab” on page 538.

Tags
See “Exceptions details pane - Tags tab” on page 537.

Workflow Trails
See “Exceptions details pane - Workflow Trails tab” on page 537.

Exceptions details pane - General tab
The General tab of the Exception details pane provides general information about the selected exception.

The General tab presents the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name of the exception.</td>
</tr>
<tr>
<td>Type</td>
<td>The module that contains the objects that should be exempted.</td>
</tr>
<tr>
<td>Requestor</td>
<td>The name of the requestor.</td>
</tr>
<tr>
<td>Effective Date</td>
<td>The start date of the exception validity period. The exception is applied to the specified objects from this date onward.</td>
</tr>
<tr>
<td>Effective Time</td>
<td>The local time at which the exception validity period begins. The exception is applied to the specified objects at this time on the specified effective date.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The end date of the exception validity period. From this date onward, the exception is no longer applicable on the specified objects.</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>The local time at which the exception validity period ends. The exception becomes invalid at this time on the specified expiration date.</td>
</tr>
<tr>
<td>Requestor Group</td>
<td>The name of the requestor group.</td>
</tr>
<tr>
<td>Requestor Email ID</td>
<td>The email address of the requestor.</td>
</tr>
<tr>
<td>Attachment</td>
<td>The name of the files that are attached with the exception.</td>
</tr>
</tbody>
</table>
Description: The description for the exception.

See “Viewing exception information in the details pane” on page 535.

**Exceptions details pane - Associations tab**

The Associations tab of the exceptions details pane provides information about the selected objects.

The Associations tab presents a list of selected checks and assets.

You may not be able to see any objects on the Associations tab if either of the following situations is present:

- The requestor has not entered the object information.
- You do not have the required permissions to view all the objects that the requestor has selected.

If guid is visible or associations are not visible then the following permissions must be given:

- Exception for asset on check or an exception for check on asset
- View Asset and View Standard AssetException for control points
- View Asset
- Exception for policy on asset or an exception for asset on policy
- View Asset and View Policies

See “Viewing exception information in the details pane” on page 535.

**Exceptions details pane - Tags tab**

The Tags tab contains a list of all the tags that are associated with a selected exception.

The Tags tab lets you apply the tags that can be associated with a selected exception. You can also remove the tags that are already associated with an exception.

See “Viewing exception information in the details pane” on page 535.

**Exceptions details pane - Workflow Trails tab**

The Workflow Trails tab lets you keep track of all the state changes that an exception has gone through.

The Workflow Trails tab contains the following information:
The name of the user who has initiated the state change of the exception.

Modifier Name

The name of the user who has initiated the state change of the exception.

Modifier SAM Account name

The SAM Account name of the modifier. The format for the SAM Account name is domainname\username.

Changed Status

The state of the exception.

Comments

The remarks that the user entered.

Status Changed on

The date and time at which the state of the exception was changed.

See “Viewing exception information in the details pane” on page 535.

Exceptions details pane - Notifications tab

The Notifications tab of the Exceptions details pane provides information about the notification of the selected exception.

The Notifications tab presents the following information:

Notification types

The following notification types are supported:

- Requested
- Update and Changed State
- Pre Expiration

The default message for each notification type is displayed upon selection.

Subject

The subject of the exception is displayed.

Message

The message of the notification is displayed along with the tokens supported.

You can change the information of the notification by selecting the notification type and by changing the subject and the messages. After changing the information you have to click Save. When the notification is sent, the actual values replace the tokens.

See “Viewing exception information in the details pane” on page 535.

Requesting an exception

A requestor can request an exception through the Request Exception Wizard.

A requestor can request an exception on the following objects:
Standards, sections, or checks
See “Requesting an exception for assets on checks” on page 379.

Control points
See “Requesting an exception for control points” on page 539.

Policies
See “Requesting an exception for assets on policies” on page 540.

Similarly, you can request an exception by launching the Request Exception Wizard from the Standards view, Assets view, and the Evaluation Results dialog.

See “Launching the Request Exception Wizard” on page 541.

See “About exception states ” on page 533.

**Requesting an exception for control points**

A requestor can request an exception for specified control points in the organization.

**To request an exception**

1. Go to Manage > Exceptions.

2. In the Exceptions view, do either of the following:
   - On the taskbar, click **Request Exception**.
   - In the table pane, right-click anywhere on the grid and select **Request Exception**.

3. In the Request Exception Wizard, in the Specify Exception Details panel, enter the following details and click **Next**:
   - In the Title box, enter the name of the exception.
   - In the Type box, select **Entitlements**.
     In the Template box, let the displayed template name remain as Entitlement Exception.
   - In the Description box, type a description for the exception.
   - In the Attachment box, browse to enter the name of the file that you want to attach.
   - In the Exception Validity group box, in the Effective Date box, select the date on which the exception becomes applicable. In the Expiration Date box, select the date on which the exception becomes invalid. Click **Next**.

4. In the Select Control Points panel, click **Add** to select the control points.
5 In the Select Control Points dialog box, expand the Asset System folder and select a folder. Select the control points that you want to exempt and click **Add**. Click **Add All** to select all the control points. To remove one or more control points from the Selected Items list, click **Remove** or **Remove All** respectively. Click **OK**.

6 In the Select Control Points panel, click **Next**.

7 In the Specify Requestor Information panel, type or browse to enter the Requestor and the Requestor Group. Enter the Requestor Email ID and Comments.

8 In the Specify Notification Information panel, edit the notification information for the notification type. Select the tab of the notification type. Modify the Subject and the Message. Click **Next**.

9 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.

The exception is created and its state is set to Requested.

See “Launching the Request Exception Wizard” on page 541.

See “About exception states ” on page 533.

**Requesting an exception for assets on policies**

A requestor can request an exception on the policies for specific assets in the organization.

**To request an exception**

1 Go to Manage > Exceptions.

2 In the Exceptions view, do either of the following:
   - On the taskbar, click **Request Exception**.
   - In the table pane, right-click anywhere on the grid and select **Request Exception**.

3 In the Request Exception Wizard, in the Specify Exception Details panel, enter the following details and click **Next**:
   - In the Title box, enter the name of the exception.
   - In the Type box, select **Policies**.
     - In the Template box, let the displayed template name remain as Policy Exception.
   - In the Description box, type a description for the exception.
In the Attachment box, browse to enter the name of the file that you want to attach.

In the Exception Validity group box, in the Effective Date box, select the date on which the exception becomes applicable. In the Expiration Date box, select the date on which the exception becomes invalid. Click Next.

4 In the Select Policies and Assets panel, click Add to select the policies.

5 In the Select Policies dialog box, expand the Policies folder and select a folder. Select the policies and click Add. Click Add All to select all the policies. To remove one or more policies or all the policies from the Selected Items list, click Remove or Remove All. Click OK.

6 In the Select Policies and Assets panel, click Add to select the assets. In the Asset Object Chooser dialog box, expand the Assets folder and select a folder. Select the assets and click Add. Click Add All to select all the assets. To remove the assets from the Selected Items list, select the assets and click Remove. Click Remove All to remove all the assets. Click OK.

7 In the Select Policies and Assets panel, click Next.

8 In the Specify Requestor Information panel, type or browse to enter the Requestor and the Requestor Group. Enter the Requestor Email ID and Comments.

9 In the Specify Notification Information panel, edit the notification information for the notification type. Select the tab of the notification type. Modify the Subject and the Message. Click Next.

10 In the Summary panel, verify the details that you have entered in the wizard. Click Back to modify any data. Click Finish to exit the wizard.

The exception is created and its state is set to Requested.

See “Launching the Request Exception Wizard” on page 541.

See “About exception states” on page 533.

Launching the Request Exception Wizard

You can request an exception through the Request Exception Wizard. The Request Exception Wizard can be launched from various views.

To launch the Request Exception Wizard from the Standards view

1 Go to Manage > Standards

2 In the Standards view, select the standards, sections, or checks for which you want to request an exception and do one of the following:

   On the taskbar, click Request Exception.
■ On the Tasks menu, click Request Exception.
■ In the table pane, right-click the selection and select Request Exception.

To launch the Request Exception Wizard from the Assets view
1 Go to Manage > Asset Management > Assets.
2 In the Assets view, select the assets for which you want to create an exception and do one of the following:
   ■ On the taskbar, click Request Exception.
   ■ On the Tasks menu, click Request Exception.
   ■ In the table pane, right-click the selection and select Request Exception.

To launch the Request Exception Wizard from the Exceptions view
1 Go to Manage > Exceptions.
2 In the Exceptions view, do one of the following:
   ■ On the taskbar, click Request Exception.
   ■ In the table pane, right-click anywhere on the grid and select Request Exception.

Approving an exception

An approver can approve an exception through the Approve Exception Wizard. An approver can approve an exception request on the following objects:
■ Standards, sections, or checks
  See “Approving an exception for assets on checks” on page 542.
■ Control points
  See “Approving an exception for control points” on page 543.
■ Policies
  See “Approving an exception for policies” on page 544.

See “About exception states ” on page 533.

Approving an exception for assets on checks

An approver can approve an exception request on the checks for specific assets in the organization.
To approve an exception

1. Go to Manage > Exceptions.

2. In the table pane of the Exceptions view, do either of the following:
   - Select the exception that you want to approve, right-click, and select Approve Exception.
   - Select the exception that you want to approve and select Approve Exception on the taskbar.

3. In the View Exception Details panel, view the exception information that the requestor has entered. Click Next.

4. In the View or Select Checks and Assets panel, view the information that the requestor has entered. All the objects (checks and assets) may not be visible in case of either of the following situations:
   - The requestor has not entered the object information.
     In this case, click Add to specify the objects for which the exception must be created.
   - You do not have the required permissions to view all the objects that the requestor has selected. In this case, ensure that you get the required permissions.

5. Click Next.

6. In the Specify Comments panel, in the Comments box, enter your comments.

7. In the View the Notification Information panel, read the notification information. Select the tab to view the notification of a particular notification type. After reading the information, click Next.

8. In the Summary panel, verify the details that you have entered in the wizard. Click Back to modify any data. Click Finish to exit the wizard.

The state of the exception is set to Approved. In the table pane, the exception is present under the Approved list.

Approving an exception for control points

An approver can approve an exception request for specific control points in the organization.

To approve an exception

1. Go to Manage > Exceptions.

2. In the table pane of the Exceptions view, do either of the following:
Select the exception that you want to approve, right-click, and select **Approve Exception**.

Select the exception that you want to approve and select **Approve Exception** on the taskbar.

3 In the View Exception Details panel, view the exception information that the requestor has entered. Click **Next**.

4 In the View or Select Control Points panel, view the information that the requestor has entered. All the objects (control points) may not be visible in case of either of the following situations:

   - The requestor has not entered the object information.
     In this case, click **Add** to specify the objects for which the exception must be created.

   - You do not have the required permissions to view all the objects that the requestor has selected. In this case, ensure that you get the required permissions.

5 Click **Next**.

6 In the Specify Comments panel, in the Comments box, enter your comments.

7 In the View the Notification Information panel, read the notification information. Select the tab to view the notification of a particular notification type. After reading the information, click **Next**.

8 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.

The state of the exception is set to Approved. In the table pane, the exception is present under the Approved list.

**Approving an exception for policies**

An approver can approve an exception request on the policies for specific assets in the organization.

**To approve an exception**

1 Go to Manage > Exceptions.

2 In the table pane of the Exceptions view, do either of the following:
   - Select the exception that you want to approve, right-click, and select **Approve Exception**.
   - Select the exception that you want to approve and select **Approve Exception** on the taskbar.
3 In the View Exception Details panel, view the exception information that the requestor has entered. Click Next.

4 In the View or Select Policies and Assets panel, view the information that the requestor has entered. All the objects (policies and assets) may not be visible in case of either of the following situations:
   - The requestor has not entered the object information.
     In this case, click Add to specify the objects for which the exception must be created.
   - You do not have the required permissions to view all the objects that the requestor has selected. In this case, ensure that you get the required permissions.

5 Click Next.

6 In the Specify Comments panel, in the Comments box, enter your comments.

7 In the View the Notification Information panel, read the notification information. Select the tab to view the notification of a particular notification type. After reading the information, click Next.

8 In the Summary panel, verify the details that you have entered in the wizard. Click Back to modify any data. Click Finish to exit the wizard.

The state of the exception is set to Approved. In the table pane, the exception is present under the Approved list.

### Setting the exception state to In Review

An approver can set the exception state to In Review to show that the exception is under the review process.

**To set the In Review state**

1 Go to Manage > Exceptions.

2 In the Exceptions view, select the exception, right-click, and select Set Status to In Review.

3 In the Comments dialog box, type your comments and select In Review.

See “About exception states” on page 533.

### Setting the exception state to Request Clarification

An approver can set the exception state to Request Clarification to show that some additional information is required before the exception can be approved.
To set the Request Clarification state

1. Go to Manage > Exceptions.
2. In the Exceptions view, select the exception, right-click, and select Request Clarification.
3. In the Comments dialog box, type your comments and select Request Clarification.

See “About exception states” on page 533.

Setting the exception state to Deny

An approver can set the exception state to Deny to show that the exception request has been rejected.

To set the Deny state

1. Go to Manage > Exceptions.
2. In the Exceptions view, select the exception, right-click, and select Deny Exception.
3. In the Comments dialog box, type your comments and select Deny.

See “About exception states” on page 533.

Setting the exception state to Expire

A requestor can set the exception state to Expire to make the exception invalid.

To set the Expire state

1. Go to Manage > Exceptions.
2. In the Exceptions view, select the exception, right-click, and select Terminate Exception.
3. In the Confirm Terminate dialog box, click Terminate.

See “About exception states” on page 533.

Modifying an exception

A requestor can modify the exception information through the details pane.

You cannot edit an expired exception.

Note: When an exception is modified, the state of the exception is set to Requested.
To modify an exception

1. Go to Manage > Exceptions.
2. In the Exception view, select the exception that you want to modify.
3. In the details pane, on the general tab, you can edit the following information:
   - Effective Date
   - Expiration Date
   - Requestor Email ID
   - Description
4. On the Associations tab, click Add to select and add the objects to the exception. To remove the objects, select the objects and click Remove.
5. On the Tags tab, click Add Tag to add a tag for the exception. To remove tags, select the tags and click Remove Tag.
6. Click the save icon to save your changes.
Working with exceptions
Managing standards

This chapter includes the following topics:

■ Concepts in standards management
■ Concepts in checks
■ About the Standards view
■ About the standard migration utility for ESM and CCS
■ Working with standards
■ Working with sections
■ Working with checks
■ Working in the details pane
■ Working with Evaluation Results
■ About risk score calculation
■ About compliance score calculation

Concepts in standards management

Standards, sections, and checks form the backbone of the Standards module. Before you begin to perform the standards tasks, you must go through the following concepts:

■ Standards
  See “About standards” on page 550.
■ Predefined standards
  See “About predefined standards” on page 550.
About standards

Standards provide the means for assessing the compliance of an asset. In Control Compliance Suite, a standard is a hierarchical organizational structure of sections and checks.

Control Compliance Suite makes available a set of predefined standards that are installed along with the product. These standards are mostly derived from some published guidelines by established organizations such as CIS or NSA.

You can also create new standards that are based on your specific requirements. In Control Compliance Suite, the standards hierarchy is explained as follows:

- A standard contains one or more sections.
- Each section can further contain other sections or checks.
- A check is always contained within a section in a standard.

See “About sections” on page 556.
See “About checks” on page 556.
See “About predefined standards” on page 550.
See “Working with standards” on page 598.
See “About versioning scheme” on page 569.

About predefined standards

Predefined standards are the standards that are installed along with Control Compliance Suite. These standards are present in the Predefined folder in the
tree pane of the Standards view. The predefined standards are not editable, but can be copied to the user-defined folder. The copies can then be modified.

You can perform only the following actions on the predefined standards:

- Copy
- Export
- Set up a data collection job
- Run an evaluation job
- Request an exception
- Run collection-evaluation-reporting job

Control Compliance Suite ships with the predefined standards for the following platforms:

- ESM
  See “Predefined standards for ESM” on page 551.
- Oracle
  See “Predefined standards for Oracle” on page 553.
- SQL
  See “Predefined standards for SQL” on page 553.
- UNIX
  See “Predefined standards for UNIX” on page 554.
- Windows
  See “Predefined standards for Windows” on page 554.
- NetWare
  See “Predefined standards for NetWare” on page 555.
- Exchange
  See “Predefined standards for Exchange” on page 555.

See “About standards” on page 550.
See “Working with standards” on page 598.

Predefined standards for ESM

The predefined standards are the standards that are installed along with the product. The predefined standards are present in the predefined folder in the tree pane. These standards are not editable.

Each check expression in a standard is mapped to an ESM policy. You can also map multiple checks of an ESM policy to one CCS standard. The checks that a
A predefined standard contains map to only one ESM policy. However, in customized standards, you can map each check to different CCS standards.

**Note:** You cannot edit a predefined standard. You can copy the predefined standards and then customize them as per your requirement.

See “Copying and pasting a standard” on page 603.

Table 11-1 contains the following information:

- The name of the predefined CCS standards.
- The corresponding ESM policies, which contain the checks that map to each CCS standard.
- The location of the policy installer.

<table>
<thead>
<tr>
<th>Predefined CCS standard</th>
<th>ESM policy</th>
<th>ESM policy installer in the product disc</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM - CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0</td>
<td>Security essentials W2K3DC v2.0</td>
<td>Content_Updates\Policies\Security Essentials\Policies\Windows_2003_Security Essentials.exe</td>
</tr>
<tr>
<td>ESM - CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0</td>
<td>Security essentials W2K3MS v2.0</td>
<td>Content_Updates\Policies\Security Essentials\Policies\Windows_2003_Security Essential.exe</td>
</tr>
<tr>
<td>ESM - CIS for Solaris 10 Benchmark v4.0</td>
<td>Security essentials Sol 10 v4.0</td>
<td>Content_Updates\Policies\Security Essentials\Policies\Solaris\Solaris10_Security Essentials.exe</td>
</tr>
<tr>
<td>ESM - Change Notifications for Windows</td>
<td>WS3 Server SOA Change</td>
<td>Content_Updates\Policies\Sarbanes-Oxley\Policies\Microsoft\Intel\w3s-ix86\Windows_2003_SOA_Change_Notification.exe</td>
</tr>
</tbody>
</table>
Table 11-1  CCS standard to ESM policy mapping (continued)

<table>
<thead>
<tr>
<th>Predefined CCS standard</th>
<th>ESM policy</th>
<th>ESM policy installer in the product disc</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM - Change Notifications for UNIX</td>
<td>Sol 8-9 SOA Change</td>
<td>Content_Updates\Policies\Sarbanes-Oxley\Policies\Solaris\Solaris_SOA_Change_Notification.exe</td>
</tr>
<tr>
<td>File, Folder Entitlements</td>
<td>File, Folder Entitlements</td>
<td>Content_Updates\Policies\Sarbanes-Oxley\Policies\BestPractice_Entitlement_Reporting.exe</td>
</tr>
<tr>
<td>User, Group Entitlements</td>
<td>User, Group Entitlements</td>
<td>Content_Updates\Policies\Sarbanes-Oxley\Policies\BestPractice_Entitlement_Reporting.exe</td>
</tr>
</tbody>
</table>

Note: The ESM - Change Notifications for Windows and ESM - Change Notifications for UNIX standards are based on the Change Notification category of messages in Enterprise Security Manager.

Predefined standards for Oracle

The predefined standards for the Oracle platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Oracle

See “About predefined standards” on page 550.

The following predefined standard for the Oracle platform is installed with the product:

- CIS Oracle 9i and 10g Database Security Benchmark v2.0
  You must ensure that you configure bv-Control for Windows SQL Server, bv-Control for UNIX, and bv-Control for Windows with the Information Server for this standard.

Predefined standards for SQL

The predefined standards for the SQL platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Sql
See “About predefined standards” on page 550.

The following predefined standards for the SQL platform are installed with the product:

- CIS Security Configuration Benchmark for Microsoft SQL Server 2005 v1.1.1
- CIS Security Configuration Benchmark for Microsoft SQL Server 2005 v1.1.1
- The Australian Government Information and Communications Technology Security Manual for MS-SQL Server
  You must ensure that you configure bv-Control for Windows SQL Server and bv-Control for Windows with the Information Server for this standard.
- Security Essentials for SQL Server 2008

Predefined standards for UNIX

The predefined standards for the UNIX platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Unix

See “About predefined standards” on page 550.

The following predefined standards for the UNIX platform are installed with the product:

- Security Essentials for AIX 5.1 and Above
- Security Essentials for Solaris 10
- Security Essentials for HP-UX
- Security Essentials for Red Hat Enterprise Linux 2.1 and Above
- Security Essentials for SuSE Linux Enterprise Server

Note: Along with the predefined standards, the regulatory standards for the UNIX platform are also installed with the product.

Predefined standards for Windows

The predefined standards for the Windows platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Windows

See “About predefined standards” on page 550.

The following predefined standards for the Windows platform are installed with the product:
CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0
- CIS Legacy Settings Benchmark for Windows XP Professional v2.0
- CIS Windows 2000 Server Operating System Server Level Two Benchmark for Stand-alone and Member Servers v2.2.1
- CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0
- CIS Benchmark for IIS 5.0 and 6.0 for Microsoft Windows 2000, XP and Server 2003 v1.0
- The Australian Government Information and Communications Technology Security Manual for Windows
- US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista
- Windows Patch Assessment Check Library
- Security Essentials for Windows Server 2008 R2

**Note:** Along with the predefined standards, the regulatory standards for the Windows platform are also installed with the product.

### Predefined standards for NetWare

The predefined standards for the NetWare platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > NetWare

See “About predefined standards” on page 550.

The following predefined standards for the NetWare platform are installed with the product:
- Security Essentials for NetWare

### Predefined standards for Exchange

The predefined standards for the Exchange platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Exchange

See “About predefined standards” on page 550.
The following predefined standards for the Exchange platform are installed with the product:

- Security Essentials for Exchange 2007

**About sections**

You use a section to organize or to group related checks. A section can contain another section. Hence, a section can be a collection of checks and other sections.

For example, consider that you have one set of checks that relate to account passwords. Another set of checks concern the account lockout policy. You can create two separate sections for each set of checks and place these sections within another section for overall account handling.

See “About standards” on page 550.

See “About checks” on page 556.

See “About versioning scheme” on page 569.

See “Working with sections” on page 618.

**About checks**

A check is a test that is performed against one or more assets to determine a pass or a fail status.

A check is composed of one or more check expressions. Multiple check expressions can be joined through operators to form a check formula.

See “About standards” on page 550.

See “About sections” on page 556.

See “About versioning scheme” on page 569.

See “Working with checks” on page 624.

See “About operators” on page 590.

**About data collection jobs**

You create a data collection job to collect data from the assets for specific standards.

The information that you specify during the data collection process is saved in the data collection job. Hence you do not need to specify the collection criteria every time you perform the collection process. Data collection jobs can be scheduled to run at predefined intervals. The jobs can also be modified and deleted.
You can create or edit a data collection job through the **Create or Edit Data Collection Job** wizard.

You can create a collection job from the Standards view, Assets view, and the Job Management view. You can modify, delete, or track the status of a data collection job only from the Job Management view.

See “About advanced options for data collection” on page 557.

See “Setting up a data collection job from the Standards view” on page 609.

---

**About advanced options for data collection**

The Control Compliance Suite provides you with the ability to collect data only for the assets for which data was never collected in the previous job runs. When you specify a periodic schedule to run a data collection job after specific intervals, some assets may be down. Due to this, the data for those assets may not be collected during the specified periodic schedule.

The advanced options for data collection lets you specify a sub-schedule within the main schedule of the periodic data collection. You can specify the number of days after which the job must be repeated within the main schedule. The job is run after every specified interval until the specified day.

These options help you get the most updated data for all the available assets in the scope for the data collection job.

See “Setting up a data collection job from the Standards view” on page 609.

---

**About evaluation jobs**

You create an evaluation job to evaluate the assets in your organization against specific standards.

The information that you specify during the evaluation process is saved in the evaluation job. Hence, an evaluation job lets you perform the evaluation process repeatedly without having to specify the evaluation criteria again. Evaluation jobs can be scheduled to run at predefined intervals. You can modify and delete the evaluation jobs.

You can create or edit an evaluation job through the Create or Edit Evaluation Job wizard.

---

**Note:** Before you run an evaluation job, you must run a data collection job to obtain accurate evaluation results.
You can create an evaluation job from the Standards view, the Assets view, and the Job Management view. You can edit or delete an evaluation job only from the Job Management view.

See “Running an evaluation job from the Standards view” on page 607.

About target types

You use a target type to filter the assets during the data collection and the evaluation process. The target type filters the assets on the basis of the asset type. You specify the target type at the time of check creation. A check with a specific target type is applicable only on the specific asset type. For example, an asset of the type Windows Machine cannot be evaluated against a check of the UNIX target type.

The target type can be defined only at the check level. The target type for a standard lists the target type of the checks that are present within the standard. For example, consider a standard that contains two checks. The target type of one check is Windows 2000 Machines and the target type of the other check is Windows 2003 Machines. Then the list of target types for the concerned standard contains both Windows 2000 Machines and Windows 2003 Machines.

The target types that exist for the checks within the predefined standards are known as predefined target types.

Control Compliance Suite contains predefined target types for the following platforms:

- **SQL**
  See “About SQL predefined target types” on page 559.

- **Windows**
  See “About Windows predefined target types” on page 559.

- **UNIX**
  See “About UNIX predefined target types” on page 560.

- **Oracle**
  See “About Oracle predefined target types” on page 564.

- **Enterprise Security Manager**
  See “About ESM predefined target types” on page 565.

- **Exchange**
  See “About Exchange predefined target types” on page 566.

- **NDS**
  See “About NDS predefined target types” on page 568.
About SQL predefined target types

The SQL predefined target types are as follows:

Table 11-2 Supported SQL target types

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server 2005 Instances</td>
<td>All Microsoft SQL Server 2005 instances.</td>
</tr>
<tr>
<td>SQL Server 2000 Instances</td>
<td>All Microsoft SQL Server 2000 instances.</td>
</tr>
<tr>
<td>SQL Server 7 Instances</td>
<td>All Microsoft SQL Server 7 instances.</td>
</tr>
<tr>
<td>SQL Server Instances</td>
<td>All Microsoft SQL Server instances.</td>
</tr>
<tr>
<td>SQL Databases</td>
<td>All SQL databases.</td>
</tr>
<tr>
<td>SQL Server 2008 Instances</td>
<td>All Microsoft SQL Server 2008 instances.</td>
</tr>
</tbody>
</table>

See “About target types” on page 558.

About Windows predefined target types

The Windows predefined target types are listed as follows:

Table 11-3 Supported Windows predefined target types

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 or Later Member Servers</td>
<td>All Windows 2000 or later Server Machine Types (no domain controllers)</td>
</tr>
<tr>
<td>Windows 2000 Member Servers</td>
<td>All Windows 2000 Server Machine Types (no domain controllers)</td>
</tr>
<tr>
<td>All Windows Machines</td>
<td>All Windows computers</td>
</tr>
<tr>
<td>Windows 2000 Advanced Servers</td>
<td>Windows 2000 Advanced Server computers (no domain controllers)</td>
</tr>
<tr>
<td>Windows 2000 Machines</td>
<td>Windows 2000 computers only</td>
</tr>
<tr>
<td>Windows 2000 or Later Machines</td>
<td>All Windows 2000 or later computers.</td>
</tr>
<tr>
<td>Windows 2000 Professional Machines</td>
<td>Windows 2000 Professional computers</td>
</tr>
<tr>
<td>Target type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows 2003 Domain Controller Servers</td>
<td>Windows 2003 Domain Controller Server computers</td>
</tr>
<tr>
<td>Windows 2003 Machines</td>
<td>Windows 2003 computers only</td>
</tr>
<tr>
<td>Windows 2003 Member Servers</td>
<td>Windows 2003 Domain Member Server (no domain controllers)</td>
</tr>
<tr>
<td>Windows Vista Machines</td>
<td>Windows Vista computers only</td>
</tr>
<tr>
<td>Windows XP Professional Machines</td>
<td>Windows XP computers only</td>
</tr>
<tr>
<td>Windows 2000 Domain Controller Servers</td>
<td>All Windows 2000 Server Machine Types (Domain Controllers)</td>
</tr>
<tr>
<td>Windows 2008 R2 Machine</td>
<td>All Windows 2008 R2 computers</td>
</tr>
<tr>
<td>Windows server 2008 Machines</td>
<td>All Windows server 2008 computers</td>
</tr>
</tbody>
</table>

See “About target types” on page 558.

**About UNIX predefined target types**

The UNIX predefined target types are as follows:

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 5.1 and later Machines</td>
<td>All computers that are installed with version AIX 5.1 or later</td>
</tr>
<tr>
<td>AIX 5.1 Machines</td>
<td>All computers that are installed with AIX 5.1</td>
</tr>
<tr>
<td>AIX 5.2 Machines</td>
<td>All computers that are installed with AIX 5.2</td>
</tr>
<tr>
<td>AIX 5.3 Machines</td>
<td>All computers that are installed with AIX 5.3</td>
</tr>
<tr>
<td>AIX 6.1 Machines</td>
<td>All computers that are installed with AIX 6.1</td>
</tr>
<tr>
<td>All AIX Machines</td>
<td>All computers that are installed with AIX</td>
</tr>
<tr>
<td>All HP-UX Machines</td>
<td>All computers that are installed with HP-UX computers</td>
</tr>
<tr>
<td>All Redhat non Enterprise Linux Machines</td>
<td>All computers that are installed with RedHat Linux excluding the RedHat Enterprise Linux.</td>
</tr>
<tr>
<td>Target type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>All SuSE Linux Enterprise Server Machines</td>
<td>All computers that are installed with SuSE Linux Enterprise Server</td>
</tr>
<tr>
<td>All SuSE Linux Machines</td>
<td>All computers that are installed with SuSE Linux</td>
</tr>
<tr>
<td>Fedora Machines</td>
<td>All the Fedora computers.</td>
</tr>
<tr>
<td>HP-UX 11.00 and 11.23 Machines</td>
<td>All computers that are installed with HP-UX 11.00 or 11.23</td>
</tr>
<tr>
<td>HP-UX 11.00 and 11.11 Machines</td>
<td>All computers that are installed with HP-UX 11.00 or 11.11</td>
</tr>
<tr>
<td>HP-UX 11.00 Machines</td>
<td>All computers that are installed with HP-UX 11.00</td>
</tr>
<tr>
<td>HP-UX 11.00, 11.11 and 11.23 Machines</td>
<td>All computers that are installed with HP-UX 11.00, 11.11 or 11.23</td>
</tr>
<tr>
<td>HP-UX 11.11 and 11.23 Machines</td>
<td>All computers that are installed with HP-UX 11.11 or 11.23</td>
</tr>
<tr>
<td>HP-UX 11.11 Machines</td>
<td>All computers that are installed with HP-UX 11.11</td>
</tr>
<tr>
<td>HP-UX 11.23 Machines</td>
<td>All computers that are installed with HP-UX 11.23</td>
</tr>
<tr>
<td>HP-UX 11.x Machines</td>
<td>All computers that are installed with HP-UX 11.x</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 2.1 and 3.0 Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 2.1 or 3.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 2.1 and 4.0 Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 2.1 or 4.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 2.1 and Later Machines</td>
<td>All computers that are installed with Linux 2.1 or later</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 2.1 Machines</td>
<td>All computers that are installed with Linux 2.1</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 2.1, 3.0 and 4.0 Machines</td>
<td>All computers that are installed with 2.1, 3.0, or 4.0</td>
</tr>
<tr>
<td>Target type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3.0 and 4.0 Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 3.0 or 4.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3.0 and Later Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 3.0 or later</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3.0 Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 3.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 4.0 and Later Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 4.0 or Later</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 4.0 Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 4.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.0 and Later Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux 5.0 or Later</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.0</td>
<td>All computers that are installed with Red Hat Enterprise Linux 5.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Machines</td>
<td>All computers that are installed with Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>Redhat 7.0 Machines</td>
<td>All computers that are installed with RedHat 7.0</td>
</tr>
<tr>
<td>Redhat 7.1 Machines</td>
<td>All computers that are installed with RedHat 7.1</td>
</tr>
<tr>
<td>Redhat 7.2 Machines</td>
<td>All computers that are installed with Redhat 7.2</td>
</tr>
<tr>
<td>Redhat 7.3 Machines</td>
<td>All computers that are installed with Redhat 7.3</td>
</tr>
<tr>
<td>Redhat 8.0 Machines</td>
<td>All computers that are installed with Redhat 8.0</td>
</tr>
<tr>
<td>Solaris 10 Machines</td>
<td>All computers that are installed with Solaris 10</td>
</tr>
<tr>
<td>Solaris 2.6 and later Machines</td>
<td>All computers that are installed with Solaris 2.6 or later</td>
</tr>
<tr>
<td>Solaris 2.6, 7 and 8 Machines</td>
<td>All computers that are installed with Solaris 2.6, 7, or 8</td>
</tr>
<tr>
<td>Target type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Solaris 7 and earlier Machines</td>
<td>All computers that are installed with Solaris 7 or earlier</td>
</tr>
<tr>
<td>Solaris 7 and later Machines</td>
<td>All computers that are installed with Solaris 7 or later</td>
</tr>
<tr>
<td>Solaris 7 Machines</td>
<td>All computers that are installed with Solaris 7</td>
</tr>
<tr>
<td>Solaris 7,8 and 9</td>
<td>All computers that are installed with Solaris 7, 8, or 9</td>
</tr>
<tr>
<td>Solaris 7,8,9 and 10</td>
<td>All computers that are installed with Solaris 7, 8, 9, or 10</td>
</tr>
<tr>
<td>Solaris 7,8</td>
<td>All computers that are installed with Solaris 7 or 8</td>
</tr>
<tr>
<td>Solaris 8 and 9</td>
<td>All computers that are installed with Solaris 8 or 9</td>
</tr>
<tr>
<td>Solaris 8 and earlier Machines</td>
<td>All computers that are installed with Solaris 8 or earlier</td>
</tr>
<tr>
<td>Solaris 8 and later Machines</td>
<td>All computers that are installed with Solaris 8 or later</td>
</tr>
<tr>
<td>Solaris 8 Machines</td>
<td>All computers that are installed with Solaris 8</td>
</tr>
<tr>
<td>Solaris 8,9 and 10</td>
<td>All computers that are installed with Solaris 8, 9, or 10</td>
</tr>
<tr>
<td>Solaris 9 and 10</td>
<td>All computers that are installed with Solaris 9 or 10</td>
</tr>
<tr>
<td>Solaris 9 and later Machines</td>
<td>All computers that are installed with Solaris 9 or later</td>
</tr>
<tr>
<td>Solaris 9 Machines</td>
<td>All computers that are installed with Solaris 9</td>
</tr>
<tr>
<td>Solaris Servers</td>
<td>All computers that are installed with Solaris Servers</td>
</tr>
<tr>
<td>SuSE Linux 8.0, 8.1 and 8.2 Machines</td>
<td>All computers that are installed with SuSE Linux 8.0, 8.1, or 8.2</td>
</tr>
</tbody>
</table>
### Table 11-4  
**Supported UNIX target types (continued)**

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuSE Linux 9.0, 9.1, 9.2 and 9.3 Machines</td>
<td>All SuSE Linux 9.0, 9.1, 9.2 or 9.3 computers</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 10 Machines</td>
<td>All SuSE Linux Enterprise Server 10 computers</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 9 Machines</td>
<td>All SuSE Linux Enterprise Server 9 computers</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 8.1 and 10 Machines</td>
<td>All computers that are installed with SuSE Linux 8.1, or 10</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 8.1 and 9 Machines</td>
<td>All computers that are installed with SuSE Linux 8.1, or 9</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 8.1 Machines</td>
<td>All computers that are installed with SuSE Linux 8.1</td>
</tr>
<tr>
<td>SuSE Linux Enterprise Server 9 and 10 Machines</td>
<td>All computers that are installed with SuSE Linux 9 or 10</td>
</tr>
<tr>
<td>UNIX Machines - All UNIX Machines</td>
<td>All UNIX computers</td>
</tr>
<tr>
<td>VMware 3.0 and Later Machines</td>
<td>All computers that are installed with VMware 3.0 or later</td>
</tr>
<tr>
<td>VMware ESX Server 3.0 Machines</td>
<td>All computers that are installed with VMware ESX Server 3.0</td>
</tr>
<tr>
<td>VMware ESX Server 3.5 Machines</td>
<td>All computers that are installed with VMware ESX Servers 3.5</td>
</tr>
<tr>
<td>VMware ESX Server 3.x Machines</td>
<td>All computers that are installed with VMware ESX Server 3.x</td>
</tr>
<tr>
<td>All VMware ESX Machines</td>
<td>All computers that are installed with VMware ESX</td>
</tr>
</tbody>
</table>

See “About target types” on page 558.

### About Oracle predefined target types

The predefined target types for Oracle are listed as follows:
### Table 11-5  Supported Oracle target types

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 10g Databases</td>
<td>All Oracle 10g databases.</td>
</tr>
<tr>
<td>Oracle 8i Databases</td>
<td>All Oracle 8i databases.</td>
</tr>
<tr>
<td>Oracle 9i and 10g Databases</td>
<td>All Oracle 9i and 10g databases.</td>
</tr>
<tr>
<td>Oracle 9i Databases</td>
<td>All Oracle 9i databases.</td>
</tr>
<tr>
<td>Oracle 10g and 11g Databases</td>
<td>All Oracle 10g and 11g databases.</td>
</tr>
<tr>
<td>Oracle 11g Databases</td>
<td>All Oracle 11g Databases</td>
</tr>
<tr>
<td>Oracle 9i, 10g, and 11g Databases</td>
<td>All Oracle 9i, 10g, and 11g databases.</td>
</tr>
<tr>
<td>Oracle Databases</td>
<td>All Oracle databases.</td>
</tr>
<tr>
<td>Oracle Unix Databases</td>
<td>All Oracle databases on UNIX operating system.</td>
</tr>
<tr>
<td>Oracle Windows Databases</td>
<td>All Oracle databases on Windows operating system.</td>
</tr>
<tr>
<td>Oracle Windows Servers</td>
<td>All Oracle Servers with Windows operating system.</td>
</tr>
<tr>
<td>Oracle Servers</td>
<td>All Oracle Servers.</td>
</tr>
<tr>
<td>Oracle Unix Servers</td>
<td>All Oracle Servers with UNIX operating system.</td>
</tr>
</tbody>
</table>

See “About target types” on page 558.

### About ESM predefined target types

### Table 11-6  Supported ESM target types

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ESM Agent Machines</td>
<td>All ESM agents running on any operating system</td>
</tr>
<tr>
<td>All UNIX ESM Agent Machines</td>
<td>All ESM agents running on any UNIX operating system</td>
</tr>
<tr>
<td>Sun Solaris 10 ESM Agent Machines</td>
<td>All ESM agents running on Solaris 10 operating system</td>
</tr>
</tbody>
</table>
Table 11-6  
**Supported ESM target types (continued)**

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 ESM Agent Machines</td>
<td>All ESM agents running on Windows 2003 operating system</td>
</tr>
<tr>
<td>Windows XP ESM Agent Machines</td>
<td>All ESM agents running on Windows XP operating system</td>
</tr>
<tr>
<td>Windows Vista ESM Agent Machines</td>
<td>All ESM agents running on Windows Vista operating system</td>
</tr>
<tr>
<td>Windows 2008 ESM Agent Machines</td>
<td>All ESM agents running on Windows 2008 operating system</td>
</tr>
<tr>
<td>AS/400 ESM Agent Machines</td>
<td>All ESM agents running on AS/400 operating system</td>
</tr>
<tr>
<td>All Windows ESM Agent Machines</td>
<td>All ESM agents running on any Windows operating system</td>
</tr>
<tr>
<td>All Windows 2000 ESM Agent Machines</td>
<td>All ESM agents running on Windows 2000 operating system</td>
</tr>
<tr>
<td>OpenVMS ESM Agent Machines</td>
<td>All ESM agents running on OpenVMS operating system</td>
</tr>
</tbody>
</table>

**Note:** To create customized checks for ESM application modules, such as DB2 or SQL Server, you must use the underlying OS platform target type.

**About Exchange predefined target types**

The Exchange predefined target types are as follows:

Table 11-7  
**Supported Exchange target types**

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Server</td>
<td>All Exchange servers</td>
</tr>
<tr>
<td>Exchange Organization</td>
<td>The entire Exchange organization</td>
</tr>
<tr>
<td>Exchange Administrative Group</td>
<td>All administrative groups in the Exchange organization</td>
</tr>
<tr>
<td>Exchange 2000 Servers</td>
<td>All Exchange 2000 servers in the organization</td>
</tr>
</tbody>
</table>
Table 11-7  Supported Exchange target types (continued)

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2003 Servers</td>
<td>All Exchange 2003 servers in the organization</td>
</tr>
<tr>
<td>Exchange 2007 Servers</td>
<td>All Exchange 2007 servers in the organization</td>
</tr>
<tr>
<td>Exchange 2007 Hub Transport Servers</td>
<td>All Exchange 2007 Hub Transport Servers</td>
</tr>
</tbody>
</table>

See “About target types” on page 558.

About NetWare predefined target types

The NetWare predefined target types are listed as follows:

Table 11-8  Supported NetWare predefined target types

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetWare 5.1 Machines with NDS 7.x</td>
<td>All the computers that are installed with NetWare version 5.1 with NDS 7.x.</td>
</tr>
<tr>
<td>NetWare 5.1 Machines with NDS 8.x</td>
<td>All the computers that are installed with NetWare version 5.1 with NDS 8.x.</td>
</tr>
<tr>
<td>NetWare 5.1, 6.0, and 6.5 Machines</td>
<td>All the computers that are installed with NetWare version 5.1, 6.0, or 6.5.</td>
</tr>
<tr>
<td>NetWare 5.1 Machines</td>
<td>All the computers that are installed with NetWare version 5.1.</td>
</tr>
<tr>
<td>NetWare 6.0 and 6.5 Machines</td>
<td>All the computers that are installed with NetWare version 6.0 or 6.5.</td>
</tr>
<tr>
<td>NetWare 6.0 Machines</td>
<td>All the computers that are installed with NetWare version 6.0.</td>
</tr>
<tr>
<td>NetWare 6.5 Machines</td>
<td>All the computers that are installed with NetWare version 6.5.</td>
</tr>
</tbody>
</table>
Table 11-8  Supported NetWare predefined target types (continued)

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetWare 4.11 and 4.2 Machines</td>
<td>All the computers that are installed with NetWare version 4.11 and 4.2.</td>
</tr>
<tr>
<td>NetWare 4.11 and 4.2 Machines with NDS 6.x</td>
<td>All the computers that are installed with NetWare version 4.11 or 4.2 with NDS 6.x.</td>
</tr>
<tr>
<td>NetWare Machines with eDirectory 8.6.2</td>
<td>All the computers that are installed with NetWare eDirectory 8.6.2.</td>
</tr>
<tr>
<td>NetWare Machines with eDirectory 8.7.0</td>
<td>All the computers that are installed with NetWare eDirectory 8.7.0.</td>
</tr>
<tr>
<td>NetWare Machines with eDirectory 8.7.1</td>
<td>All the computers that are installed with NetWare eDirectory 8.7.1.</td>
</tr>
<tr>
<td>NetWare Machines with eDirectory 8.7.3</td>
<td>All the computers that are installed with NetWare eDirectory 8.7.3.</td>
</tr>
<tr>
<td>NetWare Machines with eDirectory 8.8</td>
<td>All the computers that are installed with NetWare eDirectory 8.8.</td>
</tr>
<tr>
<td>NetWare Machines with NDS 6.x</td>
<td>All the NetWare computers that are installed with NDS 6.x.</td>
</tr>
<tr>
<td>NetWare Machines with NDS 7.x</td>
<td>All the NetWare computers that are installed with NDS 7.x.</td>
</tr>
<tr>
<td>NetWare Machines with NDS 8.x</td>
<td>All the NetWare computers that are installed with NDS 8.x.</td>
</tr>
<tr>
<td>All NetWare Servers</td>
<td>All NetWare Servers.</td>
</tr>
</tbody>
</table>

About NDS predefined target types

The NDS predefined target types are listed as follows:

Table 11-9  Supported NDS target types

<table>
<thead>
<tr>
<th>Target type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All NDS Trees</td>
<td>All the NDS trees</td>
</tr>
</tbody>
</table>
About compliance score

The compliance score is a percentage value between 0 and 100 that represents the level of adherence to a standard. This score is derived from the checks that are present in a standard.

The checks in the Not Applicable status are not considered when you calculate the compliance score.

The compliance score is available when you evaluate an asset against one or more standard. The result of the evaluation process provides the compliance and the risk score.

See “Working with Evaluation Results” on page 653.

See “About risk score” on page 569.

About risk score

In Control Compliance Suite, a risk score is used to quantify the risk that is associated with an asset in your organization.

The risk score is calculated on the basis of the CIA values for an asset and the risk attributes of a check. You should give due consideration before you specify these values in the product.

You can specify the asset CIA values through the assets details pane or with the pre rules in the asset view.

See “Using a Pre rule to set the values of the common fields” on page 309.

You can specify the check risk attributes through the checks details pane or at the time of check creation.

See “Specifying or editing the check attributes” on page 651.

The risk calculations are based on the Common Vulnerabilities Scoring System version 2.

See “About risk score calculation” on page 657.

About versioning scheme

Each standard, section, and check follows a versioning scheme. The version consists of three numerical values that are separated by a period.

The components of the versioning scheme are explained as follows:
The first digit in the versioning scheme represents the major version. This value tells us the schema version of the specific check, section, or standard XML. The schema may need to be changed to support a new feature. In such cases, only the major version number changes.

The second digit in the versioning scheme represents the minor version. This version changes when a standard, section, or check is modified, for example, added, deleted, moved, or copied. But this version does not change if the standard, section, or check is modified for fixing a bug.

The third digit in the versioning scheme represents the fix version. This version changes when the standard, section, or check is modified with respect to its description, expression, the CIA values or any other property.

Following is the syntax for a version number:

(Major Version).(Minor Version).(Fix Version)

The change in version number is propagated to the top in the hierarchy. If a check is added to a section, the minor version of the parent section and the parent standard is incremented. If the version of a child section is incremented, then the respective version of the parent section is also incremented. This process helps in identifying precisely what has changed in a standard.

The following table lists the effect on the version number of actions such as creating, modifying, and deleting:

<table>
<thead>
<tr>
<th>Action</th>
<th>Effect on Version Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a check</td>
<td>The minor version of the parent section and the parent standard changes.</td>
</tr>
<tr>
<td>Modify a check</td>
<td>If a check is modified, then the fix version of the check, the parent section and the parent standard changes.</td>
</tr>
<tr>
<td>Delete a check</td>
<td>The minor version of the parent section and the parent standard changes.</td>
</tr>
<tr>
<td>Create a section</td>
<td>The minor version of the parent section (if any) and the parent standard changes.</td>
</tr>
<tr>
<td>Modify a section</td>
<td>If a section is modified, then the fix version of the section, the parent section, and the parent standard changes.</td>
</tr>
<tr>
<td>Delete a section</td>
<td>The minor version of the parent section (if any) and the parent standard changes.</td>
</tr>
</tbody>
</table>

See “About sections” on page 556.

See “About checks” on page 556.
About the standards filters

The Filter by pane in the Standards view contains the filters that you can use to display only the required standards.

The Control Compliance Suite provides the following default filters for filtering the standards, sections, and checks:

- **Target Platform**
  - Lets you filter the standards according to the specified target type.

- **Author**
  - Lets you filter the standards according to the specified author name.

- **Compliance Score**
  - Lets you filter the standards according to the specified range of compliance score.

- **Evaluated Between**
  - Lets you filter the standards according to the specified range of evaluation dates.
  - The last evaluation date is considered for filtering the standards.

- **Select tags**
  - Lets you filter the standards according to the specified tags.
  - You can browse to add the tags in the Tags list.
  - You can select either of the following options:
    - **Match Any.**
      - Select the Match Any option to display the standards that match any one of the listed tags.
    - **Match All.**
      - Select the Match All option to display the standards that match all the listed tags.

See “About the Filter by pane” on page 61.

See “Customizing the filter options” on page 67.

See “Using filters in the Filter by pane” on page 67.

About policy mapping in ESM

The check expressions in a standard are mapped with the policies in Enterprise Security Manager. When you execute a data collection job for a standard on ESM assets, the ESM data collector collects messages for the corresponding ESM policy.
from the ESM manager. Each check expression within a section of a CCS standard is mapped to an ESM policy.

If you create a custom standard, then you must change the name of the ESM policy that corresponds to the CCS standard.

See “About CCS ESM policy run configurations” on page 150.

About changing an ESM policy name

Every check in the CCS standard is linked to an ESM policy. You can rename an existing ESM policy name for some checks in an ESM standard from the CCS console. You can change the ESM policy name for a whole standard, a section, or a check level.

Note: You cannot rename the pre-defined ESM policies.

See “Changing an ESM policy name at the standard level” on page 618.

See “Changing an ESM policy name at the section level” on page 623.

See “Changing an ESM policy name at the check level” on page 637.

List of standards

Following is the List of standards for the Control Compliance Suite 10.0 version:

Table 11-10  List of standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS Legacy Settings Benchmark for Windows XP Professional v2.01</td>
<td>The CIS Legacy Settings Benchmark for Windows XP Professional v1.3.0 contains a set of baseline configuration parameters for Microsoft Windows XP Professional systems.</td>
</tr>
</tbody>
</table>
Table 11-10  List of standards (continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS Oracle 9i and 10g Database Security Benchmark v2.0</td>
<td>The CIS Oracle 9i and 10g Database Security Benchmark v2.0 contains a set of baseline configuration parameters for Oracle 9i and 10g. Policies and Checks covered in this technical standard are specific to CIS L1 benchmark and are applicable to UNIX platforms only.</td>
</tr>
<tr>
<td>CIS Security Benchmark for HP-UX v1.3.1</td>
<td>The CIS Security Benchmark for HP-UX v1.3.1 contains checks for a set of baseline configuration parameters recommended by Center for Internet Security (CIS) benchmark version 1.3.1 for HP-UX 11.i.</td>
</tr>
<tr>
<td>CIS Solaris 10 Benchmark v4.0</td>
<td>The CIS Solaris 10 Benchmark v4.0 contains checks for a set of baseline configuration parameters recommended by Center for Internet Security (CIS) benchmark version 4.0 for Solaris 10 release.</td>
</tr>
<tr>
<td>CIS VMware ESX Server 3.x Benchmark v1.0</td>
<td>The CIS VMware ESX Server 3.x Benchmark v1.0 contains checks for a set of baseline configuration parameters recommended by Center for Internet Security (CIS) benchmark version 1.0 for VMware ESX Server 3.x.</td>
</tr>
<tr>
<td>CIS Windows 2000 Server Operating System Level Two Benchmark for Stand-alone and Member Servers v2.2.1</td>
<td>The CIS Windows 2000 Server Operating System Level Two Benchmark for Stand-alone and Member Servers v2.2.1 contains a set of baseline configuration parameters for Windows 2000 Server systems.</td>
</tr>
<tr>
<td>CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0</td>
<td>The CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0 contains a set of baseline configuration parameters for Microsoft Windows Server 2003 systems.</td>
</tr>
<tr>
<td>Security Essentials for AIX 5.x and 6.1</td>
<td>The Security Essentials for AIX 5.x and 6.1 contains checks for a set of baseline configuration parameters recommended for AIX 5.x and 6.1.</td>
</tr>
<tr>
<td>Standard</td>
<td>Overview</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CIS Security Configuration Benchmark for</td>
<td>The CIS Security Configuration Benchmark for Microsoft SQL Server 2005 v1.1.1 document is derived from research conducted utilizing the SQL Server 2005 environment on Windows XP Desktops and Windows 2003 servers. This document provides the necessary settings and procedures for the secure installation, setup, configuration, and operation of an MS SQL Server 2005 system. With the use of the settings and procedures in this document, an SQL Server 2005 database may be secured from conventional “out of the box” threats. Recognizing the nature of security cannot and should not be limited to only the application; the scope of this document is not limited to only SQL Server 2005 specific settings or configurations, but also addresses backups, archive logs, “best practices” processes and procedures that are applicable to general software and hardware security. The Level column indicates the following: - Level 1 settings are generally considered “safe” to apply to most systems. The use of these configuration recommendations is not likely to have a negative impact on performance or functionality unless otherwise noted in the Comments. - Level 2 settings provide a higher level of security, but will result in a negative impact to performance and functionality. It is extremely important to conduct testing of security configurations on non-production systems prior to implementing them on production systems.</td>
</tr>
<tr>
<td>Standard</td>
<td>Overview</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NetWare 2008</td>
<td>The Security Essentials for NetWare provides guidelines for securing the installation and configuration of Novell NetWare systems.</td>
</tr>
<tr>
<td>Security Essentials for Red Hat Enterprise</td>
<td>The Security Essentials for Red Hat Enterprise Linux 5.0 provides guidelines for securing Red Hat Enterprise Linux systems including RHEL 2.1, 3.0, 4.0, and 5.0</td>
</tr>
<tr>
<td>Linux 5.0</td>
<td></td>
</tr>
<tr>
<td>Enterprise Server</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>R2</td>
<td></td>
</tr>
<tr>
<td>Communications Technology Security Manual for</td>
<td></td>
</tr>
<tr>
<td>MS-SQL Server</td>
<td></td>
</tr>
<tr>
<td>The Australian Government Information and</td>
<td></td>
</tr>
<tr>
<td>Communications Technology Security Manual for</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td>The Australian Government Information and</td>
<td></td>
</tr>
<tr>
<td>Communications Technology Security Manual for</td>
<td></td>
</tr>
</tbody>
</table>
Table 11-10  List of standards (continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Patch Assessment Check Library</td>
<td>The Windows Patch Assessment Check Library is a collection of checks that evaluate service pack and patch compliance for Microsoft and other platforms and products. This check library is derived from the same source data used by bv-Control for Windows Patch assessment component and should be updated concurrently.</td>
</tr>
<tr>
<td>Change Notifications for UNIX</td>
<td>The Change Notifications standard is based on Change Notification category of messages in Enterprise Security Manager.</td>
</tr>
<tr>
<td>Change Notifications for Windows</td>
<td>The Change Notifications standard is based on Change Notification category of messages in Enterprise Security Manager.</td>
</tr>
</tbody>
</table>
The Center for Internet Security (CIS) publishes a configuration benchmark for Windows Server 2003 domain controller servers that defines Consensus Baseline Security Settings for various operating system components. CIS considers these recommended configurations safe for administrators of any security skill level to implement.

The CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller systems that consists of four major categories:

- Additional Security Protection
- Auditing and Account Policies
- Microsoft Service Packs and Security Updates
- Security Settings

To harden Windows Server 2003 security for domain controller servers, networks should at a minimum comply with the recommendations published by CIS.

### Table 11-10 List of standards (continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Overview</th>
</tr>
</thead>
</table>
| CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controllers v2.0 | The Center for Internet Security (CIS) publishes a configuration benchmark for Windows Server 2003 domain controller servers that defines Consensus Baseline Security Settings for various operating system components. CIS considers these recommended configurations safe for administrators of any security skill level to implement. The CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller systems that consists of four major categories:
- Additional Security Protection
- Auditing and Account Policies
- Microsoft Service Packs and Security Updates
- Security Settings
To harden Windows Server 2003 security for domain controller servers, networks should at a minimum comply with the recommendations published by CIS. |
CIS has published Solaris Benchmark v4.0 (for Solaris 10 release) that provides consensus baseline security settings for Solaris systems. Technical Standard - Security Essential for Solaris 10 evaluates systems against Security Essential for Solaris 10 and provides compliance status and the hardening recommendations to improve security of Solaris systems. The standard contains nine major sections and associated sub sections as mentioned in benchmark. Sections contain checks for security settings and recommendations. Recommendations are intended to provide helpful information to organizations attempting to improve the security of their networks, systems, and devices.

Before applying recommendations you are advised to check relevant vendor documentations to avoid discrepancies.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Overview</th>
</tr>
</thead>
</table>
| CIS Security Benchmark for Sun Solaris 10 v4.0 | CIS has published Solaris Benchmark v4.0 (for Solaris 10 release) that provides consensus baseline security settings for Solaris systems. Technical Standard - Security Essential for Solaris 10 evaluates systems against Security Essential for Solaris 10 and provides compliance status and the hardening recommendations to improve security of Solaris systems. The standard contains nine major sections and associated sub sections as mentioned in benchmark. Sections contain checks for security settings and recommendations. Recommendations are intended to provide helpful information to organizations attempting to improve the security of their networks, systems, and devices.

Before applying recommendations you are advised to check relevant vendor documentations to avoid discrepancies. |
Table 11-10  List of standards (continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Overview</th>
</tr>
</thead>
</table>
| CIS Windows Server 2003 Legacy Security Settings for Domain Member Server v2.0 | The Center for Internet Security (CIS) publishes a configuration benchmark for Windows Server 2003 domain member servers that defines Consensus Baseline Security Settings for various operating system components. CIS considers these recommended configurations safe for administrators of any security skill level to implement. The CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0 includes legacy recommendations for Windows Server 2003 systems that consists of four major categories:  
  ■ Additional Security Protection  
  ■ Auditing and Account Policies  
  ■ Microsoft Service Packs and Security Updates  
  ■ Security Settings  
  To harden Windows Server 2003 security for domain member servers, networks should at a minimum comply with the legacy recommendations published by CIS. |

Concepts in checks

Before you begin to perform the checks-related operations, you should familiarize yourself with the following concepts in checks:

■ Field expression  
  See “Field expression” on page 580.

■ Check expression  
  See “Check expression” on page 581.

■ Preconditions  
  See “Preconditions” on page 582.

■ Check formula  
  See “Check formula” on page 581.
Field expression

In a field expression, an operator is used to compare a field with a particular value that a user specifies.

A field expression is composed of the following:

- **Field**
  Name of the field whose value you want to compare.

- **Value**
  The value against which you want to compare a specified field. This value is also known as a field value.

- **Operator**
  The operator specifies the action that must be performed. For example, if you want to obtain a field A that has the exact value of 100, you must use the equal (=) operator. Every field value has a defined set of operators. You can only select an operator from the range of operators that are defined for the selected field value.
  See “Field expression operators” on page 591.

The syntax for a field expression is as follows:

<Field><Operator><Value>

The following table lists some examples of a field expression:

<table>
<thead>
<tr>
<th>Field</th>
<th>Operator</th>
<th>Value</th>
<th>Field expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>=</td>
<td>SOUTH REGION</td>
<td>Domain Name=SOUTH REGION</td>
</tr>
<tr>
<td>Auditing</td>
<td>!=</td>
<td>Yes</td>
<td>Auditing Enabled!=Yes</td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See “About checks” on page 556.
See “Concepts in checks” on page 579.
See “Check expression” on page 581.
See “Creating a new check” on page 633.
See “Check Advanced Settings” on page 587.

Check expression

A check expression compares a property of an asset against a data value that a user specifies. The result of the comparison is a pass, a fail, or an unknown value.

A check expression is composed of the following:

- **Field expression (mandatory)**
  See “Field expression” on page 580.

- **Data Items filter (optional)**
  See “Data Items filter” on page 582.

See “About checks” on page 556.
See “Concepts in checks” on page 579.
See “Creating a new check” on page 633.

Check formula

A check formula is created by using check expressions.

A check formula is composed of either of the following:

- **A single check expression**
  See “Check expression” on page 581.

- **Multiple check expressions that are connected by the use of check formula operators.**
  See “Check formula operators” on page 593.

When a check formula is composed of only one check expression, then the check formula and the check expression are the same. Hence, their outcome is the same.

See “About checks” on page 556.
See “Concepts in checks” on page 579.
See “Check Advanced Settings” on page 587.
See “Creating a new check” on page 633.
Preconditions

A precondition is a logical condition that must be met before a check can be evaluated against the target asset.

In Control Compliance Suite, a check consists of a precondition and the actual check formula. If the check has a precondition, then the precondition is evaluated before the execution of check formula. If the precondition is not met then the check formula is not evaluated and the check outcome is set to Not Applicable.

The common use of a precondition is to verify some condition on the target asset before the assessment of the asset for compliance.

For example, consider the check: Is directory 'XYZ' owned by 'PQR' and has group set to 'ABC'? You may want to first verify if the specified directory 'XYZ' exists on the target computer before checking for the ownership. In this case, the precondition would be a verification of the fact whether the directory 'XYZ' exists.

See “About checks” on page 556.

See “Concepts in checks” on page 579.

See “Creating a new check” on page 633.

Data Items filter

A data items filter lets you filter the data against which the field expression is evaluated in a check.

A data items filter is composed of one or more filter statements. Each filter statement is a field expression.

See “Field expression” on page 580.

You can specify a data items filter in the Advanced Settings dialog box when you create or edit a check.

See “Check Advanced Settings” on page 587.

If you specify multiple filter statements, then the final data for evaluation is determined by the following options:

- Return only the data that matches all of the filter statements.
  The AND operator is applied on the result of each filter statement to determine the final data for evaluation purpose.

- Return only the data that matches any one of the filter statements.
  The OR operator is applied on the result of each data item to determine the final data for evaluation purpose.

See “About checks” on page 556.
Missing data items

Data items are termed as 'missing' in the following situations:
- No value for the field is present.
- Application of an evaluation condition filter returns no data values.

You must specify the outcome for missing data in the evaluation results. You can set this value when you create a check in the Advanced Settings dialog box of the Create Check wizard. You can also modify the Missing Data Outcome value after the check is created.

You can set the following values as the outcome for missing data items:
- Pass
- Fail
- Unknown

The default value for a missing data outcome is Unknown.

Multiple data items

An evaluation condition consists of a field expression. When you specify an evaluation condition, all data items of the specified field are matched against the condition.

The result of each tested data item is one of the following:
- Pass
- Fail
- Unknown

To calculate the final result for all the tested data items, you must specify the action to take for multiple data items. You can specify this action in the Advanced Settings dialog box of the Create Check wizard.

See “Concepts in checks” on page 579.
See “Creating a new check” on page 633.
In the Advanced Settings dialog box, you can select either of the following options to specify the action for multiple data items:

- All must meet the evaluation condition
  The AND operator is applied on the individual results of each data item.

- At least one must meet the evaluation condition
  The OR operator is applied on the individual results of each data item.

See “Operators AND and OR” on page 593.
See “About checks” on page 556.
See “Concepts in checks” on page 579.
See “Creating a new check” on page 633.

Check risk attributes

The attributes of a check that are used to calculate the risk are known as the risk attributes.

A check has the following risk attributes:

- Confidentiality Impact
  This attribute measures the impact to confidentiality if a specified check fails. Confidentiality is the act of limiting the access and disclosure of information to only authorized users. The impact of unauthorized disclosure of confidential information can lead to security risk, loss of public confidence, or legal action against the organization.
  You can assign the following values to this attribute:

  - NoImpact
    No impact to the confidentiality of the system.
    The corresponding weight that is assigned to this value is 0.0.

  - Partial
    Considerable information disclosure has occurred. Access to some system files is possible but the attacker does not have control over the data that is obtained. The scope of the loss is constrained.
    The corresponding weight that is assigned to this value is 0.275.

  - Complete
    Total information disclosure has occurred. All the system files are revealed. The attacker has access to all the system data.
    The corresponding weight that is assigned to this value is 0.66.
Integrity Impact
This attribute measures the impact to integrity if a specified check fails. Integrity refers to the genuineness of the information. Integrity dictates that information must be protected from improper modification. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. Continuous use of corrupted data can result in inaccuracy, fraud, or erroneous decisions.
You can assign the following values to this attribute:

- **No Impact**
  - No impact to the integrity of the system.
  - The corresponding weight that is assigned to this value is 0.0.

- **Partial**
  - Modification of some information has occurred but the attacker does not have control over what can be modified. Modification scope is limited.
  - The corresponding weight that is assigned to this value is 0.275.

- **Complete**
  - Total compromise of system integrity has occurred. The attacker is able to modify any files on the target system.
  - The corresponding weight that is assigned to this value is 0.66.

Availability Impact
This attribute measures the impact to availability if a specified check fails. Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space affect the availability of a system. If a mission-critical asset is unavailable to its end users, the mission of the organization may be affected.
You can assign the following values to this attribute:

- **No Impact**
  - No impact to the availability of the system.
  - The corresponding weight that is assigned to this value is 0.0.

- **Partial**
  - Reduced performance or interruptions in availability of information.
  - The corresponding weight that is assigned to this value is 0.275.
Total shut down of the affected resource. The attacker can render the resource completely unavailable.

The corresponding weight that is assigned to this value is 0.66.

Access Vector
This attribute reflects how vulnerability is exploited in a system.
According to the type of access that is required for the attacker to exploit the vulnerability, this attribute can be assigned the following values:

- **Local Accessible**
  The attacker has either physical access to the vulnerable system or a local (shell) account.
  The corresponding weight that is assigned to this value is 0.395.

- **Adjacent Network Accessible**
  The attacker has access to either the broadcast or the collision domain of the vulnerable software.
  The corresponding weight that is assigned to this value is 0.646.

- **Network Accessible**
  The vulnerable software is bound to the network stack and the attacker does not require local network access or local access.
  The corresponding weight that is assigned to this value is 1.0.

Access Complexity
This attribute measures the complexity of the attack that is required to exploit the vulnerability in a system.
The possible values for this attribute are as follows:

- **Low**
  Specialized access conditions do not exist.
  The corresponding weight that is assigned to this value is 0.71

- **Medium**
  The access conditions are specialized to a limited degree.
  The corresponding weight that is assigned to this value is 0.61.
High
Specialized access conditions exist.
The corresponding weight that is assigned to this value is 0.35.

- **Authentication**
  This attribute measures the number of times an attacker must authenticate to a target for exploiting the vulnerability. This attribute does not measure the strength or complexity of the authentication process. Authentication gauges only the fact whether an attacker is required to provide credentials before the exploration of the vulnerability.
  The possible values for this attribute are as follows:

  - **Multiple Instances**
    The attacker is required to authenticate two or more times to exploit the vulnerability. The same credentials may be used each time.
    The corresponding weight that is assigned to this value is 0.45

  - **Single Instance**
    The attacker needs to log into the system such as at a command line or through a desktop session or Web interface.
    The corresponding weight that is assigned to this value is 0.56.

  - **No Authentication**
    Authentication is not required to exploit the vulnerability.
    The corresponding weight that is assigned to this value is 0.704

See “About checks” on page 556.
See “About risk score calculation” on page 657.

**Check Advanced Settings**

The check fundamentals such as evaluation condition, data items filters, and multiple data items are important concepts to understand the process of creating a check. You can set these values in the Advanced Settings dialog box when you create a check.

For example, assume a table exists in the database with the name EXAMPLE. You can treat this table equivalent to a category in an evaluation condition.

Table 11-12 contains the following fields and values:
CASE I: The following evaluation condition is set and no filter is applied on the evaluation condition:

<table>
<thead>
<tr>
<th>Evaluation Condition</th>
<th>Equivalent field expression for the evaluation condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A &gt; 9</td>
<td>A &gt; 9</td>
</tr>
</tbody>
</table>

For the field A, three data values (9, 10, and 11) are present in the table. Each data value is tested against the specified evaluation condition and the following results are obtained:

- A = 9 Result = FAIL
- A = 10 Result = PASS
- A = 11 Result = PASS

To calculate the final result for the tested data, you must specify the action that should be taken for multiple data items.

You can select either of the following options to specify the action for multiple data items:

- All must meet the evaluation condition.
  - The AND operator is applied on the individual results of each data item.
- At least one must meet the evaluation condition.
  - The OR operator is applied on the individual results of each data item.

If the AND operator is applied for the sample check, then the final result is as follows:
Final test result: FAIL (Applying the All must meet the evaluation condition option)

CASE II: The same evaluation condition is set and a data items filter that consists of a single filter statement is applied:

Evaluation Condition: In the table EXAMPLE, the value of the field A should be greater than 9.

Equivalent field expression for the evaluation condition: A > 9

Evaluation condition filter: D > 50

On applying the filter statement, only those values of the field A are tested that match the filter statement. In the example, now only the values 10 and 11 are checked against the evaluation condition.

The individual results for the tested data values are as follows:

A = 10  Result = PASS
A = 11  Result = PASS

If you now specify the action for multiple data items as "All must meet the evaluation condition", then the final result is as follows:

Final test result: PASS (PASS AND PASS) (Applying the All must meet the evaluation condition option)

CASE III: The same evaluation condition is set and two filter statements are specified in the data items filter as follows:

Evaluation Condition: In the table EXAMPLE, the value of the field A should be greater than 9.

Equivalent field expression for the evaluation condition: A > 9

Filter statement 1: D > 50

Filter statement 2: C = P

Managing standards | Concepts in checks | 589
In the CASE III, the following values are returned on applying each filter statement:

- **D > 50**
  - The following values are returned:
    - A = 10
    - A = 11

- **C = P**
  - The following values are returned:
    - A = 9

When you apply more than one filter statement on the evaluation condition, you must specify the behavior for multiple filter statements. This behavior is used to determine the data items that would be considered for evaluation purpose.

You can select either of the following options to specify the behavior for multiple filter statements:

- Return only the data that matches all of the filter statements.
  - The AND operator is applied on each data item.

- Return only the data that matches any one of the filter statements.
  - The OR operator is applied on each data item.

If you consider only the data items that match any one of the filter statements, then the final data values are obtained as follows:

Applying OR operator as follows:

\[(A = 10) \lor (A = 11) \lor (A = 9)\]

- All the three data values are available for testing.
- A=9
- A=10
- A=11

You can then proceed to test each data item against the evaluation condition.

See “About checks” on page 556.

See “Concepts in checks” on page 579.

See “Creating a new check” on page 633.

### About operators

An operator is used to indicate an action that is performed on one or more elements. An operator can be a symbol or a word that signifies a particular action.

In the Standards module, the following operators are used:

- Field expression operators
See “Field expression operators” on page 591.

■ Check formula operators
See “Check formula operators” on page 593.

**Field expression operators**

The operators that are allowed in a field expression are known as the field expression operators. These operators are used to make a comparison between two given values.

**Table 11-13** lists the descriptions of the available field expression operators.

**Table 11-13  ** Field expression operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Operator Name</th>
<th>Expression using sample values A, B, and the operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>The equality operator</td>
<td>A = B</td>
<td>A must be equal to B</td>
</tr>
<tr>
<td>!= or &lt;&gt;</td>
<td>The inequality operator</td>
<td>A!=B</td>
<td>A must not be equal to B</td>
</tr>
<tr>
<td>&lt;</td>
<td>The less than operator</td>
<td>A &lt; B</td>
<td>A must be less than B</td>
</tr>
<tr>
<td>&lt;=</td>
<td>The less than or equal operator</td>
<td>A &lt;= B</td>
<td>A must be less than or equal to B</td>
</tr>
<tr>
<td>&gt;</td>
<td>The greater than operator</td>
<td>A &gt; B</td>
<td>A must be greater than B</td>
</tr>
<tr>
<td>&gt;=</td>
<td>The greater than or equal operator</td>
<td>A &gt;= B</td>
<td>A must be greater than or equal to B</td>
</tr>
<tr>
<td>Like</td>
<td>The like operator</td>
<td>A Like B</td>
<td>The SQL like operator (same syntax and semantics).</td>
</tr>
<tr>
<td>Not Like</td>
<td>The not like operator</td>
<td>A Not Like B</td>
<td>The SQL not like operator. Note the space between not and like. Any amount of white space (blanks, tabs, new lines, or carriage returns) is allowed here. The white space is not strictly required, but it is best not to omit it.</td>
</tr>
<tr>
<td>=~</td>
<td>The match operator</td>
<td>A=-B</td>
<td>The regular expression matching operator.</td>
</tr>
<tr>
<td>Operator</td>
<td>Operator Name</td>
<td>Expression using sample values A, B, and the operator</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------</td>
<td>-------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>!-</td>
<td>The no match operator.</td>
<td>A!-B</td>
<td>The negative of the expression matching operator.</td>
</tr>
<tr>
<td>is null</td>
<td>The is null operator</td>
<td>A is null</td>
<td>The SQL is null operator. A field expression employing this operator must not have a value specified. At least one white-space character is required between is and null.</td>
</tr>
<tr>
<td>is not null</td>
<td>The is not null operator</td>
<td>A is not null</td>
<td>The negative of is null. The white space between not and null is not strictly required, but it is best not to omit it.</td>
</tr>
<tr>
<td>Exact</td>
<td>The exact operator</td>
<td></td>
<td>Forces case-sensitive string comparison.</td>
</tr>
<tr>
<td>Inexact</td>
<td>The inexact operator</td>
<td></td>
<td>Forces case-insensitive string comparison.</td>
</tr>
<tr>
<td>%</td>
<td>Contains operator</td>
<td>A%B</td>
<td>In case of a single valued field, value on RHS has to be partially or completely matching with LHS. In case of a multi valued field, every value on RHS has to be present on the LHS.</td>
</tr>
<tr>
<td>!%</td>
<td>The Not Contains operator</td>
<td>A!%B</td>
<td>The negative of the Contains operator.</td>
</tr>
<tr>
<td>%~</td>
<td>The Contains Match operator</td>
<td>A%~B</td>
<td>In case of a single valued field, the regular expression on RHS should match field value on LHS. In case of a multi valued field, every regular expression on RHS should match at least one element on LHS.</td>
</tr>
<tr>
<td>!%~</td>
<td>The Not Contains Match operator</td>
<td>A!%~B</td>
<td>The negative of the Contains Match operator.</td>
</tr>
</tbody>
</table>
See “About operators” on page 590.

Check formula operators

The operators that are allowed to be used in a check formula are known as the check formula operators.

The check formula operators are as follows:

- AND
- OR
- NOT
- IF
- THEN
- ELSE

See “Operators AND and OR” on page 593.

See “Operator NOT” on page 594.

See “Operators IF, THEN, ELSE” on page 594.

When you create a check, you can specify the operators in the Create Expression(s) panel of the Create Check wizard. By default, the AND operator is used to connect two or more expressions. You can specify the operators in the Formula box by either typing or selecting the displayed operators.

See “About operators” on page 590.

See “Concepts in checks” on page 579.

Operators AND and OR

The AND and OR operators are used to connect two or more check expressions in a check formula.

Table 11-14 defines the outcome of the check formula when AND and OR operators are used to define logical combinations of check expressions. In the table, A and B represent check expressions.

<table>
<thead>
<tr>
<th>If A equals</th>
<th>If B equals</th>
<th>Then A AND B equals</th>
<th>Then A OR B equals</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASS</td>
<td>PASS</td>
<td>PASS</td>
<td>PASS</td>
</tr>
<tr>
<td>PASS</td>
<td>FAIL</td>
<td>FAIL</td>
<td>PASS</td>
</tr>
</tbody>
</table>
Table 11-14  Use of AND and OR operators (continued)

<table>
<thead>
<tr>
<th>If A equals</th>
<th>If B equals</th>
<th>Then A AND B equals</th>
<th>Then A OR B equals</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASS</td>
<td>MANUAL REVIEW</td>
<td>MANUAL REVIEW</td>
<td>PASS</td>
</tr>
<tr>
<td>FAIL</td>
<td>PASS</td>
<td>FAIL</td>
<td>PASS</td>
</tr>
<tr>
<td>FAIL</td>
<td>FAIL</td>
<td>FAIL</td>
<td>FAIL</td>
</tr>
<tr>
<td>FAIL</td>
<td>MANUAL REVIEW</td>
<td>FAIL</td>
<td>MANUAL REVIEW</td>
</tr>
<tr>
<td>MANUAL REVIEW</td>
<td>PASS</td>
<td>MANUAL REVIEW</td>
<td>MANUAL REVIEW</td>
</tr>
<tr>
<td>MANUAL REVIEW</td>
<td>FAIL</td>
<td>FAIL</td>
<td>MANUAL REVIEW</td>
</tr>
<tr>
<td>MANUAL REVIEW</td>
<td>MANUAL REVIEW</td>
<td>MANUAL REVIEW</td>
<td>MANUAL REVIEW</td>
</tr>
</tbody>
</table>

See “Check formula operators” on page 593.
See “About operators” on page 590.

Operator NOT

The NOT operator can be used in a check formula.

Table 11-15 defines the outcome of the check formula when the NOT operator is used to define logical combinations of check expressions. In the table, A represents a check expression.

Table 11-15  Usage of NOT operator

<table>
<thead>
<tr>
<th>If A equals</th>
<th>Then NOT A equals</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASS</td>
<td>FAIL</td>
</tr>
<tr>
<td>FAIL</td>
<td>PASS</td>
</tr>
<tr>
<td>MANUAL REVIEW</td>
<td>MANUAL REVIEW</td>
</tr>
</tbody>
</table>

See “Check formula operators” on page 593.
See “About operators” on page 590.

Operators IF, THEN, ELSE

An IF, THEN, ELSE operator is defined as follows:
If (condition)
Then (true expression)
Else (false expression)

The value is obtained in the following way when you use this operator:
- The value is unknown if the condition evaluates to unknown.
- The value is true if the condition evaluates to true.
- The value is false if the condition evaluates to false.

See “Check formula operators” on page 593.
See “About operators” on page 590.

About the Standards view

The Standards view lets you manage the standards, sections, and checks in the Control Compliance Suite.

You can access the standards management view from Manage > Standards.

The Standards view contains the following panes:

Tree pane
The tree pane appears on the left side of the console window under the navigation bar.

The pane displays a hierarchical, folder-based structure of the standards that are stored in the CCS directory.

**Note:** The tree pane displays the custom standards, as well as the predefined standards for the supported platforms. The regulatory standards are also displayed for the Windows and the UNIX platform.

Filter by pane
The Filter by pane appears in the lower left side of the console window under the tree pane.

You can specify filters in this pane so that only the required standards, sections, and checks are displayed in the table pane.

You can use the following filters in the standards view:
- Target Platform
- Author
- Compliance Score
- Evaluated Between
- Select Tags
Table pane

The table pane appears in the right side of the console window under the taskbar.

This pane displays the standards, sections, and checks. **Note:** The simple and the complex checks in the Table pane are tagged differently. You can differentiate between the simple and complex checks visually by the icon. The icon that indicates the complex checks has a red mark on the upper left corner.

Details pane

The details pane appears in the lower-right side of the console window under the table pane.

This pane displays the details of the standard, section, or check that is selected in the details pane.

The taskbar of the Standards view is divided into the following major tasks:

**Standard Tasks**

- Create Standard
  See “Creating a new standard” on page 603.
- Import Standard
  See “Importing a standard” on page 605.
- Export Standard
  See “Exporting a standard” on page 605.
- Create Check
  See “Creating a new check” on page 633.
- Create Section
  See “Creating a new section” on page 621.

**Evaluation Tasks**

**ESM Tasks**

Change ESM Policy Name

See “Changing an ESM policy name at the standard level” on page 618.
Common Tasks

- Move
  See “Moving a standard” on page 604.
  See “Moving a section” on page 622.
  See “Moving a check” on page 632.

- Delete
  See “Deleting a standard” on page 606.
  See “Deleting a section” on page 623.
  See “Deleting a check” on page 633.

- Request Exception
  See “Requesting an exception” on page 538.
  See “Launching the Request Exception Wizard” on page 541.

See “About the standards filters” on page 571.
See “Working with standards” on page 598.
See “Working with sections” on page 618.
See “Working with checks” on page 624.
See “Viewing standard information in the details pane” on page 598.

About the standard migration utility for ESM and CCS

Symantec has developed independent utilities to migrate the following to CCS 9.0.1 or later format:

- Customized ESM policies
- Customized CCS 8.60 standards

Both the utilities use command-line functionality to migrate the policies or standards. Once you migrate the policies or standards to CCS 9.0.1 or later format, you can import them into CCS 9.0.1 or later.

For more information on how to use the utilities, see the guide available with the utility.

For 9.0.1 or later release, the web package of the utilities is available along with the web package of CCS 9.0.1 or later. The web package of CCS 9.0.1 or later is available on the Platinum site.

To gain access to the latest utilities, contact Technical Support for assistance.
Working with standards

You can perform the following tasks on standards:

■ View standard information in the details pane
   See “Viewing standard information in the details pane” on page 598.

■ Create a new standard.
   See “Creating a new standard” on page 603.

■ Copy and paste a standard.
   See “Copying and pasting a standard” on page 603.

■ Move a standard.
   See “Moving a standard” on page 604.

■ Import a standard.
   See “Importing a standard” on page 605.

■ Export a standard.
   See “Exporting a standard” on page 605.

■ Rename a standard.
   See “Renaming a standard” on page 606.

■ Delete a standard.
   See “Deleting a standard” on page 606.

■ Evaluate an asset against a standard.
   See “Running an evaluation job from the Standards view” on page 607.

■ Create a chained job
   See “Running a collection-evaluation-reporting job from the Standards view” on page 612.

Viewing standard information in the details pane

You can view the information about a standard through the details pane in the standards view.

To view the standards information

1. Go to Manage > Standards.
2. In the table pane of the Standards view, select the standard for which you want to display the information.
3. View the information for the selected standard in the details pane.

   The standards details are contained in the following tabs:
- General
  See “Standard details pane - General tab” on page 599.

- Description
  See “Standard details pane - Description tab” on page 600.

- Evaluations
  See “Standard details pane - Evaluations tab” on page 600.

- References
  See “Standard details pane - References tab” on page 601.

- Exceptions
  See “Standard details pane - Exceptions tab” on page 601.

- Tags
  See “Standard details pane - Tags tab” on page 601.

See “About the details pane” on page 62.

**Standard details pane - General tab**

The General tab of the Standards details pane provides general information about the selected standard.

The General tab contains the following information:

- **Standard Name**: The name of the standard. This value is editable. See “Renaming a standard” on page 606.
- **Target Type(s)**: This list reflects the target type of all the checks that are present within the standard. See “About target types” on page 558.
- **Version**: The current version of the standard. See “About versioning scheme” on page 569.
- **Author**: For a predefined standard, the value of Author is Symantec. For a user-defined standard, this value refers to the user who created the standard.
- **Creation Date**: The date and time of creation of the standard.
- **Last Updated**: The date and time when the standard was last updated.
- **Number of Checks**: The total number of checks in the standard.
- **Last Evaluation**: The date and time when the standard was last evaluated.
The number of assets against which the standard was evaluated.

Compliance Score  The Compliance score of the standard.
  See “About compliance score” on page 569.

Risk Score  The risk score of the standard.
  See “About risk score” on page 569.

See “About the details pane” on page 62.
See “Viewing standard information in the details pane” on page 598.
See “Working in the details pane” on page 648.

**Standard details pane - Description tab**

The Description tab of the Standard details pane lets you describe the standard.

The Description tab has the following views:

- **Read only**
  This view lets you only read the standard description.

- **Edit**
  This view lets you make changes to the standard description.

See “About the details pane” on page 62.
See “Viewing standard information in the details pane” on page 598.
See “Working in the details pane” on page 648.

**Standard details pane - Evaluations tab**

The evaluations tab of the standard details pane provides the history of the last ten evaluation results for the standard.

The evaluations tab contains the following information:

- **Evaluation Date**  Specifies the date and time at which the evaluation job was run.
- **Evaluated against**  The name of all the assets against which the standard was evaluated. A comma (,) is used to separate the assets.
- **Compliance (%)**  The compliance value in percentage for all the assets against which the standard was evaluated.
- **Risk score**  The risk score of the asset.
- **Standard version**  Displays the version of the standard.
Standard details pane - References tab
The References tab lists the hyperlinks that lead to additional information about the standard.

The References tab contains the following information:

- **Name** The reference name
- **URL** The hyperlink for locating the reference information

You can perform the following tasks using the References tab:

- **Add reference information**
  See “Adding reference information” on page 651.
- **Edit reference information**
  See “Editing reference information” on page 652.
- **Delete reference information**
  See “Deleting reference information” on page 653.

See “Viewing section information in the details pane” on page 619.
See “About the details pane” on page 62.
See “Working in the details pane” on page 648.

Standard details pane - Tags tab
The Tags tab contains the list of all the tags that are associated with the selected standard.

The Tags tab lets you add a new tag to associate with the selected standard. You can also remove a tag that is already associated with the standard.

Standard details pane - Exceptions tab
The Exceptions tab lets you view the exception-related details of the checks within the standard.

The Exceptions tab contains the following information:

- **Title** The title that was specified at the time of creating the exception.
- **Effective Date** The start date of the exception validity period. The exception becomes valid from this date.
Expiration Date  The last day of the exception validity period. The exception becomes invalid after this date.

Last Modified On  The date and time when the exception was modified the last time.

See “About the details pane” on page 62.
See “Viewing standard information in the details pane” on page 598.
See “Working in the details pane” on page 648.

About multi-select functionality
You can select more than one standard, section, or check at a time to perform the common tasks.

The following tasks can be performed when you select multiple standards:
- Move
- Copy
- Delete
- Request exception
- Evaluate
- Set up a data collection job
- Set up collection-evaluation-reporting job

The following tasks can be performed when you select multiple sections or only multiple checks:
- Move
- Copy
- Delete
- Request exception

The following tasks can be performed when you select standards, sections, or checks simultaneously:
- Delete
- Request exception
Creating a new standard

You can create a new standard in the Standards view.

To create a new standard

1. Go to Manage > Standards.
2. In the Standards view, in the tree pane, select the folder in which you want to create the new standard.
3. Do one of the following:
   - On the taskbar, select Create Standard.
   - On the Tasks menu, select Create Standard.
   - In the table pane, right-click on an empty grid and select Create Standard.
4. In the Create Standard dialog box, in the Name box, type the name of the new standard.
5. In the Description box, enter the description information.
6. Click OK.

After you click OK, the Edit Standard dialog box is displayed. This dialog box lets you create a new section or a new check within the recently created standard. You can choose to close the dialog box and create a section or a check later.

Copying and pasting a standard

You can copy the predefined and the user-defined standards. You can copy multiple standards at a time to any folder except the predefined folder.
To copy and paste a standard using the context menu

1. Go to Manage > Standards.
2. In the table pane of the Standards view, right-click the standard that you want to copy and select Copy.

   This step lets you copy the selected standard. But to view the copied standard, you must perform the paste operation as explained in the next step.

3. In the tree view, select the folder where you want to locate the copied standard. In the table pane, right-click in the empty space in the grid and select Paste.

   You can paste a standard only within a folder. The paste option is disabled when you try to paste a standard within a section, or a check.

   After you paste a standard, a Progress Status bar is displayed. This bar shows the progress of the paste operation. A message appears when the paste operation is successful.

To copy and paste a standard using the menu bar

1. Go to Manage > Standards.
2. In the table pane of the Standards view, select the standard that you want to copy and on the menu bar, click Edit and then Copy.
3. Place the cursor where you want to place the copied standard. On the menu bar, click Edit and then paste.

Moving a standard

You can move the user-defined standards to any location except the predefined folder. The predefined standards cannot be moved.

To move a standard

1. Go to Manage > Standards.
2. In the table pane of the Standards view, do either of the following:

   - Right-click the standard that you want to move and select Move.
   - Select the standard that you want to move and on the taskbar, click Common Tasks > Move.
   - Select the standard that you want to move and on the Tasks menu, select Move.

3. In the Move Standard - Manage dialog box, select the destination folder to which you want to move the standard. Click OK.

See “About multi-select functionality” on page 602.
Importing a standard

You can import a standard that is compliant with the Control Compliance Suite. You can import the standard to any folder except the predefined container.

**Note:** When a standard is imported, the version of the standard is taken into consideration. Therefore, changing the name of the standard in the XML does not lead to creation of a new standard.

To import a standard

1. Go to Manage > Standards.
2. In the tree pane of the Standards view, select the folder to which you want to import the standard.
3. Do either of the following:
   - On the Tasks menu, select Import Standard.
   - On the taskbar, click Import Standard.
4. In the Import Standard dialog box, in the File Path box, type or browse to the standard file that you want to import.
   - The Container Folder displays the folder to which the standard is to be imported.
5. Click OK.

Exporting a standard

You can export a standard to a file system that is located outside the Control Compliance Suite. Exporting a standard can assist you in creating a backup of the standard. You cannot export a section or a check.

To export a standard

1. Go to Manage > Standards.
2. In the table pane of the Standards view, do one of the following:
   - Select the standard that you want to export and on the Tasks menu, select Export Standard.
Select the standard that you want to export and on the taskbar, click **Standard Tasks > Export Standard**.

Right-click the standard that you want to export and select **Export Standard**.

3. In the Export Standard - Manage dialog box, enter the name of the file that you want to export and the folder path.

4. Click **OK**.

See “**Working with standards**” on page 598.

### Renaming a standard

You can change the standard name through the General tab of the details pane.

**To rename a standard**

1. Go to Manage > Standards.

2. In the table pane of the Standards view, select the standard that you want to rename.

3. In the details pane, on the General tab, type the new name in the Standard Name text box.

4. Click the save icon.

See “**Working with standards**” on page 598.

### Deleting a standard

You can delete only the user-defined standards. The predefined standards cannot be deleted.

**To delete a standard**

1. Go to Manage > Standards.

2. In the table pane of the Standards view, do either of the following:

   - Right-click the standard that you want to delete and select **Delete**.

   - Select the standard that you want to delete and on the Tasks menu, click **Common Tasks > Delete**.

   - Select the standard that you want to delete and on the taskbar, click **Delete**.

3. In the Manage Standards box, select **Yes** to delete the selected standard.

See “**About multi-select functionality**” on page 602.

See “**Working with standards**” on page 598.
Running an evaluation job from the Standards view

You can evaluate the assets in your organizations against specific standards. The Create or Edit Evaluation Job wizard lets you create or edit an evaluation job. See “About evaluation jobs” on page 557.

To run an evaluation job

1. Go to Manage > Standards.
2. In the Standards view, do one of the following:
   - Right-click the standard that you want to evaluate and select Run Evaluation.
   - Select the standard that you want to evaluate and on the taskbar, click Run Evaluation.
   - Select the standard that you want to evaluate and on the Tasks menu, select Run Evaluation.
3. In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.
4. In the Description box, type a description for the evaluation job and click Next.
5. In the Select Targets panel, in the tree pane, select a folder. You can further select from the displayed folder contents.

   The selected assets are displayed in the Selected Items list.
6. After this step, you can configure automatic remediation.

   If you do not want to configure remediation, you can skip the Select Asset Types for Remediation panel and click Next to reach the Schedule Job panel.

   For a detailed procedure of configuring the automatic remediation visit the following link:

   See “To remediate the assets automatically” on page 608.
7. In the Schedule Job panel, select any one of the following:
   - If you want to run the evaluation job after the wizard closes, check Run Now.
   - If you want to run the job at a specified interval, check Run Periodically and enter the following information.

     In the Start On box, enter the start date and time to run the job.

     Under the Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click Next.
You must set a password in the System Management > User Preferences > Data Collection Password. If you fail to set the password, a warning message appears when you schedule the job. You can click OK in the message box and specify the scheduling details. But you must set the password before the scheduled time for running the job.

8 In the Add Result Viewers panel, add the users or the groups that have the permissions to view the evaluation results and reports.

It is recommended to add the groups as the result viewers.

9 In the Specify Notification Details panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check Send notification, enter the following information and then click Next:

- Enter the subject and message of the notification mail.
- Enter the sender and the receiver email ID.

Notification can be sent to multiple recipients.

10 In the Summary panel, review the information that you have entered. Click Back to make any changes, else click Next.

11 Click Finish to exit the wizard.

To monitor the current status of the job, go to Monitor > Jobs.

To remediate the assets automatically

1 In the Select Asset Type for Remediation Ticketing panel, check the Enable Automatic Remediation Ticketing option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and click Next.

2 In the Specify Remediation Ticketing Criteria panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select Apply to all standards if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select Apply to all standards, you must specify the remediation ticketing criteria for each standard.

Click Next.

3 In the Select Remediation Ticket Type panel, select one of the following:

- Create an email notification.
This option lets you create an email notification that you want to send for notification.

- Create a service desk ticket.
  This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.
  You can choose the Enable closed-loop verification option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.
  See “About closed-loop verification” on page 664.

Click Next.

4 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the Configure Notification Details for Remediation Ticketing panel. Click Next.

If you select Consolidate multiple assets in a single ticket/email, a single notification is sent that includes all the non-compliant assets.

You can check Make this the default Email Notification template if you want to use the same message for all the service desk ticket requests.

5 If you choose to create a service desk ticket as a remediation action, specify the message that you want to send as a service desk request in the Configure Service Desk Ticket panel. Click Next.

If you select Consolidate multiple assets in a single ticket/email, a single service desk ticket is generated that includes all the non-compliant assets.

You can check Make this the default Service Desk Ticket template if you want to use the same message for all the service desk ticket requests.

6 Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel.

See “Working with standards” on page 598.

Setting up a data collection job from the Standards view

You can run a data collection job from the Standards view. You can use the New Data Collection Job wizard to create a job to start the process of collecting data for the specified standards.

To set up a data collection job

1 Go to Manage > Standards.

2 In the table pane, select the standard for which you want to run the data collection job. On the taskbar, click Evaluation Tasks > Setup Data Collection.
3 In the Create or Edit Data Collection Job wizard, in the Specify Job Name and Description panel, in the Name field, type the name of the data collection job.

4 In the Description box, type a description for the evaluation job and click Next.

5 In the Select Assets panel, navigate through the assets and select an asset for which you want to set up a data collection.

6 Click Add to add the asset to the data collection job and click Next.
In the **Schedule Job** panel, select one of the following options:

- **Run with criteria**
  
  Lets you collect the data for the assets for which the data is older than the specified number of days or is missing.

- **Run now**
  
  Runs the job immediately, only once.

- **Run periodically**
  
  Runs the job periodically based on the specified interval.
  
  Lets you specify the date and time to be the periodic schedule on.
  
  The **Run Periodically** option presents more options within the schedule.

The following table describes the options under the **Run periodically options**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run once</td>
<td>Runs the job only once based on the date and time that you specify in the <strong>Start On</strong> option.</td>
</tr>
<tr>
<td>Run every # days</td>
<td>Runs the job at regular intervals based on the number of days you specify.</td>
</tr>
<tr>
<td>Sub-schedule for data collection</td>
<td>Lets you specify the number of days after which you want to repeat the job. The option also lets you specify the last day until you want the job to continue running periodically.</td>
</tr>
</tbody>
</table>

The sub-schedule is a subset of the period that you specify in the **Run every # days** option.

This schedule collects the data for the assets for which data was never collected for the standards in the job scopes.
8 In the Specify Notification Details panel, select Send notification and type the information for sending the notification and click Next.

9 In the Summary panel, review all the selections that you made and click Finish.

You can monitor the status of the job from the Monitor > Jobs view.

Running a collection-evaluation-reporting job from the Standards view

The collection-evaluation-reporting job lets you create a common job to schedule data collection, evaluation, and report generation. Control Compliance Suite provides different jobs for data collection, evaluation, and report generation tasks. In case of environments where thousands of such jobs are scheduled, a collection-evaluation-reporting job makes it easy to manage all the tasks from a single wizard.

See “About evaluation jobs” on page 557.

To run a collection-evaluation-reporting job

1 Go to Manage > Standards.

2 In the Standards view, do one of the following:
   - Right-click in the table pane and select Run Collection-Evaluation-Reporting.
   - Select the standard that you want to evaluate and on the taskbar, from the Evaluation Tasks, select Run Collection-Evaluation-Reporting.

3 In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.

4 In the Description box, type a description for the evaluation job and click Next.

5 In the Select Targets panel, navigate through the assets hierarchy, select the assets and click Next.

   You can select an asset, asset group, or an asset folder to evaluate.

6 In the Select Standards panel, from the list of standards that appear in the left section, select the standard against which you want to evaluate the assets. Click Add to add the selected standard and click Next.

   Click Add All to add all the standards that appear in the right section and click Next.

7 In the Select Report Templates panel, select one or more report templates for the evaluation job report.
After this step, you can configure automatic remediation.
If you do not want to configure remediation, you can skip the Select Asset Types for Remediation panel and click Next to reach the Schedule Job panel.
For a detailed procedure of configuring the automatic remediation visit the following link:
See “To remediate the assets automatically” on page 616.
9 In the **Schedule Job** panel, select one of the following options:

**Run with criteria**

Lets you collect the data for the assets for which the data is older than the specified number of days or is missing.

**Note:** This option is applicable to the data collection only.

**Run now**

Runs the job immediately, only once.

**Run periodically**

Runs the job periodically based on the specified interval.

Lets you specify the date and time to being the periodic schedule on.

The **Run Periodically** option presents more options within the schedule.

The following table describes the options under the **Run periodically options**:

**Run once**

Runs the job only once based on the date and time that you specify in the **Start On** option.

**Run every # days**

Runs the job at regular intervals based on the number of days you specify.
Sub-schedule for data collection

Lets you specify the number of days after which you want to repeat the job. The option also lets you specify the last day until you want the job to continue running periodically.

The sub-schedule is a subset of the period that you specify in the **Run every # days** option.

This schedule collects the data for the assets for which data was never collected for the standards in the job scope.

**Note:** The sub-schedule is applicable to the data collection only.

---

10 **In the Add Result Viewers** panel, add the users or the groups that have the permissions to view the evaluation results and reports.

It is recommended to add the groups as the result viewers.

11 **In the Specify Notification Details** panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check **Send notification**, enter the following information and then click **Next**:

- Enter the subject and message of the notification mail.
- Enter the sender and the receiver email ID.
  Notification can be sent to multiple recipients.

The Create or Edit Collection-Evaluation-Reporting wizard also lets you configure the details to remediate the assets that are non-compliant.
To remediate the assets automatically

1 In the Select Asset Type for Remediation Ticketing panel, check the Enable Automatic Remediation Ticketing option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and click Next.

2 In the Specify Remediation Ticketing Criteria panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select Apply to all standards if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select Apply to all standards, you must specify the remediation ticketing criteria for each standard.

Click Next.

3 In the Select Remediation Ticket Type panel, select one of the following:
   - Create an email notification.
     This option lets you create an email notification that you want to send for notification.
   - Create a service desk ticket.
     This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.
     You can choose the Enable closed-loop verification option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.
     See “About closed-loop verification” on page 664.

Click Next.

4 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the Configure Notification Details for Remediation Ticketing panel. Click Next.

If you select Consolidate multiple assets in a single ticket/email, a single notification is sent that includes all the non-compliant assets.

You can check Make this the default Email Notification template if you want to use the same message for all the service desk ticket requests.
If you choose to create a service desk ticket as a remediation action, specify the message that you want to send as a service desk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single service desk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the service desk ticket requests.

Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel.

See “Sizing guidelines for Collection-Evaluation-Reporting job” on page 617.

**Sizing guidelines for Collection-Evaluation-Reporting job**

The Collection-Evaluation-Reporting job supports only a certain report templates. The reports that are available for the Collection-Evaluation-Reporting job are divided into two groups. The reports that are resource intensive and contain a large amount of data may overload the Crystal Report API during report generation. These reports are classified as heavy-weight reports. The reports that contain less data may not overload the Crystal Report API during report generation. These reports are classified as light-weight reports.

The heavy-weight reports are as follows:

- Compliance by Asset
- Compliance by Technical Check

The light-weight reports are as follows:

- Compliance Summary
- Asset Risk Summary
- Asset Evaluation Result Change
- Assets at Highest Risk
- Asset Group Compliance
- Evaluation Results Asset View
- Evaluation Results Standard View
- Remediation Asset View
- Remediation Standard View

A heavy-weight report always fails to generate when the number of assets are above the 200 assets data point. The collection-evaluation-reporting job may succeed, but the report is not generated.
A light-weight report can handle between 200 and 500 assets. The Asset Evaluation Result Change report fails above the 500 asset data point.

See “Running a collection-evaluation-reporting job from the Standards view” on page 612.

Changing an ESM policy name at the standard level

You can rename an existing ESM policy name at the standard level. The policy name in the expressions of all the checks in the standard that you have selected is changed to the newly entered policy name.

---

**Note:** The ESM policy name is case sensitive.

---

**To change an ESM policy name at the standard level**

1. Right-click a standard and click **Change ESM Policy Name**.
2. In the Change ESM Policy Name dialog box, enter the new policy name.
3. Click **OK**.

See “About changing an ESM policy name” on page 572.

See “Changing an ESM policy name at the section level” on page 623.

See “Changing an ESM policy name at the check level” on page 637.

---

**Working with sections**

You can perform the following tasks on sections:

- View section information in the details pane
  - See “Viewing section information in the details pane” on page 619.

- Create a new section.
  - See “Creating a new section” on page 621.

- Copy and paste a section.
  - See “Copying and pasting a section” on page 621.

- Move a section.
  - See “Moving a section” on page 622.

- Rename a section.
  - See “Renaming a section” on page 623.

- Delete a section.
  - See “Deleting a section” on page 623.
Viewing section information in the details pane

You can view the information about a section from the details pane.

**To view the section information**

1. Go to **Manage > Standards**.
2. In the table pane of the Standards view, select the section for which you want to display the information.
3. View the information for the selected section in the details pane.

The section details are contained in the following tabs:

- **General**
  See “Section details pane - General tab” on page 619.

- **Description**
  See “Section details pane - Description tab” on page 620.

- **References**
  See “Section details pane - References tab” on page 620.

- **Exceptions**
  See “Section details pane - Exceptions tab” on page 621.

See “About the details pane” on page 62.

**Section details pane - General tab**

The General tab of the Section details pane provides general information about the selected section.

The General tab contains the following information:

- **Section Name**
  Name of the section. You can modify the name of the section. This value is editable.
  See “Renaming a section” on page 623.

- **Version**
  The current version of the section.
  See “About versioning scheme” on page 569.

- **Author**
  For a section that is contained within a predefined standard, the value of Author is Symantec.
  For a section that is contained within a user-defined standard, this value refers to the user who created the standard.

- **Creation Date**
  The date and time of creation of the section.
Section details pane - Description tab
The Description tab of the Section details pane lets you describe the standard. The Description tab has the following views:

- Read only
  This view lets you only read the section description.

- Edit
  This view lets you make changes to the section description.

See “Viewing section information in the details pane” on page 619.
See “About the details pane” on page 62.
See “Working in the details pane” on page 648.

Section details pane - References tab
The References tab lists the hyperlinks that lead to additional information about the section.

The References tab contains the following information:

- Name
  The reference name

- URL
  The hyperlink for locating the reference information

You can perform the following tasks using the References tab:

- Add reference information
  See “Adding reference information” on page 651.

- Edit reference information
  See “Editing reference information” on page 652.

- Delete reference information
  See “Deleting reference information” on page 653.
Section details pane - Exceptions tab

The Exceptions tab lets you view the exception-related details of the section.

The Exceptions tab contains the following information:

<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>The title that was specified at the time of creating the exception.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date</strong></td>
<td>The start date of the exception validity period. The exception becomes valid from this date.</td>
</tr>
<tr>
<td><strong>Expiration Date</strong></td>
<td>The last day of the exception validity period. The exception becomes invalid after this date.</td>
</tr>
<tr>
<td><strong>Last Modified On</strong></td>
<td>The date and time when the exception was last modified.</td>
</tr>
</tbody>
</table>

Creating a new section

You can create a new section only with reference to a standard or another section. Therefore, before you create a new section, you identify the standard or the section to which you want to add the new section.

**To add a new section to a standard or to another section**

1. Go to Manage > Standards.
2. In the Standards view, right-click the standard or the section to which you want to add the new section and select Create Section.
3. In the Section Name dialog box, enter the name of the new section. Click OK.

The new section is added to the standard. You can enter further information for the section such as description and references through the details pane.

See “Working with sections” on page 618.

Copying and pasting a section

You can copy the predefined and the user-defined sections to custom standards. You can copy one or more sections at a time to any folder except the predefined folder.

If you copy a section under the same standard, a copy of the section is created once. If you copy the same section again in the same standard, the newly copied section overwrites the previously copied section. You can copy a section under the same standard only once.
To copy and paste a section using the context menu
1. Go to Manage > Standards.
2. In the table pane of the Standards view, right-click the section that you want to copy and select **Copy**.
   This step lets you copy the selected section. But to view the copied section, you must perform the paste operation as explained in the next step.
3. Place the cursor under the standard or the section where you want to paste the copied section. Right-click the mouse and select **Paste**.
   The Progress Status bar is displayed. This bar shows the progress of the paste operation. A message appears when the section is pasted.

To copy and paste a section using the menu bar
1. Go to Manage > Standards.
2. In the table pane of the Standards view, right-click the section that you want to copy and on the menu bar, click **Edit** and then **Copy**.
3. Put the cursor where you want to place the copied section. On the menu bar, click **Edit** and then **paste**.

See “**About multi-select functionality**” on page 602.
See “**Working with sections**” on page 618.

### Moving a section

You can move the user-defined sections to any location except the predefined folder. You cannot move the predefined sections.

To move a section
1. Go to Manage > Standards.
2. In the table pane of the Standards view, do one of the following:
   - Right-click the section that you want to move and select **Move**.
   - Select the section that you want to move and on the taskbar, click **Common Tasks > Move**.
   - Select the section that you want to move and on the Tasks menu, select **Move**.
3. In the Move Standard - Manage dialog box, select the destination folder to which you want to move the section. Click **OK**.

See “**About multi-select functionality**” on page 602.
See “**Working with sections**” on page 618.
Renaming a section

You can change the section name through the General tab of the details pane.

To rename a section

1. Go to Manage > Standards.
2. In the table pane of the Standards view, select the section that you want to rename.
3. In the details pane, on the General tab, type the new name in the Section Name text box.
4. Click the save icon.

See “Working with sections” on page 618.

Deleting a section

You can delete only the user-defined sections. You cannot delete the predefined sections.

To delete a section

1. Go to Manage > Standards.
2. In the table pane of the Standards view, do one of the following:
   - Right-click the section that you want to delete and select Delete.
   - Select the section that you want to delete and on the taskbar, click Common Tasks > Delete.
   - Select the section that you want to delete and on the Tasks menu, select Delete.
3. In the Manage Standards box, select Yes to delete the selected section.

See “About multi-select functionality” on page 602.

See “Working with sections” on page 618.

Changing an ESM policy name at the section level

You can rename an existing ESM policy name at the standard level. The policy name in the expressions of all the checks in the section that you have selected is changed to the newly entered policy name.
To change an ESM policy name at the section level

1. Right-click a section and click **Change ESM Policy Name**.
2. In the Change ESM Policy Name dialog box, enter the new policy name.
3. Click **OK**.

See “About changing an ESM policy name” on page 572.

See “Changing an ESM policy name at the standard level” on page 618.

See “Changing an ESM policy name at the check level” on page 637.

**Working with checks**

You can perform a number of tasks with checks. You can cut, copy, paste, create, and delete checks. You can also create new check expressions to customize the checks.

You can perform the following tasks on checks:

- View check information in the details pane
  
  See “Viewing check information in the details pane” on page 624.

- Create a new check.
  
  See “Creating a new check” on page 633.

- Copy and paste a check.
  
  See “Copying and pasting a check” on page 631.

- Move a check.
  
  See “Moving a check” on page 632.

- Rename a check.
  
  See “Renaming a check” on page 632.

- Delete a check.
  
  See “Deleting a check” on page 633.

- Modify a check.
  
  See “Editing a check” on page 636.

**Viewing check information in the details pane**

You can view the information about a check through the details pane.
To view the check information

1. Go to Manage > Standards.
2. In the table pane of the Standards view, navigate to the check for which you want to display the information and select the check.
3. View the information for the selected check in the details pane.

The check details are contained in the following tabs:

- General
  See “Check details pane - General tab” on page 625.
- Description
  See “Check details pane - Description tab” on page 627.
- Expression
  See “Check details pane - Expression tab” on page 628.
- Parameters
  See “Check details pane - Parameters tab” on page 628.
- Remediation
  See “Check details pane - Remediation tab” on page 629.
- Issue
  See “Check details pane - Issue tab” on page 629.
- CVE
  See “Check details pane - CVE tab” on page 630.
- References
  See “Check details pane - References tab” on page 630.
- Target Type
  See “Check details pane - Target Type tab” on page 630.
- Exceptions
  See “Check details pane - Exceptions tab” on page 631.

See “About the details pane” on page 62.

Check details pane - General tab

The General tab of the Check details pane provides general information about the selected check.

The General tab contains the following information:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Name</td>
<td>The name of the check. This value is editable.</td>
</tr>
<tr>
<td></td>
<td>See “Renaming a check” on page 632.</td>
</tr>
<tr>
<td>Target Type</td>
<td>The type of asset to which the check is applicable.</td>
</tr>
<tr>
<td></td>
<td>See “About target types” on page 558.</td>
</tr>
<tr>
<td>Author</td>
<td>The value of Author is Symantec for a check that is contained within a predefined standard. For a check that is contained within a user-defined standard, this value refers to the user who created the check.</td>
</tr>
<tr>
<td>Version</td>
<td>The current version of the check.</td>
</tr>
<tr>
<td></td>
<td>See “About versioning scheme” on page 569.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>The date and time of creation of the check.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date and time when the check was last updated.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Confidentiality value has one of the following states:</td>
</tr>
<tr>
<td></td>
<td>■ Not Defined</td>
</tr>
<tr>
<td></td>
<td>■ No Impact</td>
</tr>
<tr>
<td></td>
<td>■ Partial</td>
</tr>
<tr>
<td></td>
<td>■ Complete</td>
</tr>
<tr>
<td>Integrity</td>
<td>Integrity value has one of the following states:</td>
</tr>
<tr>
<td></td>
<td>■ Not Defined</td>
</tr>
<tr>
<td></td>
<td>■ No Impact</td>
</tr>
<tr>
<td></td>
<td>■ Partial</td>
</tr>
<tr>
<td></td>
<td>■ Complete</td>
</tr>
<tr>
<td>Availability</td>
<td>Availability value has one of the following states:</td>
</tr>
<tr>
<td></td>
<td>■ Not Defined</td>
</tr>
<tr>
<td></td>
<td>■ No Impact</td>
</tr>
<tr>
<td></td>
<td>■ Partial</td>
</tr>
<tr>
<td></td>
<td>■ Complete</td>
</tr>
<tr>
<td>Access Vector</td>
<td>Access Vector has one of the following states:</td>
</tr>
<tr>
<td></td>
<td>■ Not Defined</td>
</tr>
<tr>
<td></td>
<td>■ Local Accessible</td>
</tr>
<tr>
<td></td>
<td>■ Adjacent Network Accessible</td>
</tr>
<tr>
<td></td>
<td>■ Network Accessible</td>
</tr>
</tbody>
</table>
Access Complexity has one of the following states:
- Not Defined
- Low
- Medium
- High

Authentication has one of the following states:
- Not Defined
- Multiple Instances
- Single Instance
- No Authentication

For a user-defined check, you can modify the following information about the check through the General tab:
- Check Name
  See “Renaming a check” on page 632.
- Confidentiality
- Integrity
- Availability
- Access Vector
- Access Complexity
- Authentication

See “Viewing check information in the details pane” on page 624.
See “About the details pane” on page 62.
See “Working in the details pane” on page 648.

Check details pane - Description tab

The Description tab of the Check details pane lets you describe the standard.

The Description tab has the following views:
- Read only
  This view lets you only read the check description.
- Edit
  This view lets you make changes to the check description.

See “Viewing check information in the details pane” on page 624.
See “About the details pane” on page 62.
See “Working in the details pane” on page 648.

**Check details pane - Expression tab**

The Expression tab of the check details pane states the check formula and the specified pre-conditions.

The Expression tab contains the following information:

- **Pre-Condition**: States the pre-condition.
- **Formula**: States the check formula.

Click the Switch to expanded mode icon to expand the individual expressions in the formula and view the complete formula.

To view information for each expression in the formula, click the expression in the formula. The Expression text dialog box appears. This dialog box contains the selected expression.

You can also edit the pre-condition and the check formula through the Expression tab.

See “Viewing check information in the details pane” on page 624.

See “About the details pane” on page 62.

See “Working in the details pane” on page 648.

**Check details pane - Parameters tab**

Some checks in the predefined standards use complex algorithms. The custom algorithms make use of named procedures. You must use the Parameters tab in the details pane to modify the values of the parameter.

- **Name**: The name of the parameter.
- **Value**: The value of the parameter.

The Parameters tab also lets you add or remove the indexed parameters in case of complex checks. To add or remove the indexed parameters, you must select an indexed parameter, right-click and select **Add new parameter**. Another parameter with the next order in the index is created. You can also remove an indexed parameter. If you remove an indexed parameter, the indexing for the other parameters of the same type changes.

Consider the following examples:
Consider that you have indexed parameters such as "Permission0," "Permission1," and "Permission2. You remove the index parameter "Permission1." The parameter "Permissions2" is renamed to "Permissions1."

The permissions algorithms parameters for the Windows platform are more complex than those of other complex algorithms.

The Permissions algorithms for Windows use parameter sets as follows:

- Accounts
- Permissions that the account is allowed to use
- Scope to which the permissions are applied

See “Viewing check information in the details pane” on page 624.

See “About the details pane” on page 62.

See “Working in the details pane” on page 648.

Check details pane - Remediation tab

The Remediation tab of the check details pane states the recommended fixes for the issue.

The Remediation tab has the following views:

- Read only
  This view lets you only read the remediation information that was entered when the check was created.

- Edit
  This view lets you make changes to the remediation information.

See “Viewing check information in the details pane” on page 624.

See “About the details pane” on page 62.

See “Working in the details pane” on page 648.

Check details pane - Issue tab

The Issue tab of the check details pane states the reason for creating the check.

The Issue tab has the following views:

- Read only
  This view lets you only read the issue information that was entered when the check was created.

- Edit
  This view lets you make changes to the issue information.
See “Viewing check information in the details pane” on page 624.
See “About the details pane” on page 62.
See “Working in the details pane” on page 648.

**Check details pane - CVE tab**
The CVE tab of the check details pane lists the number for the common vulnerabilities and exposures information.
See “Viewing check information in the details pane” on page 624.
See “About the details pane” on page 62.
See “Working in the details pane” on page 648.

**Check details pane - References tab**
The References tab lists the hyperlinks that lead to additional information about the check.
The References tab contains the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>The reference name</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The hyperlink for locating the reference information</td>
</tr>
</tbody>
</table>

You can perform the following tasks using the References tab:
- Add reference information
  See “Adding reference information” on page 651.
- Edit reference information
  See “Editing reference information” on page 652.
- Delete reference information
  See “Deleting reference information” on page 653.
See “Viewing check information in the details pane” on page 624.
See “About the details pane” on page 62.
See “Working in the details pane” on page 648.

**Check details pane - Target Type tab**
The Target Type tab of the check details pane shows the target type that is mapped to the selected check. The tab also displays the filter that is used for the target type.
See “Viewing check information in the details pane” on page 624.

See “About the details pane” on page 62.

See “Working in the details pane” on page 648.

**Check details pane - Exceptions tab**

The Exceptions tab lets you view the exception-related details of the check.

The Exceptions tab contains the following information:

<table>
<thead>
<tr>
<th>Title</th>
<th>The title that was specified at the time of creating the exception.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date</td>
<td>The start date of the exception validity period. The exception becomes valid from this date.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The last day of the exception validity period. The exception becomes invalid after this date.</td>
</tr>
<tr>
<td>Last Modified On</td>
<td>The date and time when the exception was last modified.</td>
</tr>
</tbody>
</table>

**Copying and pasting a check**

You can copy the predefined and the user-defined checks. You can copy one or more checks at a time to any folder except the predefined folder.

If you copy a check under the same section, a copy of the check is created once. If you copy the same check again in the same section, the check overwrites the previously copied check. You can copy a check under the same section only once.

**To copy and paste a check using the context menu**

1. Go to Manage > Standards.
2. In the table pane of the Standards view, right-click the check that you want to copy and select **Copy**.
   
   This step lets you copy the selected check. But to view the copied check, you must perform the paste operation as explained in the next step.
3. Place the cursor under the section where you want to paste the copied check. Right-click the mouse and select **Paste**.

   The Progress Status bar is displayed. This bar shows the progress of the paste operation. A message appears when the check is pasted.
To copy and paste a check using the menu bar

1. Go to Manage > Standards.
2. In the table pane of the Standards view, right-click the check that you want to copy and on the menu bar, click Edit and then Copy.
3. Place the cursor where you want to locate the copied check. On the menu bar, click Edit and then paste.

See “About multi-select functionality” on page 602.
See “Working with checks” on page 624.

Moving a check

You can move the user-defined checks to any location except the predefined folder. The predefined checks cannot be moved.

To move a check

1. Go to Manage > Standards.
2. In the table pane of the Standards view, do one of the following:
   ■ Right-click the check that you want to move and select Move.
   ■ Select the check that you want to move and on the taskbar, click Common Tasks > Move.
   ■ Select the check that you want to move and on the Tasks menu, select Move.
3. In the Move Standard - Manage dialog box, select the destination folder to which you want to move the check. Click OK.

See “About multi-select functionality” on page 602.
See “Working with checks” on page 624.

Renaming a check

You can change the check name through the General tab of the details pane.

To rename a check

1. Go to Manage > Standards.
2. In the table pane of the Standards view, select the check that you want to rename.
3 In the details pane, on the General tab, type the new name in the Check Name text box.

4 Click the save icon.

See “Working with checks” on page 624.

Deleting a check

You can delete only the user-defined checks. You cannot delete the predefined checks.

To delete a check

1 Go to Manage > Standards.

2 In the table pane of the Standards view, do one of the following:
   - Right-click the check that you want to delete and select Delete.
   - Select the check that you want to delete and then on the taskbar, click Common Tasks > Delete.
   - Select the check that you want to delete and then in the Tasks menu, select Delete.

3 In the Manage Standards dialog box, select Yes to delete the selected check.

See “About multi-select functionality” on page 602.

See “Working with checks” on page 624.

Creating a new check

You must use the Create Check wizard to create a new check.

The Create Check wizard provides you the following options to create a new check:

- **Quick Check Builder**: This option lets you create a check that does not include a pre-condition.
- **Advanced Check Builder**: This option lets you create a check that includes a pre-condition.

To create a new check

1 Go to Manage > Standards.

2 In the table pane of the Standards view, navigate to the section to which you want to add the new check. Right-click the section and select Create Check.
3 In the Specify Name and Target panel of the Create Check wizard, enter the following information:

- In the Name text box, type the name of the new check.
- In the Description text box, type a description for the new check. This information is optional.
- In the Target Type text box, select the type of asset to which the new check is applicable.
  You can also create custom target types to evaluate specific standards against a targeted set of assets.
- Select either the Quick Check Builder option or the Advanced Check Builder option.
  The Quick Check Builder option lets you create a check without a precondition.
  The Advanced Check Builder option lets you add a precondition to the new check.

4 Click Next

To proceed with check creation using the Quick Check Builder option

1 In the Create Expression(s) panel, enter the following information to create an evaluation condition.

- In the Category list box, select the category of the field.
- In the Field list box, select the name of the field.
- In the Operator list box, select the operator.
- In the Value text box, specify a value for the field.
  To specify values for a LIST field, you must enclose all the values in a curly bracket and use a comma to separate each value. For example, {sam, ram, mac}.

2 Click the plus (+) sign to add the recently created field expression to the Expression(s) list.

  The new expression is added to the Formula box by default. If a check includes only a single expression, then the check formula is the same as the expression.

3 Repeat step 1 and step 2 to create any number of expressions.

4 In the Formula text box, you can use the check formula operators to connect the various expressions.

  By default, the new expressions are connected using the AND operator.
5 Click the Validate Formula icon to validate the check formula that you have created. Click **Next**.

6 In the Check Summary panel, you can view the information that you have entered. Click **Back** to make any changes and click **Finish** to exit the wizard.

**To proceed with check creation using the Advanced Check Builder option**

1 In the Create a Precondition panel, enter the following information to create an evaluation condition.
   - In the Category list box, select the category of the field.
   - In the Field list box, select the name of the field.
   - In the Operator list box, select the operator.
     See “About operators” on page 590.
   - In the Value text box, specify a value for the field.
     To specify values for a LIST field, you must use a comma to separate the multiple values and enclose all the values in a curly bracket. For example, \{sam, ram, mac\}.

2 Click the plus (+) sign to add the recently created field expression to the Expression(s) list.

   The new expression is added to the Formula box by default. If a check includes only a single expression then the check formula is the same as the expression.

3 Repeat steps 1 and 2 to create any number of expressions.

4 In the Formula text box, you can use the check formula operators to connect the various expressions.

   By default, the new expressions are connected using the AND operator.

5 Click the Validate Formula icon to validate the check formula that you have created. Click **Next**.

6 In the Create Expression(s) panel, enter the information in the same manner as in steps 1 to 5. Click **Next**.

7 In the Specify Check Content panel, enter the optional information such as risk rating, remediation, issue, CVE, and references. Click **Next**.

   See “Editing a check” on page 636.

8 In the Check Summary panel, you can view the information that you have entered. Click **Back** to make any changes and click **Finish** to exit the wizard.

   See “Viewing check information in the details pane” on page 624.

   See “Check details pane - Remediation tab” on page 629.
See “Check details pane - Issue tab” on page 629.
See “Check details pane - CVE tab” on page 630.
See “Check details pane - References tab” on page 630.
See “About the target type schema” on page 445.
See “Creating a new target type” on page 466.
See “Editing a target type” on page 467.

Editing a check

You can make changes to an existing check.

The following features of a check can be edited:

- Name and risk attributes
  You can change the name, target type, and the risk rating values of the check from the General tab of the details pane.
  See “Renaming a check” on page 632.
  See “Specifying or editing the check attributes” on page 651.

- Description
  You can change the description of the check from the Description tab of the details pane.
  See “Specifying or editing the description” on page 649.

- Remediation, issue, and references
  You can change the remediation, issue, and references information from the respective tabs on the details pane.
  See “Specifying or editing the remediation information” on page 650.
  See “Specifying or editing the check issue” on page 649.
  See “Editing reference information” on page 652.

- Pre-condition and Check formula
  You can change the pre-condition and the check formula from the Edit Check wizard.

  **Note:** You cannot edit the checks that contain a “proc:”call in the pre-condition of the check algorithm.

  **Note:** You cannot edit the pre-condition and the check formula of a custom check.
To change the pre-condition and the check formula

1. In the table pane of the Standards view, do either of the following:
   ■ Right-click the check that you want to modify and select **Edit**.
   ■ Select the check that you want to modify and on the Expressions tab of the details pane, click **Edit**.
   ■ Go to the **Expressions** tab in the check details pane.

2. In the Specify a target filter panel of the Edit Check wizard, enter the following information to create a field expression:
   ■ In the Category list box, select the category of the field.
   ■ In the Field list box, select the name of the field.
   ■ In the Operator list box, select the operator.
   ■ In the Value text box, specify a value for the field.

3. Click the plus (+) sign to add the recently created field expression to the Expression(s) list.

   The new expression is added to the Formula box by default. If a check includes only a single expression then the check formula is the same as the expression.

4. Repeat step 2 and step 3 to create any number of expressions.

5. In the Formula text box, you can use the check formula operators to connect the various expressions.

   By default, the new expressions are connected using the AND operator.

6. Click **Validate Formula** to validate the check formula that you have created.

7. In the Expressions panel, enter the information in the same manner as in steps 1 to 5.

8. In the Review panel, you can view the information that you have entered. Click **Back** to make any changes and click **Finish** to exit the wizard.

See “**Working with checks**” on page 624.

See “**Creating a new check**” on page 633.

### Changing an ESM policy name at the check level

You can rename an existing ESM policy name at the check level. The policy name in the expressions of the check that you have selected is changed to the newly entered policy name.
To change an ESM policy name at the check level

1. Right-click a check and click **Change ESM Policy Name**.
2. In the Change ESM Policy Name dialog box, enter the new policy name.
3. Click **OK**.

See “**About changing an ESM policy name**” on page 572.

See “**Changing an ESM policy name at the standard level**” on page 618.

See “**Changing an ESM policy name at the section level**” on page 623.

Creating an ESM check

You can create the CCS ESM checks using the Check Builder wizard.

The Check Builder wizard provides you with the following options to create checks:

- **The Quick Check Builder option**
  - Lets you create a check without a precondition.

- **The Advanced Check Builder option**
  - Lets you add a precondition to the new check.

The check execution process in ESM includes the following:

- The CCS evaluation engine checks if the ESM agent reports the security messages that the corresponding CCS ESM check generates.

- If the ESM agents reports security messages, then the CCS check is reported as "Fail."
  - In case of a failed check, the evidence report includes the following:
    - The ESM message title
    - The message name
    - The message information

- If the ESM agent does not report any security message, then the CCS evaluation engine checks if the agent reports any error message.

- If the ESM agents reports error messages, then the CCS check is reported as "Unknown" and the evidence report includes the ESM error messages.

- If the ESM agent does not report any security message or any error message, then the CCS check is reported as "Pass."
Note: You must include the policy name and the module name in the data filter when you create an expression in an ESM check. The ESM data collector uses the policy name and module name that you specify when it collects data for the checks.

See “Creating a CCS ESM check by using the Quick Check Builder option” on page 639.

See “Creating a CCS ESM check by using the Advanced Check Builder option” on page 644.

Creating a CCS ESM check by using the Quick Check Builder option

You can create CCS ESM checks by using the Quick Check Builder option.

To create a CCS ESM check by using the Quick Check Builder option

1 In the Standards pane, right-click the section to which you want to add the new check and click Create Check.

2 In the Specify Name and Target Type panel of the Check Builder, enter the following information:
   - In the Name text box, type a name for the new check.
   - In the Description text box, type a description for the check. This field is optional.
   - From the Target Type drop-down list, expand the Enterprise Security Manager Platform node, and then click the type of asset that you want to be evaluated. See “About ESM predefined target types” on page 565.
   - Click Quick Check Builder.

3 Click Next.

4 In the Create Expressions panel, create a message expression by performing the following steps:
   - From the Category drop-down list, select a category for the ESM entity. For example, select ESM Message.
   - In the Field drop-down list, select a field for the ESM message entity that you want the check to report on. For example, select Message String ID.
   - From the Operator drop-down list, select the operator. For example, select !=.
   - From the Value text box, select a value for the specified value. For example, select ESM_DISABLED_ACCOUNT.
See the Symantec_Enterprise_Security_Manager_Checks_Reference.chm for information on the messages that ESM checks generate. This file is located in the Documentation folder in the product disc.

- Click the Add icon to add the recently created check expression to the Expression(s) list.
  By default, the new expressions are connected using the AND operator.

See the Symantec_Enterprise_Security_Manager_Checks_Reference.chm for information on the messages that ESM checks generate. This file is located in the Documentation folder in the product disc.

5 Add data filters for ESM module name and ESM policy name.

See “Configuring the advanced settings for the data filters of an ESM check expression” on page 641.

6 Update the CCS check formula so that the CCS check behaves as per the check execution rules.

See “Editing the check formula for a new CCS ESM check” on page 643.

7 Click Next.

8 In the Review panel, view the information that you have entered and then click Finish.

See “Creating an ESM check” on page 638.

See “Creating a CCS ESM check by using the Advanced Check Builder option” on page 644.

### Creating a message expression for a new CCS ESM check

You need to add a message expression for each message that the corresponding CCS ESM check generates.

**To create a message expression**

1 Click the Add icon to add the recently created check expression to the Expression(s) list.
  By default, the new expressions are connected using the AND operator.

2 Select the expression that you have created from the Expression(s) list box and click Advanced Settings. Alternatively, double-click the expression in the Expression(s) list.

See “Configuring the advanced settings for the data filters of an ESM check expression” on page 641.

See “Configuring the advanced settings for the data filters of an ESM check expression” on page 641.
Configuring the advanced settings for the data filters of an ESM check expression

You must add the policy name and the module name to the ESM check that you want to create.

To configure the advanced settings for an ESM check expression

1. In the Create Expression(s) panel of the CCS Check Builder wizard, do the following:
   - In the Category drop-down list, click ESM Message.
   - In the Field drop-down list, click ESM Module Name.
   - Select the = operator and then select a module name from the Value drop-down list.
   - Click the plus (+) sign to add the expression to the Expression(s) list.
   - In the Expression(s) list, double-click the expression.

2. To add a data filter for policy name, do the following:
   - From the Field drop-down list, select ESM Policy.
   - Select the = operator and then type a policy name in the Value drop-down list. For example, type Security essentials W2K3MS v2.0. ESM policy names are case sensitive.
   - The = operator is the only operator that ESM data collector supports for ESM policy data filter.
   - Click the plus sign (+) to add the expression.

3. In the Advanced Settings dialog box, do the following to add a data filter for the module name:
   - From the Field drop-down list, select ESM Module Name.
   - Select the = operator and then select a module name from the Value drop-down list. For example, select Account Integrity.
   - Click the plus sign (+) to add the expression.

4. In the Data items filter section, click Return only the data which matches ALL of the filter statements. This option is mandatory to create a valid CCS ESM check.

5. In the Action for multiple data items section, click ALL must meet the evaluation condition.
6 In the **Outcome of missing data items** section, specify whether the check should report as Pass, Fail, or Unknown if the check does not find the expected data against the specified evaluation condition.

7 Click **OK**.

See “Creating an ESM check” on page 638.

**Creating an ESM error expression for a new ESM check**

You must add an error expression to the ESM check that you want to create. An error expression checks if an ESM agent reports any error message.

To **create an ESM error expression**

1 In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.

2 In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click one of the following options:

   - Quick Check Builder
   - Advanced Check Builder

3 Click **Next**.

4 In the Create Expressions panel, enter the following information to create an error expression:

   - In the Category drop-down list, select **Message**.
   - In the Field drop-down list, select **Is Error Message**.
   - In the Operator drop-down list, select the “=” operator.
   - In the Value text box, select **False**.

An expression that contains "Is Error Message = False" lets you mark a check for manual review if an ESM module generates error messages.
5 Click the plus sign (+) to add the recently created field expression to the Expression(s) list.

The new expression is added to the Formula box by default. If a check includes only a single expression then the check formula is the same as the expression.

You can create as many expressions as you want.

6 Select the expression from the Expression(s) list box and click Advanced Settings. Alternatively, double-click the expression in the Expression(s) list.

For every expression that you create on a Message entity, you must add data filters for module name and policy name.

See “Configuring the advanced settings for the data filters of an ESM check expression” on page 641.

See “Creating an ESM check” on page 638.

**Editing the check formula for a new CCS ESM check**

After you create the message expression and the error expression, you must edit the check formula to ensure that the check that you create behaves as per the specifications.

To edit the check formula for a new CCS ESM check

1 In the Standards pane, right-click the section to which you want to add the new check and click Create Check.

2 In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click one of the following options:
   - Quick Check Builder
   - Advanced Check Builder

3 Click Next.
In the Create Expressions panel, enter the necessary information to create an error expression.

In the Formula box, edit the predicate as follows:

Type If ([message expression]) THEN (IF ([error expression]) THEN (True) ELSE (Unknown)) ELSE ([False])

Following is the explanation for the message expression and error expression:

<table>
<thead>
<tr>
<th>Message expression</th>
<th>Name of the message expression that you have created, which corresponds to the messages that an ESM check generates. If the check generates multiple messages, you must specify the message expressions by using the logical AND operator. For example, E1 AND E2.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error expression</td>
<td>Name of the error expression.</td>
</tr>
</tbody>
</table>

Creating a CCS ESM check by using the Advanced Check Builder option

You can create CCS ESM checks by using the Advanced Check Builder option.

To create a CCS ESM check by using the Advanced Check Builder option

1. In the Standards pane, right-click the section to which you want to add the new check and click Create Check.

2. In the Specify Name and Target Type panel of the Check Builder, enter the following information:
   - In the Name text box, type a name for the new check.
   - In the Description text box, type a description for the check. This field is optional.
   - From the Target Type drop-down list, expand the Enterprise Security Manager Platform node, and then click the type of ESM asset that you want to evaluate. See “About ESM predefined target types” on page 565.
   - Click Advanced Check Builder.

3. In the Create a Precondition panel, enter the following details to narrow down the scope for targets that the check considers during evaluation. You
can add multiple pre-conditions for a check or you may choose to skip the Create a Precondition panel. The information that you provide in the Create a Precondition panel are optional.

- From the Category drop-down list, select the category of the ESM entity.
- From the Field drop-down list, select the field for the category that you want the check to report on. Click the Browse Fields icon to view the description of each field.
- From the Operator drop-down list, select the operator.
- From the Value drop-down list, select the value for the field that you have selected.
- Click the Add icon to add the pre-condition to the Expressions list box. You can see the name of the check formula that you create in the Formula box.
- Double-click the evaluation condition and configure the advanced settings for the check expression and then Next.

4 In the Create Expressions panel, create a message expression by performing the following steps:

- From the Category drop-down list, select a category for the ESM entity. For example, select ESM Message.
- In the Field drop-down list, select a field for the ESM message entity that you want the check to report on. For example, select Message String ID.
- From the Operator drop-down list, select the operator. For example, select !=.
- From the Value text box, select a value for the specified value. For example, select ESM_DISABLED_ACCOUNT.
- See the Symantec_Enterprise_Security_Manager_Checks_Reference.chm for information on the messages that ESM checks generate. This file is located in the Documentation folder in the product disc.
- Click the Add icon to add the recently created check expression to the Expression(s) list.
- By default, the new expressions are connected using the AND operator.

5 Add data filters for ESM module name and ESM policy name.

6 Do the following to add an error expression to the check that you want to create. The error expression checks if an ESM agent reports any error message.
In the Category drop-down list, select **Message**.

In the Field drop-down list, select **Is Error Message**.

In the Operator drop-down list, select the “=” operator.

In the Value text box, select **False**.

An expression that contains "Is Error Message = False" lets you mark a check for manual review if an ESM module generates error messages.

Click the plus sign (+) to add the recently created field expression to the Expression(s) list.

The new expression is added to the Formula box by default. If a check includes only a single expression then the check formula is the same as the expression.

You can create as many expressions as you want.

Select the expression from the Expression(s) list box and click **Advanced Settings**. Alternatively, double-click the expression in the Expression(s) list.

For every expression that you create on a Message entity, you must add data filters for module name and policy name.

**7** Update the CCS Check formula so that the CCS check behaves as per the check execution rules.

See “Creating an ESM check” on page 638.

See “Editing the check formula for a new CCS ESM check” on page 643.

**8** Click **Next**.
9 In the **Specify Check Content** panel, enter the information on the content of the check. This information is optional.

- **Risk Rating**: Lets you enter the check attributes. These values are used to calculate the Risk Score.
- **Remediation**: Lets you enter the remediation for the issue.
- **Issue**: Lets you enter more information on the issue.
- **CVE**: Lets you enter the ID for common vulnerabilities and exposures.
- **References**: Lets you enter the URL for a Web site for more information.

10 In the Review panel, view the information that you have entered and then click **Finish**.

See “Creating an ESM check” on page 638.

See “Creating a CCS ESM check by using the Quick Check Builder option” on page 639.

**Specifying the content for a new CCS ESM check**

You can specify the check content when you create an ESM check by using the Specify Check Content panel.

**To specify the content for a new CCS ESM check**

1 In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.

2 In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click **Advanced Check Builder**.

3 Click **Next**.
4 In the Create Expressions panel, enter the necessary information to create an error expression and then click Next.

See “Creating an ESM error expression for a new ESM check” on page 642.

5 In the Specify Check Content panel, enter the information on the content of the check. This information is optional.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Rating</td>
<td>Lets you enter the check attributes. These values are used to calculate the Risk Score.</td>
</tr>
<tr>
<td>Remediation</td>
<td>Lets you enter the remediation for the issue.</td>
</tr>
<tr>
<td>Issue</td>
<td>Lets you enter more information on the issue.</td>
</tr>
<tr>
<td>CVE</td>
<td>Lets you enter the ID for common vulnerabilities and exposures.</td>
</tr>
<tr>
<td>References</td>
<td>Lets you enter the URL for a Web site for more information.</td>
</tr>
</tbody>
</table>

See “Creating a CCS ESM check by using the Advanced Check Builder option” on page 644.

See “Creating a CCS ESM check by using the Quick Check Builder option” on page 639.

### Working in the details pane

You can perform the following tasks using the details pane:

- Rename a standard, section, or check
  See “Renaming a standard” on page 606.
  See “Renaming a section” on page 623.
  See “Renaming a check” on page 632.

- Enter or edit the description for a standard, section, or check.
  See “Specifying or editing the description” on page 649.

- Add, edit, or delete the reference information for a standard, section, or check.
  See “Adding reference information” on page 651.
  See “Editing reference information” on page 652.
  See “Deleting reference information” on page 653.

- Enter or edit the remediation information for a check.
See “Specifying or editing the remediation information” on page 650.

■ Enter or edit the issue information for a check.
  See “Specifying or editing the check issue ” on page 649.

■ Add or edit the CVE information for a check.
  See “Adding the CVE information” on page 650.
  See “Editing the CVE information” on page 651.

■ Enter or edit the risk attributes of a check
  See “Specifying or editing the check attributes” on page 651.

Specifying or editing the description

You can specify the description when you create a standard, section, or check. You can also enter the description from the details pane after creating a standard, section, or check. You can edit the description only through the details pane.

To specify or edit the description using the details pane

1 Go to Manage > Standards.

2 In the Standards view, select the standard, section, or check for which you want to enter or modify the description.

3 On the Description tab, click the Switch between Edit and Read-only view icon.

   This icon lets you switch between the Read-only and the Edit view.

4 Enter a description or modify the existing description.
   You can use the Bold, list item, and the Web link icon on the taskbar.

5 Click the save icon.

   See “Working in the details pane” on page 648.

Specifying or editing the check issue

You can enter or edit the issue information for a check through the details pane. You can also enter the check issue at the time of creating a check.

To specify or edit the issue information using the details pane

1 Go to Manage > Standards.

2 In the table pane, navigate to the check for which you want to edit the issue information. Select the check.

3 In the details pane, on the Issue tab, click the icon with two arrows.

   This icon lets you switch between the Read-only and the Edit view.
4 Enter the issue or edit the existing issue.
   You can use the Bold, list item, and the Web link icon on the taskbar.
5 Click the Save icon.
See “Working in the details pane” on page 648.

Specifying or editing the remediation information
You can specify or edit the remediation information for a check through the details pane.

To edit the remediation information
1 Go to Manage > Standards.
2 In the table pane, navigate to the check for which you want to edit the remediation information. Select the check.
3 In the details pane, on the Remediation tab, click the Switch between Edit and Read-only view icon.
   This icon lets you switch between the Read-only and the Edit view.
4 Enter or edit the remediation information.
   You can use the Bold, list item, and the Web link icon on the taskbar.
5 Click the save icon.
See “Working in the details pane” on page 648.

Adding the CVE information
You can add the CVE information for a check through the details pane. You can also enter the CVE information at the time of creating a check.

To add the CVE information using the details pane
1 Go to Manage > Standards.
2 In the table pane, navigate to the check for which you want to edit the CVE information. Select the check.
3 In the details pane, on the CVE tab, click the add (+) icon.
4 In the Add CVE dialog box, enter the CVE text that you want to add.
5 Click Add.
6 Click the save icon.
See “Working in the details pane” on page 648.
Editing the CVE information

You can edit the CVE information for a check through the details pane.

To edit the CVE information

1. Go to Manage > Standards.
2. In the table pane, navigate to the check for which you want to edit the CVE information. Select the check.
3. Select the CVE text that you want to edit and click the edit icon.
4. In the Edit CVE dialog box, enter the CVE text and click Update. Click the save icon.
5. To delete the CVE information, select the required text and click the delete icon. Click the save icon.

See “Working in the details pane” on page 648.

Specifying or editing the check attributes

You can specify or edit the risk attributes of a check through the details pane.

See “Check risk attributes” on page 584.

To specify or edit the risk attributes

1. Go to Manage > Standards.
2. In the table pane, navigate to the check for which you want to edit the risk attributes. Select the check.
3. In the details pane, on the General tab, select the values for the following:
   - Confidentiality
   - Integrity
   - Availability
   - Access Vector
   - Access Complexity
   - Authentication
4. Click the save icon.

See “Working in the details pane” on page 648.

Adding reference information

You can add reference information through the Reference tab in the details pane.
To add the reference information

1. Go to Manage > Standards.
2. In the Standards view, select the standard, section, or check for which you want to add the reference information.
3. In the details pane, on the References tab, click the add icon.
4. In the Add References window, in the Link Text box, type the name for the reference text.
5. In the Link box, type the URL path.
6. Click Add in the Add References window.
   The reference link information is added on the Reference tab.
7. Click the save icon.

See “Working in the details pane” on page 648.

Editing reference information

You can edit the reference information through the Reference tab in the details pane.

To edit the reference information

1. Go to Manage > Standards.
2. In the Standards view, select the standard, section, or check for which you want to edit the reference information.
3. In the details pane, on the References tab, select the reference that you want to edit.
4. Click the edit icon.
5. In the Edit References window, in the Link Text box, edit the name for the reference text.
6. In the Link box, edit the URL path.
7. Click Update.
   The reference is updated with the new information.
8. Click the save icon.

See “Working in the details pane” on page 648.
Deleting reference information

You can delete the reference information through the Reference tab in the details pane.

To delete the reference information

1. Go to Manage > Standards.
2. In the Standards view, select the standard, section, or check for which you want to add the reference information.
3. In the details pane, on the References tab, select the reference that you want to delete.
4. Click the delete icon.
5. In the Delete Row message box, click Yes to delete the selected reference link.
6. Click the save icon.

See “Working in the details pane” on page 648.

Working with Evaluation Results

The Evaluation Result Details dialog box lets you view the results of an evaluation job run.

When you select the Standard based view option in this dialog box, the following information is available:

- Asset Name
- Failed
- Check in Error
- Manual Review
- Not Applicable
- Passed
- Compliance %
- Risk Score
- Data Collection Date

When you select the Asset based view option in this dialog box, the following information for a check against a specific asset is available:

- Check name
- Status
You can perform the following tasks using the Evaluation Result Details dialog box:

- Export the evaluation results.
  See “Exporting the evaluation results” on page 655.

- Request exception on assets.
  See “Requesting an exception using the Evaluation Result Details dialog box” on page 656.

You can export the evaluation results either through the menu bar or the context menu.

**About exporting the evaluation results**

You can export the evaluation results that are available in the Evaluation Result Details dialog box.

The Evaluation Result Detail dialog box consists of three panes.

The top left pane lets you select the view that you want to display. Based on the view that you select, the relevant information is displayed in the other two panes.

The top right pane displays the summary of the evaluation results in the form of a pie chart.

The bottom pane displays the evaluation results in the form of data columns.

You can export the evaluation result details that are available in the bottom pane in either of the following ways:

- Export results using the menu bar
  You can use the menu bar to export the evaluation result details that pertain to both the Standard based view and the Asset based view.
However, for the Asset based view, you can export the results for only one asset at a time using the menu bar option. Also, you cannot export the evidence details information through this option. You can export the evaluation results in the following formats:

- Export results using the context menu
  You can use the context menu that is available when you right-click a particular asset to export all check information. This information includes the evidence details.
  Using the context menu options, you can export the evaluation results of multiple assets at a time but you can export only in the Excel format.

---

**Note:** You must have Excel installed on your computer to be able to export the evaluation results using the context menu.

---

The generated report layout is different for both the discussed options.

See “Exporting the evaluation results” on page 655.

### Exporting the evaluation results

You can export the evaluation results that are available in the Evaluation Result Details dialog box.

**To launch the Evaluation Result Details dialog box**

1. Go to Manage > Standards.
2. In the table pane of the Standard view, select the standard for which you want to view the evaluation results.
3. In the details pane, on the Evaluations tab, click the View Detail icon.
   The Evaluation Result Details dialog box is launched.

**To export the evaluation results using the menu bar for asset based view**

1. In the Evaluation Results dialog box, select **Asset based view**.
2. Select the asset for which you want to export the result.
3. On the File menu, select **Export to** and then select the format in which you want to export.
4. In the Export to dialog box, in the file name box, specify the name of the file where you want to save the evaluation results. Click **Save**.
To export the evaluation results using the menu bar for standard based view

1. In the Evaluation Results dialog box, select **Standard based view**.
2. Select the standard for which you want to export the result.
3. On the File menu, select **Export to** and then select the format in which you want to export.
4. In the Export to dialog box, in the file name box, specify the name of the file where you want to save the evaluation results. Click **Save**.

To export the evaluation results using the context menu

1. In the Evaluation Results dialog box, select **Asset based view**.
2. Select the assets for which you want to export the result, right-click, and select **Export Results**.
3. In the Save result as dialog box, in the file name box, specify the name of the file where you want to save the evaluation results. Click **Save**.

See “About exporting the evaluation results” on page 654.

Requesting an exception using the Evaluation Result Details dialog box

You can request an exception through the Evaluation Result Details dialog box.

**To launch the Evaluation Result Details dialog box**

1. Go to Manage > Standards.
2. In the table pane of the Standard view, select the standard for which you want to view the evaluation results.
3. In the details pane, on the Evaluations tab, click the View Detail icon. The Evaluation Result Details dialog box is launched.

**To request an exception from the standard-based view**

1. In the Evaluation Result Details dialog box, do either of the following.
   - Select Standard-based view.
   - Select Asset-based view. Go to step 3.
2. In the left pane, select a standard or a check. In the lower pane, select the assets that you want to exempt from the selected standard or check. Right-click the selected assets and select **Request Exception**. Go to step 4.
3 In the left pane, select an asset. In the lower pane, select the checks for which you want to exempt the selected asset. Right-click the selected checks and select Request Exception.

4 In the Request Exception wizard, in the Specify Exception Details panel, enter the title, description, and any attachment for the exception.

5 Enter the effective date and the expiration date. Click Next.

6 In the Select Checks and Assets panel, view the selected checks and assets. Click Next.

7 In the Specify Requestor Information panel, browse to enter the requestor and the requestor group information. Also, enter the requestor email ID and any comments.

8 In the Summary panel, view the details that you have specified. Click Back to make any changes and click Finish to exit the wizard.

Viewing the evidence details

You can view the evidence details for a check that has a failed, an error, or an unknown outcome.

To view the evidence details

1 In the Evaluation Result Details dialog box, select Asset based view.

2 Select an asset and then select the check for which you want to view the evidence.

3 Right-click the check and select Show Detailed Evidence.

About risk score calculation

The Control Compliance Suite follows the Common Vulnerabilities Scoring System (CVSS) version 2 to calculate the risk that is associated with a particular asset.

Control Compliance Suite performs the following calculations in the scoring process:

- Base score calculations
  See “Base score calculation” on page 658.

- Adjusted base score calculations
  See “Adjusted base score calculation” on page 658.

- Risk score calculations
  See “Risk score calculation” on page 659.
Base score calculation

The base score is calculated using the following attributes that are assigned to each check:

- Confidentiality Impact (C)
- Integrity Impact (I)
- Availability Impact (A)
- Access Vector (Av)
- Access Complexity (Ac)
- Authentication (Au)

See “Check risk attributes” on page 584.

The formula that is used to calculate the base score is as follows:

\[
\text{Base score} = \text{round}_\text{to}_\text{1}_\text{decimal} \left( \left( 0.6 \times \text{Impact} \right) + \left( 0.4 \times \text{Exploitability} \right) - 1.5 \right) \times f(\text{Impact})
\]

The Impact, Exploitability, and the \( f(\text{Impact}) \) values in the base score formula are calculated from the check attributes as follows:

\[
\text{Impact} = 10.41 \times \left( 1 - (1 - \text{Confidentiality Impact}) \times (1 - \text{Integrity Impact}) \times (1 - \text{Availability Impact}) \right)
\]

\[
\text{Exploitability} = 20 \times (\text{Access Vector}) \times (\text{Access Complexity}) \times (\text{Authentication})
\]

\[
f(\text{impact}) = 0 \text{ if Impact} = 0, f(\text{impact}) = 1.176 \text{ if Impact is not equal to 0.}
\]

The range of the base score values is from 0.0-10.0.

See “About risk score calculation” on page 657.

Adjusted base score calculation

The Adjusted base score is calculated for an asset and a check pair. This score is calculated using the attributes of the asset and the check.

The following formula is used to calculate the adjusted base score:

\[
\text{Adjusted base score} = \text{round}_\text{to}_\text{1}_\text{decimal} \left( \left( 0.6 \times \text{Adjusted Impact} \right) + \left( 0.4 \times \text{Exploitability} \right) - 1.5 \right) \times f(\text{Adjusted Impact})
\]

The Adjusted Impact, Exploitability, and the \( f(\text{Adjusted Impact}) \) values in the Adjusted base score formula are calculated as follows:
Adjusted Impact = min(10, 10.41 * (1- (1- Confidentiality Impact * Confidentiality Required) * (1-Integrity Impact * Integrity Required) * (1- Availability Impact * Availability Required)))

Exploitability = 20 * Access Vector * Access Complexity * Authentication

f(Adjusted impact) = 0 if Adjusted Impact = 0, f(impact) = 1.176 if Impact is not equal to 0.

The Adjusted base score values range from 0.0-10.0

See “About risk score calculation” on page 657.

Risk score calculation

The risk score term is applicable to an asset as well as to a standard.

For a given standard, the risk score of an asset is defined as the average of the adjusted base score of every failed check in the standard for the specific asset.

Risk score = (Total adjusted base score for all failed checks in the standard) / (Total number of failed checks)

See “Adjusted base score calculation” on page 658.

For example, consider an asset A and a standard S that contains five checks (C1, C2, C3, C4, and C5). When the asset A is evaluated against the standard S, only checks C4 and C5 are passed. The checks C1, C2, and C3 are failed.

To determine the risk score of asset A, calculate the adjusted base score of every failed check in the standard S with respect to asset A.

Assume that the following values are obtained:

Adjusted base score for check C1 with reference to asset A = 1
Adjusted base score for check C2 with reference to asset A = 2
Adjusted base score for check C3 with reference to asset A = 3

The average of the adjusted base score = (1 + 2 +3) / 3 = 2

This average adjusted base score value is the Risk score of the asset A with reference to a standard S.

See “About risk score calculation” on page 657.

Average risk score calculation

The Average risk score of an asset is calculated for all the standards against which the asset is evaluated. This score is the average of the individual risk scores of the asset for each of the standards against which the asset is evaluated.
Average risk score = (Total risk score for all standards) / (Total number of standards)

See “Risk score calculation” on page 659.

For example, consider an asset A that is evaluated against standards S1 and S2. Assume that the risk score of asset A for standard S1 is 3, and the risk score of asset A for standard S2 is 5.

The Average risk score = (3 + 5) / 2 = 4

See “About risk score calculation” on page 657.

About compliance score calculation

The Control Compliance Suite uses the following formulae to calculate the compliance score:

No. Of checks Passed / (Total number of checks – Not Applicable checks)

Compliance score of STD against an Asset = No. Of checks Passed / (Total number of checks – Not Applicable checks)

You can view the compliance score in the CCS Console at the following locations:

- General tab in the details pane of the Standards view
- General tab in the details pane of the Asset System view
- Evaluation tab in the details pane of the Standards view
- Evaluation tab in the details pane of the Asset System view
- Standards based view of the Evaluation Results dialog box
- Assets based view of the Evaluation Results dialog box
Remediating assets

This chapter includes the following topics:

- About remediation
- About automatic remediation
- About manual remediation
- About closed-loop verification
- Remediating the assets manually from the evaluation results
- Remediating the assets automatically

About remediation

Control Compliance Suite (CCS) provides a remediation feature that lets you identify the assets that are not in compliance. The remediation feature helps you resolve the issues that is caused by the non-compliance by sending the notification to the appropriate personnel. Remediation lets you specify the criteria to identify the non-compliant assets and then lets you choose the method of notification for the identified assets. You can either notify the appropriate personnel with a ServiceDesk ticket or with an email. The appropriate personnel resolves the issue and then closes the ticket.

You must configure the remediation settings to create the ServiceDesk tickets and to send email notifications.

See “Configuring the remediation settings” on page 176.

Control Compliance Suite provides a closed-loop verification feature where the assets that were remediated earlier are reevaluated for compliance. The closed-loop verification feature is available only when you select the ServiceDesk ticket method of notification.
About automatic remediation

Control Compliance Suite provides a feature to remediate the assets that are non-compliant. You can remediate the assets automatically or manually.

To automatically remediate the assets, you can schedule a specific remediation action as a part of the evaluation job or the collection-evaluation-reporting job. Automatic remediation immediately triggers a specified remediation action on the non-compliant assets that satisfy a specified criteria at the end of the job.

The automatic remediation works in the following way:

- Create a new evaluation job or a collection-evaluation-reporting job.
- Specify the evaluation job details.
- Enable automatic remediation and select the asset types.
- Specify remediation criteria.
- Select a remediation action.
- Schedule the evaluation job or the collection-evaluation-reporting job.
- Specify the notification details.

You must configure the remediation settings to create ServiceDesk tickets and to send email notifications for asset remediation. You can configure the settings from Settings > General > Application Configuration-Remediation Settings.

| Table 12-1 Remediation options |
| Option                  | Description                                                                 |
| ServiceDesk URL         | The hyperlink that is used to create ServiceDesk tickets for asset remediation. http://servername/WebServicename |
Table 12-1  Remediation options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS Web server</td>
<td>Name of the computer that hosts the Web server. The name can be specified in any format: computer name, IP address, or the fully qualified DNS.</td>
</tr>
<tr>
<td>Submitting contact</td>
<td>The email address from which the email notifications are sent for asset remediation.</td>
</tr>
<tr>
<td>Maximum assets per ticket</td>
<td>The Maximum number of assets that is included in a remediation ticket for each asset type. The default value is 20. The minimum value is 1.</td>
</tr>
</tbody>
</table>

See “Configuring the remediation settings” on page 176.

See “About remediation” on page 661.

See “Remediating the assets automatically” on page 667.

See “About manual remediation” on page 663.

About manual remediation

Control Compliance Suite provides a feature to remediate the assets that are non-compliant. You can remediate the assets automatically or manually.

To manually remediate the assets, you can select specific assets from the Evaluation Result Details dialog box and specify the remediation action.

The Evaluation Result Details dialog box can be launched from the Monitor > Evaluation Results view or from the Evaluations tab in the details pane of the Asset System view.

See “Remediating the assets manually from the evaluation results” on page 665.

The manual remediation works in the following way:

- Navigate to the evaluation results details dialog box.
- Select the remediate task.
- Select the asset types.
- Specify remediation criteria.
- Select remediation action.
Select the assets to perform the remediation action from the assets that match the criteria.

You must configure the remediation settings to create the ServiceDesk tickets and to send email notifications.

See “Configuring the remediation settings” on page 176.
See “About automatic remediation” on page 662.
See “About remediation” on page 661.

**About closed-loop verification**

The Control Compliance Suite provides the closed-loop verification feature where the assets once remediated are reevaluated for compliance. The closed-loop verification feature is available only for the ServiceDesk remediation action. The verification is optional and can be enabled at any time.

When an evaluation job identifies an asset that is out of compliance, a ServiceDesk ticket is opened, and then sent to the appropriate personnel to fix the issue. After the ticket is resolved, Control Compliance Suite recollects and reevaluates the asset data based on the original evaluation scope.

You must configure the remediation settings to create ServiceDesk tickets and to send email notifications for asset remediation. You can configure the settings from **Settings > General > Application Configuration - Remediation Settings**.

<table>
<thead>
<tr>
<th>Table 12-2</th>
<th>Remediation options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>ServiceDesk URL</td>
<td>The hyperlink that is used to create ServiceDesk tickets for asset remediation. <a href="http://servername/WebServicename">http://servername/WebServicename</a></td>
</tr>
<tr>
<td>CCS Web server</td>
<td>Name of the computer that hosts the Web server. The name can be specified in any format: computer name, IP address, or the fully qualified DNS.</td>
</tr>
<tr>
<td>Submitting contact</td>
<td>The email address from which the email notifications are sent for asset remediation.</td>
</tr>
<tr>
<td>Maximum assets per ticket</td>
<td>The Maximum number of assets that is included in a remediation ticket for each asset type. The default value is 20. The minimum value is 1.</td>
</tr>
</tbody>
</table>
You can view the remediation verification job status from the Manage > Jobs view. You cannot modify, schedule, or delete the job because the job is a system-job.

See “About remediation” on page 661.

See “Remediating the assets manually from the evaluation results” on page 665.

See “Remediating the assets automatically” on page 667.

See “Configuring the remediation settings” on page 176.

---

**Remediating the assets manually from the evaluation results**

You can remediate the assets using the Evaluation Result Details dialog box. Manual remediation involvesremediating the assets after you obtain the evaluation results.

After you evaluate the assets against standards, you receive the evaluation results and the risk score. You can now specify the criteria to identify the assets that require remediation and then take action to remediate. You can further choose specific assets from the list of assets that match the specified criteria. Remediation occurs only on the selected assets. The criteria can be the risk score or by compliance score or a combination of both the scores. You can choose to send email notifications or open service desk tickets for the assets that require remediation.

**To launch the Evaluation Result Details dialog box**

1. Go to Manage > Standards.
2. In the table pane of the Standards view, select the standard for which you want to view the evaluation results.
3. In the details pane, on the Evaluations tab, click the View Detail icon.
   
   or

4. Go to Monitor > Evaluation Results.

**To remediate the assets manually**

1. In the Evaluation Result Details dialog box, click Remediation Ticketing.
2. In the Select Asset Type for Remediation Ticketing panel, select the asset types that correspond to the assets that were evaluated and click Next.
3 In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

4 In the **Select Remediation Ticket Type** panel, select one of the following:

- Create an email notification.
  This option lets you create an email notification that you want to send for notification.

- Create a ServiceDesk ticket.
  This action opens a ServiceDesk ticket request directly at the end of the evaluation results for the non-compliant assets.

  You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the ServiceDesk request is met.

  See “**About closed-loop verification**” on page 664.

Click **Next**.

5 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the ServiceDesk ticket requests.

6 If you choose to create a ServiceDesk ticket as a remediation action, specify the message that you want to send as a ServiceDesk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single ServiceDesk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the ServiceDesk ticket requests.
In the Select Assets for Remediation Ticketing panel, select specific assets from the list of assets that is displayed in the panel. The list contains the assets that match the specified remediation criteria. You can further select specific assets from the filtered assets.

Click Next.

In the Summary panel, view the details that you specified. Click Back to make any changes and click Finish to exit the Remediating the assets automatically

You can remediate the assets as a part of the evaluation or the collection-evaluation-reporting job. Automatic remediation is scheduling the remediation of assets, as a sequential step, in the evaluation job.

You can configure the remediation details in the Create or Edit Evaluation Job Wizard and in the Create or Edit Collection-Evaluation-Reporting Job Wizard.

The panels to configure the remediation details in the Create or Edit Evaluation Job wizard appear after the Specify Notification Details panel.

You can also remediate the assets from the Assets view.

See “Running an evaluation job from the Asset System view” on page 383.

To remediating the assets automatically from the Standards view

1 Go to Manage > Standards.

2 Right-click the standard that you want to evaluate and select Run Evaluation or Run Collection-Evaluation-Reporting according to your requirement.

Provide the necessary information until you reach the Select Asset Type for Remediation Ticketing panel.

3 In the Select Asset Type for Remediation Ticketing panel, check the Enable Automatic Remediation Ticketing option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and then click Next.
In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

In the **Select Remediation Ticket Type** panel, select one of the following:

- **Create an email notification**.
  
  This option lets you create an email notification that you want to send for notification.

- **Create a ServiceDesk ticket**.
  
  This action opens a ServiceDesk ticket request directly at the end of the evaluation results for the non-compliant assets.
  
  You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the ServiceDesk request is met.
  
  See “About closed-loop verification” on page 664.

Click **Next**.

If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the ServiceDesk ticket requests.

If you choose to create a ServiceDesk ticket as a remediation action, specify the message that you want to send as a ServiceDesk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single ServiceDesk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the ServiceDesk ticket requests.

Proceed with the Create or Edit Evaluation Job Wizard or the Create or Edit Collection-Evaluation-Reporting Job Wizard.
Managing baselines

This chapter includes the following topics:

■ About baseline
■ About the baselines workflow
■ About the Baselines view
■ About setting tasks to roles of baselines
■ Creating a baseline job
■ Viewing the comparison results in the Baselines view
■ Exporting the comparison results
■ Deleting the baseline record

About baseline

A baseline is a reference data. You use the baseline feature to compare the asset data with a previous reference data or a previous reference job. In the Control Compliance Suite, when you run a baseline job, the records in the newer dataset are compared against the records in the older dataset.

Baselines let you compare the assets either with an asset that is marked as baseline or with a job-run that is marked as baseline.

Control Compliance Suite supports the following types of baselines:
Asset-based baseline
Control Compliance Suite lets you mark an asset as a baseline. You collect the data for an asset and use that data as a baseline to compare or monitor the assets in the further job runs.

The asset-based baseline lets you compare multiple assets of the same type with a single reference asset periodically.

Job-based baseline
Control Compliance Suite lets you mark the entire data that is collected by the baseline job as a baseline.

The job-based baseline serves the purpose of monitoring the same set of assets. When you create a baseline job and select a job-based baseline to compare against, the entire result data for the baseline job is compared.

See “Creating a baseline job” on page 672.

See “Viewing the comparison results in the Baselines view” on page 673.

About the baselines workflow
The end-to-end sequence of using the baselines is as follows:

■ Create a primary baseline job to mark the job run or an asset as a baseline.
  If you use the baseline feature for the first time, you create a baseline job and use the same job-run as a baseline. Or you create a baseline job and mark an asset from the job as a baseline.
  See “Creating a baseline job” on page 672.

■ Create subsequent baseline jobs to compare the results or the assets with the created baselines.
  You need to create baselines jobs to compare the assets with a job run or an asset that is marked as baseline.

■ View the comparison results
  You can view the results of the baseline job in the form of comparison with the baseline.
  See “Viewing the comparison results in the Baselines view” on page 673.
About the Baselines view

The baseline management view lets you manage the baselines in the Control Compliance Suite.

Note: To view the Baselines view, you should assign the View Baselines task explicitly to the user to manage the baselines.

You can access the baseline management view from Manage > Baseline.

You can perform the following tasks from the baseline management view:

- Delete a baseline.
  See “Deleting the baseline record” on page 675.
- View comparison results.
  See “Viewing the comparison results in the Baselines view” on page 673.

See “Creating a baseline job” on page 672.

About setting tasks to roles of baselines

To run the baselines job from the Jobs view, you must create a custom role that is configured to perform specific tasks. In Control Compliance Suite, you can create a custom role for the baselines system through the Settings > Role view of the console.

See “Creating a custom role” on page 110.

The following are the required baseline tasks that should be assigned to the user with the custom role for baselines:

- Manage baseline
- View baseline
- Compare baseline
- View comparison results

The following dependency tasks should be assigned to the user with the custom role for baselines:

- Manage jobs
- View assets
- View all jobs

See “Configuring roles and permissions” on page 95.
Creating a baseline job

You create a baseline job for one of the following purposes:

■ To mark the job or an asset as a baseline.
   If you use the baseline feature for the first time, you create a baseline job and use the same job-run as a baseline. Or you create a baseline job and mark an asset from the job as a baseline.

■ To compare the records with the previous baselines.
   You need to create baselines jobs to compare the assets with a job run or an asset that is marked as baseline.

You can create the baseline job for the assets for which the data collection and the evaluation is complete.

---

Note: To view the Baselines view, you must assign the View Baselines task explicitly to the user to manage the baselines.

---

To create a baseline job

1. Go to Monitor > Jobs and from the Common Tasks select, **Baseline Job**.
2. In the **Specify Job Name and Description** panel, type the name and the description for the baseline job and click **Next**.
3. In the **Compare with Baseline** panel do one of the following:
   ■ If you create the baseline job for the first time, click **Next**.
   ■ If you already have a baseline created, select **Compare with baseline** and select a baseline from the list.
      Click **Next** and go to step 5
4. In the **Select Platform, Asset Type, and Data Collector** panel, select the platform, the asset type, and the data collector for which the baseline data should be collected.
5. In the **Add Asset Scope** panel, browse through the available assets and add the assets to the baseline job.
   You can select one or more assets of the selected asset type as scope.
   Click **Next**.
6. In the **Select Fields** panel, select the fields for the asset type.
   The fields that you select in this panel are used to collect the relevant data for the selected asset type.
   Click **Next**.
7 In the Specify Asset Field Filters panel you can do one of the following:
   ■ Use the Edit Selected Statement option to edit the existing filter and click Next. Go to step 9
   ■ Use the Delete Selected Statement option to delete the existing filter and click Next. Go to step 9
   ■ Use the Add Statement option to create a new statement.
     The Add Statement option displays the Create Filter Statement dialog box. Go to step 9

8 In the Create Filter Statement dialog use the parameter type and the conditions to create a filter statement.
   See “Examples of asset filters” on page 292.
   See “Filter statement operators” on page 293.

9 In the Schedule panel, select any one of the following:
   ■ If you want to run the job after the wizard closes, check Run Now.
   ■ If you want to run the job at a specified interval, check Run Periodically and enter the following information:
     ■ In the Start On box, enter the start date and time to run the job.
     ■ Under Run periodically options, if you want to run the job only one time, select Run Once. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click Next.

10 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:
    ■ Type the subject and message of the notification mail.
    ■ Type the email ID of the sender and the receiver.

11 In the Summary panel, review the configurations for the baseline job and click Finish.
   You can go back to the previous panels and edit the configurations any time.
   You can go to the Monitor > Jobs view to monitor the current status of the job.

**Viewing the comparison results in the Baselines view**

You view the comparison results that are gathered from the baselines job in the Manage > Baselines view.
You can view the comparison results of the baseline job runs that are completed. You can view the comparison results of only one job-run at a time.

**To view the comparison results in the Baselines view:**

1. Go to Manage > Baselines.
2. In the table pane select a job run for which you want to view the comparison results.
3. From the taskbar, select **View Comparison Results**.
4. In the View Comparison Results dialog box, view the following details:

   - **Number of Assets**: Displays the total number of assets that are compared.
   - **Search**: Lets you search a particular asset.
     - **Note**: If you search an asset immediately after you launch the View Comparison Results dialog box, only the asset name are searched. After you perform any action in the View Comparison Results dialog box, the search applies to the entire baselined data.
   - **Details**: Displays the list of changed and unchanged assets.

See “Creating a baseline job” on page 672.

### Exporting the comparison results

You can export the comparison results to the following formats:

- Excel
- Word
- PDF
- XML
- CSV
To export the comparison results

1. In the View Comparison Results dialog box, go to File > Menu > Export to.
2. Select the format to which you want to export the comparison results.
3. In the Save In dialog box, type the file name by which the comparison results must be saved.

If you export the comparison results in the XML format and if the results contain linefeeds or other XML-specific characters, then use the IE or other XML rendering browser to view the results. In this case, the multi-valued fields are separated by space. In case, you use the default viewer as notepad the XML contains special characters that indicate newline.

Deleting the baseline record

You can delete the baseline from the Manage > Baselines view.

To delete the baseline

1. Go to Manage > Baselines.
2. Right-click the baseline record that you want to delete and select Delete.
Managing baselines

Deleting the baseline record
Managing tags

This chapter includes the following topics:

- About tags
- About the Tags view
- Creating a new tag
- Creating a new tag category
- Editing a tag category
- Deleting a tag category
- Moving a tag
- Deleting a tag
- Renaming a tag

About tags

Control Compliance Suite provides a method to tag and identify the business objects such as the assets, standards, the exceptions, the policies with respect to their severity, confidentiality, utility or any other area.

Tagging the assets is a way to apply meta-information to an asset. Tags help you identify the assets in some context that might prove helpful to determine the value of the asset. You can also use the tags to filter the assets.

For example, you can create a tag that is called SOX and associate it with a relevant asset.

See “Creating a new tag category” on page 678.
See “Creating a new tag” on page 678.
About the Tags view

You can access the tags management view from Manage > Tags.

The tags management view lets you perform the following tasks:

- Create Tag
- Rename Tag
- Delete Tags
- Move Tags

The tag categories are listed in the tree pane under the Tags node. You can create or edit a tag category using the right-click option from the tree pane. When you select a tag category in the tree pane, a list of tags under the selected category appears in the table pane.

See “About tags” on page 677.

Creating a new tag

You can access the Create Tag dialog box from Manage > Tags > Create Tag.

To create a new tag

1. Go to Manage > Tags.
2. In the tables pane, right-click the tag category under which you want to create a new tag and click Create Tag.
3. In the Create Tag dialog box, type the name of the new tag that should be created.
4. Click OK.

See “Creating a new tag category” on page 678.

See “Renaming a tag” on page 680.

See “Moving a tag” on page 680.

See “Deleting a tag” on page 680.

Creating a new tag category

You can create a new tag category from the tree pane.
To create a tag category
1. Right-click the Tags node in the tree pane.
2. Select Create Tag Category.
3. Type the name of the tag in the Name field.
4. Type the description for the tag category in the Description field.
5. Click OK.

See “Creating a new tag” on page 678.
See “Editing a tag category” on page 679.
See “Deleting a tag category” on page 679.

Editing a tag category
You can edit an existing tag category from the tree pane.

To edit a tag category
1. Right-click the category that should be edited under the Tags node in the tree pane.
2. Select Edit Tag Category.
3. Edit the Name and the Description fields in the Edit Tag Category dialog box.
4. Click OK.

See “Creating a new tag category” on page 678.
See “Deleting a tag category” on page 679.

Deleting a tag category
You can delete a tag category using the option in the menu bar.

To delete a tag
1. Select a tag category that you want to delete.
2. Select Delete tag category from the menu bar.
3. Select Yes in the confirmation dialog box to delete the tag.

See “Creating a new tag category” on page 678.
See “Editing a tag category” on page 679.
Moving a tag

You can move a tag using the option from the menu bar.

To move a tag

1. Select a tag that you want to move.
2. Select Move Tag from the Common Tasks.
3. In the Move selected tags to dialog box, select the tag category to which you want to move the tags.
4. Click OK.

See “Creating a new tag” on page 678.

See “Renaming a tag” on page 680.

See “Deleting a tag” on page 680.

Deleting a tag

You can delete a tag using the option in the menu bar.

To delete a tag

1. Select a tag that you want to delete.
2. Select Delete tag from the menu bar.
3. Select Yes in the confirmation dialog box to delete the tag.

See “Creating a new tag” on page 678.

See “Renaming a tag” on page 680.

See “Moving a tag” on page 680.

Renaming a tag

You can access the Rename Tag dialog from Manage > Tags > Rename Tags.

To rename a tag

1. Go to Manage > Tags.
2. In the tables pane, right-click the tag that you want to rename and select Rename tag.
3. In the Rename Tags dialog box, type a new name for the selected tag.
4. Click OK.
See “Creating a new tag” on page 678.
See “Moving a tag” on page 680.
See “Deleting a tag” on page 680.
Managing tags

Renaming a tag
Managing policies

This chapter includes the following topics:

- About policies
- About the Policies view
- Working with policies
- Reviewing and approving policies
- Publishing and unpublishing policies
- How audiences interact with policies
- Managing clarifications

About policies

Using the policies features of the Control Compliance Suite (CCS), you can manage, publish, and track your policies across the organization. You can also collect evidence of due care of policy compliance.

A policy is a formal statement of the practices, procedures, and codes of conduct employees should know and abide by in your business. Policies can include behaviors to comply with government regulations or the best practices specified by the standards bodies. They can also include behaviors specific to your enterprise. You use the policies features in the CCS to create and distribute policies.

In the CCS, all policies are mandates. Mandates are classed as either regulations or frameworks. Generally, regulations embody government regulations, while frameworks embody best practices. Your CCS installation may include one or more regulations or frameworks. In addition, you can use the Symantec Content Studio to create your own regulations and frameworks.
Policies are mapped to the control statements that in turn are mapped to regulations and frameworks. Mapping helps you to see the existing gaps in the current policies of your organization. These gaps can exist between your current policies and the mandates with which your organization must comply. Mapping also helps you to meet the requirements of the mandates with which the organization must comply.

See “About the policy life cycle” on page 684.
See “About policy status” on page 685.
See “What is a control statement?” on page 687.
See “About mapping policies” on page 688.

About the policy life cycle

Policies are rules established by an organization that are designed to guide their employees. In an IT environment, policies are used to guide the decisions that relate to the management of the IT infrastructure. Policies can map to one or many control statements.

A policy with no control statements can indicate an unimportant policy or a policy where compliance cannot be monitored. A control statement with no policy can indicate a gap showing noncompliance with one or more regulations.

The following tasks are typical of the life cycle of a policy:

- Create a new policy.
  See “Creating a new policy” on page 693.
- Review the policy.
  See “Reviewing a policy” on page 701.
- Approve the policy.
  See “Approving a policy” on page 703.
- Publish the policy.
  See “Publishing a policy” on page 704.
- See the Control Compliance Suite Web Console Help.
- Manage clarifications.
  See “Managing clarification requests” on page 708.

About policy versioning

Every policy has a version number assigned. The version number is assigned and incremented automatically during the policy life cycle. Most policy life cycle events are specific to a particular policy version number.
A policy version is independent of its position in the policy tree structure.

The version numbers are assigned and used based on the following policy states:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>When a policy is created, its status is Draft and the policy is assigned version number 1.</td>
</tr>
<tr>
<td>Review</td>
<td>When a policy is reviewed, the policy reviewer comments are specific to the current policy and the policy version. The reviewers are not allowed to edit their comments from the previous versions of the policy.</td>
</tr>
<tr>
<td>Approved</td>
<td>When a policy is approved, it is approved with the current version number.</td>
</tr>
<tr>
<td>Publish</td>
<td>When a policy is published, it is published with the current version number.</td>
</tr>
<tr>
<td>Unpublish</td>
<td>When a published policy is recalled or saved to update, the policy is automatically unpublished. When an unpublished policy is saved, the saved policy is marked as Draft and the version automatically increments by 1. For example, if version 2 of a policy is unpublished, the new version number is 3.</td>
</tr>
<tr>
<td>Awareness and clarification</td>
<td>When a user accepts, declines, or asks for a clarification, the task is specific to the current version.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>An exception to a policy is not specific to the version. For example, if an exception is approved for version 1 of a policy, then the same exception holds for version 2. The exception remains in place as long as the exception has not expired.</td>
</tr>
</tbody>
</table>

See “About policies” on page 683.

See “About the policy life cycle” on page 684.

See “About policy status” on page 685.

### About policy status

Every policy has a status that is assigned to it at all times.

The status is one of the following:
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft</td>
<td>A policy that is authored in its initial form. The policy has not been reviewed. The policy may or may not be complete in the view of the author. Also, a policy that has been reviewed but which has change requests, or a policy that has been unpublished. Policies can only be changed while in Draft status.</td>
</tr>
<tr>
<td>In Review</td>
<td>A policy in its first draft that is considered complete by the author. The policy is automatically submitted to the policy reviewers for their comments. Reviewer comments and change requests can be made while the policy is In Review.</td>
</tr>
<tr>
<td>Pending Approval</td>
<td>A policy that may or may not have reviewer comments. If a policy does not have change requests from reviewers, the status changes to Pending Approval. The status changes automatically when the review deadline that was set during the policy creation passes. If a policy does have change requests, its status reverts automatically to Draft when the review deadline passes. After the change requests are addressed, the author can submit it for review again.</td>
</tr>
<tr>
<td>Approved</td>
<td>A policy is Approved when the author has incorporated all the reviewer comments and is completely satisfied. A policy that is marked as Approved is ready for publication.</td>
</tr>
<tr>
<td>Published</td>
<td>A policy administrator with rights to the policy can publish an approved policy. A published policy is accessible to members of the audience from the Control Compliance Suite Web Console. The policy audience includes all the users assigned to the Policy Audience role in the CCS Console who also have permission to access the policy.</td>
</tr>
<tr>
<td>Archived</td>
<td>A policy that is archived and no longer in effect. An archived policy is not visible in the Policy view. Inactive policies are stored in the database.</td>
</tr>
</tbody>
</table>

**Note:** You must explicitly assign users to the **Policy Administrator**, **Policy Reviewers**, **Policy Approvers**, and **Policy Audience** roles. No users are assigned to these roles by default, including the **CCS Administrator**.

See “About policies” on page 683.
See “About the policy life cycle” on page 684.
See “About policy versioning” on page 684.
See “About policy approval” on page 702.
See “About policy review” on page 700.
About editing policies

Before a policy has been set to In Review, you can continue to make changes to the policy. You can make changes to all aspects of the policy, including the name and the content. Only the author name and the policy version cannot be changed manually.

After a policy has been approved or published, you can issue clarifications to a policy without additional review and approval.

To make changes to a published policy, you must unpublish it. You then make changes to the new policy version. The changed policy reverts to draft status and the version number increments.

All changes to an approved or published policy require the policy to be reviewed again, then approved and published.

See “Working with policies” on page 693.
See “About selecting the policy audience” on page 689.
See “Editing a policy” on page 696.
See “Deleting a policy” on page 697.
See “Moving, copying, and pasting a policy” on page 698.

What is a control statement?

A control statement is a concise statement of a discrete portion of a regulation or framework. Because regulations and frameworks have large areas of overlap, the control statements reduce repetition by stating each portion a single time. For example, where differences exist between regulation or framework statement requirements, a single control statement can exist to which each of the entries is mapped. Since both the regulation and the framework are mapped to the single control statement, the single control statement meets the requirements of both.

A control statement is mapped when it is linked to a policy. Control statements are also mapped to mandates. Through the control statement, the policy is indirectly linked to the regulation and the framework.

See “About mandates” on page 790.
See “About regulations” on page 790.
See “About frameworks” on page 791.
See “About standards” on page 550.
About mapping policies

Policy mapping is the process of linking policies to control statements. These control statements are themselves mapped to the frameworks and regulations that your enterprise must adhere to. The control statements express the behaviors that the Control Compliance Suite can monitor and report on.

You can use the Symantec Content Studio to map policies to control statements.

See “Creating custom content” on page 792.
See “Mapping policies to control statements” on page 797.

About policy reviewers

Any user who is assigned to the Policy Reviewer role who also has permission to access the policy is a policy reviewer for the policy. Every policy reviewer must review the policy before it can be approved. The policy reviewer can comment on policies or request a change before they agree with the statement of the policy.

Policy reviewers can use the Control Compliance Suite Console or the Control Compliance Suite Web Console to review policies.

The Control Compliance Suite notifies each affected policy reviewer when a policy is submitted for review.

See “About the policy life cycle” on page 684.
See “About policy review” on page 700.

About policy approvers

Any user who is assigned to the Policy Approver role who also has permission to access the policy is a policy Approver for the policy. A policy approver can approve and publish the policy when all reviewers have reviewed the policy and all change requests have been addressed. Policy approvers can use the Control Compliance Suite Console or the Control Compliance Suite Web Console to approve policies.

The Control Compliance Suite notifies each affected policy approver when a policy is submitted for approval.

See “About the policy life cycle” on page 684.

About the policy audience

A policy does not exist as a stand-alone entity. The policy relates to both your enterprise network and to the users of the network. The users that the policy affects make up the audience of the policy.
The audience consists of a group of people within an organization. The audience members are selected when a user creates a policy. Audience members become aware of the published policies applicable to them when they log on to the Control Compliance Suite Web Console. The policy administrator or security analyst is made aware of the user acceptance status of the policy. The manager or analyst responds to any exception request or clarification request that is submitted for the policy.

The users and the groups that are assigned to the **Policy Audience** role and also have permission to a policy make up the policy audience. The audience can consist of one or more users and groups.

You can use the Roles feature and Permission Management feature to assign users to the audience of a policy.

---

**Note:** Only a user who is assigned to the CCS Administrator role can assign roles and permissions.

---

See “Configuring roles and permissions” on page 95.
See “Adding users and groups to a role” on page 107.
See “Assigning permissions from the Roles view” on page 109.
See “Assigning permissions from the Permission Management view” on page 113.

---

**About selecting the policy audience**

The users and the groups that are assigned to the **Policy Audience** role with permission to a policy make up the policy audience. The audience can consist of one or more users and groups.

You use the Roles feature and Permission Management feature to assign users to the audience of a policy.

---

**Note:** Only a user that is assigned to the CCS Administrator role can assign roles and permissions.

---

See “Configuring roles and permissions” on page 95.
See “Adding users and groups to a role” on page 107.
See “Assigning permissions from the Roles view” on page 109.
See “Assigning permissions from the Permission Management view” on page 113.
About audience interaction with policies

When you create a policy, you can assign an audience to the policy.
The policy audience uses the Control Compliance Suite Web Console to do the following:

■ Accept the policy.
■ Decline the policy.
■ Request a clarification of the policy.
■ Request an exception to the policy.
■ Review the status of clarification and exception requests.
■ Review administrator responses to the clarification and exception requests.

When a policy is published, the Control Compliance Suite sends an email notification to the members of the policy audience. In addition, if an audience member requests a clarification, the Control Compliance Suite notifies the requestor when the policy administrator responds to the request.

See “About the policy audience” on page 688.

About the Policies view

The Policies view lets you manage the policies in the Control Compliance Suite. The Policies view displays a hierarchical tree structure of all policies. The Policies view lets you view the attributes of a selected policy or filter the displayed policies.

You can access the Policies view from Manage > Policies.

The Policies view contains the following panes:

Tree pane
This pane appears on the left side of the console window under the navigation bar.
This pane displays a hierarchical, folder-based structure of the policies that are stored in the CCS directory.

Filter by pane
This pane appears in the lower left side of the console window under the tree pane.
You can specify filters in this pane so that only the required policies are displayed in the table pane.

Table pane
The table pane appears in the right side of the console window under the taskbar.
This pane displays the policies.
Details pane

The details pane appears in the lower-right side of the console window under the table pane. This pane displays the details of the policy that is selected in the details pane.

You can perform the following tasks from the Policies view:

- Create a new policy.
- Import a Microsoft Word document as the basis for a new policy.
- View the details of an existing policy.
- Edit a policy.
- Copy a policy.
- Move a policy.
- Rename a policy.
- Delete a policy.
- Submit a policy for review.
- Submit a policy for approval.
- Approve a policy.
- Publish a policy.
- Unpublish a policy.

The details pane of the Policies view lets you review and edit policies. The details pane includes the following tabs:

General

The General tab includes the policy name, version, author, status, review by date, expiration date, priority level, and rationale.

Content

The Content tab contains the text of the policy. You can use formatting tools to edit the policy. You can also preview how the policy appears in a Web browser.

Targets

The Targets tab lists the Control Compliance Suite assets to which the policy applies. You can use the tab to add and remove assets for policies in the Draft state.
The 

**Statements** tab displays any control statements that are mapped to the policy. Control statements are mapped to the policy in the Content Studio tool. The **Statements** tab contains a link that lets you open the Content Studio.

See “About Symantec Content Studio” on page 789.

**Audience**

The **Audience** tab lists the users assigned to the Policy Audience role in Control Compliance Suite that have permissions to the policy.

**Approvers**

The **Approvers** tab lists the users who are assigned the Policy Approver role who also have permission to this policy. A policy must have at least one assigned approver. If no approver is assigned, the policy can never be set to **In Review**. Only approved policies can be published.

**Reviewers**

The **Reviewers** tab lists the users who are assigned to the Policy Reviewer role who also have permission to this policy. A policy must have at least one assigned reviewer. If no reviewer is assigned, the policy can never be set to **In Review**.

**Comments**

The **Comments** tab lets reviewers review the policy and create comments or change requests for the policy.

**Clarifications**

The **Clarifications** tab lets you review and respond to clarification requests for the policy by an audience member.

The **Clarifications** tab lists all the clarification requests that are submitted by the end users. By default, the requests are grouped based on status: Open or Closed. Use the sort, group, or filter feature to quickly access a specific policy clarification.

**Tags**

The **Tags** tab lets you review the tags that are assigned to the policy. You can also add tags to the policy and remove tags from the policy using this tab.

**Exceptions**

The **Exceptions** tab lists any exceptions that are granted to this policy. Use the **Exceptions Management** view to manage these exceptions.

See “About exceptions” on page 530.

See “About the exception management system” on page 530.

---

**Note:** Only a user who is assigned to the CCS Administrator role can assign roles and permissions.

---

**Note:** You must explicitly assign users to the **Policy Reviewers**, **Policy Approvers**, and **Policy Audience** roles. No users are assigned to these roles by default, including the **CCS Administrator**.
Working with policies

You must set up the policies that suit the needs of your enterprise. The Policies view lets you manage policies and their relationships.

You can do the following:

■ Create a policy.
   See “Creating a new policy” on page 693.

■ Import a Microsoft Word file as a policy.
   See “Importing a Word policy” on page 695.

■ Move, copy, or paste a policy.
   See “Moving, copying, and pasting a policy” on page 698.

■ Delete a policy.
   See “Deleting a policy” on page 697.

■ Select the policy audience.
   See “About selecting the policy audience” on page 689.

Creating a new policy

You can create a policy from the start or copy from an existing policy template. The asterisks (*) indicate that the fields are required.

To create a new policy

1 In the Policies view, navigate in the tree pane and click the folder where you want to store the new policy.

   You can only create a policy in a folder where you have appropriate rights.

2 Do one of the following:
   ■ Click New Policy.
   ■ Click Policy Tasks > New Policy.
   ■ Right-click the folder, then click New Policy.

3 In the Create New Policy panel, do one of the following:
■ Click **Create a New Policy** and then click **Next**.

■ Click **Create a Policy Based on a Predefined Policy**, then click the policy to base the new policy on and then click **Next**.

4 In the **Specify Policy Properties** panel, enter the following information and then click **Next**:

- **Policy Name**: The name of the new policy. A name is required.

- **Review By Date**: The date by which reviewers of the policy must submit comments. The default review by date is calculated based on the value that is set in System Management > General Settings > Policies Settings. You can select a different date.

- **Expiration Date**: The date the policy expires and is no longer valid. The default expiration date is calculated based on the value that is set in System Management > General Settings > Policies Settings. You can select a different date.

- **Priority Level**: The importance you assign to the policy. The default priority is low.

- **Allow User Response**: When this option is checked, the policy can be published to the Control Compliance Suite Web Console. Users can then read and respond to the policy.

  When unchecked, the policy can be published to the Control Compliance Suite Web Console. Users can request clarifications, but cannot accept or decline the policy or request an exception from the policy. From the user perspective, the policy is read-only.

- **Rationale**: The reason for the existence of the new policy. The rationale can be as comprehensive as your needs require. A rationale is required.

5 In the **Add Policy Content** panel, type the policy. You can use the formatting toolbars when you create the policy content.

See “Getting started with the asset system” on page 225.

Click **Next**.

6 In the **Choose Policy Targets** panel, locate the asset folders that are the targets of the policy. Click the targets and click **Add** or **Add All** to add the targets to the **Selected Items** list. Click **Next**.
7 In the **Summary** panel, review the properties of the new policy. If you need to change any properties, click **Back**. If you want to map control statements to the policy, ensure that **Launch Content Studio to map Control Statements** is checked.

See “**Mapping policies to control statements**” on page 797.

8 In the **Summary** panel, click **Finish**.

See “**Working with policies**” on page 693.

See “**About selecting the policy audience**” on page 689.

See “**Importing a Word policy**” on page 695.

### Importing a Word policy

You can import a Microsoft Word .doc file as a Control Compliance Suite policy. When you import a Word document, the name of the source Word document is assigned to the new Policy. You can manually change this name.

If the policy name already exists as a policy, the Control Compliance Suite prompts you to enter a new name for the policy. You must enter a new name to import the policy.

The text of the Word document is set as the content of the new policy.

When you import one or more Word documents, the following properties are explicitly set for the newly imported policies:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Same as the source Word document name</td>
</tr>
<tr>
<td>Policy content</td>
<td>Contents of the source Word document</td>
</tr>
<tr>
<td>Policy status</td>
<td>Draft</td>
</tr>
</tbody>
</table>

All other properties have their default values.

Before approving or publishing the new policy, you should make any necessary changes to the policy.

You must install Microsoft Word and the Microsoft Office Primary Interop Assembly on the same computer as your CCS client to import Word documents.

The Microsoft Office Primary Interop Assembly may or may not be installed, depending on the version of Microsoft Office and how it is installed.

Use one of the following URLs to download the correct version of the Microsoft Office Primary Interop Assembly for your Office version:
To import a Word policy

1. In the Policies view, navigate in the tree pane and click the folder where you want to store the new policy.

2. Do one of the following:
   - Click **Import Policies**.
   - Click **Policy Tasks > Import Policies**.
   - Right-click a folder in the tree, then click **Import Policies**.

3. Click **Next**.

4. In the **Select Word Documents** panel, click **Add**.

5. In the **Select Word Documents to Import** dialog box, click the Word .doc file to import, then click **Open**.

6. Repeat step 4 and step 5 to add additional Word files to import.
   - Click **Next** to continue when all files are added.

7. In the **Select a Target Folder** panel, click the folder into which the imported files should be saved, then click **Next**.

8. In the **Input Rationale** panel, enter the rationale for the imported policies.
   - Click **Next**.

9. In the **Completing the Import Policies Wizard** panel, review the choices you have made, then click **Finish**.

See “Working with policies” on page 693.

See “Creating a new policy” on page 693.

See “About selecting the policy audience” on page 689.

Editing a policy

You can use the Control Compliance Suite Console to make changes to a policy.

To make changes to a policy, the policy must be in the draft state.
To make changes to a policy that is in review, one or more policy reviewers must request changes to the policy. The change request forces the policy to return to the draft state when the **Review by** period expires. The policy version number does not change.

To make changes to a published policy, you must unpublish the policy. Unpublishing the policy changes the policy version number and puts the new version in the draft state. You can then review, approve, and publish the new version.

See “**About policy status**” on page 685.

See “**About policy versioning**” on page 684.

See “**Unpublishing a policy**” on page 705.

**To edit a policy**

1. In the Policies view, navigate in the tree pane and click the policy to select it. You can only edit a policy to which you have appropriate rights.

2. In the **Details** pane, make changes to the policy.

3. Do one of the following:
   - Click the **Save** icon to save your changes.
   - Click the **Revert** icon to discard your changes.
   - Select another policy, then click **Yes** when prompted to save the changes to the policy.
   - Select another policy, then click **No** when prompted to save the changes to the policy.

See “**About the policy life cycle**” on page 684.

See “**Working with policies**” on page 693.

See “**Deleting a policy**” on page 697.

**Deleting a policy**

If you decide not to proceed with a draft policy you may delete the policy.

**To delete a policy**

1. In the Policies view, do one of the following:
   - Right-click any policy in the Draft state and click **Delete Policies**.
In the table pane, click the check box beside one or more policies in the Draft state, then click **Policy Tasks > Delete Policies**.

2 In the **Delete Policies** dialog box, click **Yes**.

See “About the policy life cycle” on page 684.

See “About policy versioning” on page 684.

See “About policy status” on page 685.

See “Editing a policy” on page 696.

See “Moving, copying, and pasting a policy” on page 698.

---

### Moving, copying, and pasting a policy

When you create a policy, you may want to move it to another folder at a later time. To move a policy, you can use the move task or copy and paste the policy.

**To move a policy**

1 In the Policies view, do one of the following:
   - Right-click any policy and click **Move**.
   - In the table pane, click the check box beside one or more policies, then click **Policy Tasks > Move Policies**.

2 In the **Move Policies** dialog box, click the folder where the policies should move to, then click **OK**.

**To copy and paste a policy**

1 In the Policies view, right-click any policy and click **Copy**.

2 In the **Tree** pane, click the folder where you want to paste the policy.

3 In the Policies view, in the **Details** pane, right-click then click **Paste**.

See “Working with policies” on page 693.

See “Creating a new policy” on page 693.

See “Editing a policy” on page 696.

See “Deleting a policy” on page 697.

---

### Submitting a policy for review

After you have created a policy and it is ready for review, it must be submitted to the policy reviewers.
Note: Only the policies that you have permissions to in the folder selected in the tree pane can be submitted for review.

Note: You must explicitly assign users to the Policy Reviewers role. No users are assigned to this role by default, including the CCS Administrator.

To submit a policy for review

1. In the Policies view, click a folder in the tree pane, and do one of the following:
   - Click Submit Policy For Review
   - Click Workflow Tasks > Submit Policy For Review
   - Right-click an object in the tree, then click Submit Policy For Review

2. In the Submit Policy For Review dialog box, click the check box beside the name of the policies to submit for review, then click Submit.

See “About the policy life cycle” on page 684.
See “About policy status” on page 685.
See “Reviewing and approving policies” on page 700.
See “About policy review” on page 700.
See “Reviewing a policy” on page 701.
See “Viewing the reviewer comments” on page 702.

Submitting a policy for approval

After a policy has been reviewed, the policy is submitted for approval automatically when the review period expires. If you choose, you can manually submit the policy for approval after all reviewers have commented on it.

Note: Only the policies that you have permissions to in the folder selected in the tree pane can be submitted for approval.

Note: You must explicitly assign users to the Policy Reviewers role. No users are assigned to this role by default, including the CCS Administrator.

To submit a policy for approval

1. In the Policies view, click a folder in the tree pane, and do one of the following:
Click a policy in the details pane and then click **Submit Policy For Approval**

Click **Workflow Tasks > Submit Policy For Approval**

Right-click an object in the tree, then click **Submit Policy For Approval**

2 In the **Submit Policy For Approval** dialog box, click the check box beside the name of the policies to submit for review, then click **Submit**.

See “About the policy life cycle” on page 684.

See “About policy status” on page 685.

See “About policy approvers” on page 688.

See “Reviewing and approving policies” on page 700.

See “About policy approval” on page 702.

See “Approving a policy” on page 703.

### Reviewing and approving policies

Before it can be published, experts must review any policy for fitness, suitability, legal aspects, relevance, and other matters. Policy review lets you obtain those comments and retain the feedback through the life of the policy.

See “Submitting a policy for review” on page 698.

See “Submitting a policy for approval” on page 699.

See “Approving a policy” on page 703.

See “Reviewing a policy” on page 701.

See “Viewing the reviewer comments” on page 702.

### About policy review

The policy review feature assists reviewers by providing a central location to view and comment about the policies. Reviewers can also view other reviewer comments and refer to comments that are made in the previous versions of a policy.

When a policy is ready for review, the policy administrator marks the status as In Review. The Control Compliance Suite mails information about the policy to the reviewers. The reviewers view and comment about a policy using the Reviewer Comments tab of the policy details. When the review period expires, the policy state automatically changes. The policy administrator can also change the state manually if all reviewers have reviewed the policy. If a reviewer submitted a change request, the state reverts to **Draft**. The policy author views all the
comments and updates the policy if a reviewer submitted a change request. After
the author makes any required change, the author can submit the policy for review
again.

If no change request was submitted, the status changes to “Pending Approval.”

After a policy is approved or published or when the Review By date has passed, review comments are not editable. The original comments become part of the policy history. The policy history provides a record of the comments that led to a particular version of the policy.

Note: You must explicitly assign users to the Policy Reviewers role. No users are assigned to this role by default, including the CCS Administrator.

See “About the policy life cycle” on page 684.

See “About policy status” on page 685.

See “Submitting a policy for review” on page 698.

See “Reviewing and approving policies” on page 700.

See “Reviewing a policy” on page 701.

See “Viewing the reviewer comments” on page 702.

Reviewing a policy

To review a policy, you must have the required roles and permissions, and the policy status must be marked as In Review. After a policy is approved or published or when the Review By date has passed, review comments are not editable.

Note: Only a user that is assigned to the CCS Administrator role can assign roles and permissions.

Note: You must explicitly assign users to the Policy Reviewers role. No users are assigned to this role by default, including the CCS Administrator.

To review a policy

1. In the Policies view, select the policy to review.
2. In the details pane, click Comments.
3. In the Comments pane, click Add Comment.
4 In the **Reviewer Comment Details** dialog box, type your comments in the **My Comments** section. If the comment requests a change to the policy, click **Change Request**. If a change is requested, the policy status automatically changes to **Draft** when the review by date passes.

5 Click **OK**.

See “**About the policy life cycle**” on page 684.

See “**Submitting a policy for review**” on page 698.

See “**Reviewing and approving policies**” on page 700.

See “**About policy review**” on page 700.

See “**Viewing the reviewer comments**” on page 702.

---

### Viewing the reviewer comments

To view the review comments for a policy, you must have the required roles and permissions. In addition, the policy status must be marked as In Review.

---

**Note:** Only a user that is assigned to the CCS Administrator role can assign roles and permissions.

---

**Note:** You must explicitly assign users to the **Policy Reviewers** role. No users are assigned to this role by default, including the **CCS Administrator**.

---

**To view the reviewer comments for a policy**

1 In the Policies view, select the policy to review.

2 In the details pane, click **Comments**.

3 In the **Comments** pane, double-click the reviewer comment you want to read.

4 Click **OK**.

See “**About the policy life cycle**” on page 684.

See “**Reviewing and approving policies**” on page 700.

See “**About policy review**” on page 700.

See “**Viewing a policy**” on page 701.

---

### About policy approval

The policy approval feature helps you stage the release of your policies. All policies must be approved before they are eligible for publishing. You can centralize the
policy approval process, with authority to approve the policies granted to select users who are responsible for the policies.

The policy approvers must have both the Policy Approver role and permission to access the policy.

When a policy is ready for approval, the policy administrator marks the status as Reviewed. The Control Compliance Suite notifies the approver about the policy. The policy approver can use the Control Compliance Suite Console to approve the policy.

**Note:** You must explicitly assign users to the Policy Approvers role. No users are assigned to this role by default, including the CCS Administrator.

See “Approving a policy” on page 703.

See “About the policy life cycle” on page 684.

See “Submitting a policy for approval” on page 699.

See “Reviewing and approving policies” on page 700.

### Approving a policy

Before you can publish policies, they must be approved. Policies can only be approved after they have been reviewed. In addition, the policy review by date must be in the past. Policies can be rejected as well. A rejected policy returns to the draft state.

Exceptions can be approved for approved policies just as with published policies.

**Note:** Only the policies that you have permissions to in the folder selected in the tree pane can be approved.

**To approve or reject a policy**

1. In the Policies view, click a folder in the tree pane, and do one of the following:
   - Click **Approve Policy**
   - Click **Workflow Tasks > Approve Policy**
   - Right-click an object in the tree, then click **Approve Policy**

2. In the **Approve Policy** dialog box, click the check box beside the name of the policies to publish, then click **Approve** or **Reject**.

See “About the policy life cycle” on page 684.
Publishing and unpublishing policies

By publishing policies, you send approved policies to their respective audiences and make them accessible to members of the organization. Policies are viewable in the Control Compliance Suite Web Console. After a policy is created, reviewed, and approved, it is ready to be published to the selected audience members.

A policy can be published only if the status is marked as Approved. A policy that has expired cannot be published.

When a policy is published, the selected audience members can access the policy from the Control Compliance Suite Web Console. If you want to modify or update a published policy, you must first unpublish the policy. The policy is set to Draft status with a new version number. You can edit this new version. The published version of the policy cannot be modified.

When a policy is unpublished, the current version of the policy is archived and is no longer displayed in the Control Compliance Suite Web Console Policy page. The policy is available for future publication under a new version number.

See “About the policy life cycle” on page 684.
See “About policy versioning” on page 684.
See “About policy status” on page 685.
See “Publishing a policy” on page 704.
See “Unpublishing a policy” on page 705.

Publishing a policy

Only approved policies can be published.

When you publish policies, you transmit the policies to the policy audience in the Control Compliance Suite Web Console. Members of the audience can then accept or reject the policy. The audience members can also request exceptions to the policy or clarifications of the policy.

A policy can be published only if the status is marked as Approved. A policy that has expired cannot be published.

When a policy is published, the selected audience members can access the policy from the Control Compliance Suite Web Console.
Note: Only the policies that you have permissions to in the folder selected in the tree pane can be published.

To publish a policy

1. In the Policies view, click a folder in the tree pane, and do one of the following:
   - Click Workflow Tasks > Publish Policy.
   - Right-click an object in the tree, then click Publish Policy.

2. In the Publish Policy dialog box, click the check box beside the name of the policies to publish, then click Publish.

See “About the policy life cycle” on page 684.
See “About policy versioning” on page 684.
See “About policy status” on page 685.
See “Publishing and unpublishing policies” on page 704.
See “Unpublishing a policy” on page 705.

Unpublishing a policy

Only published policies can be unpublished. When you unpublish a policy, the policy is removed from the Control Compliance Suite Web Console. An unpublished policy is no longer accessible to the policy audience. The policy state changes to Archived. A new version of the policy is created with the Draft state.

Note: Only the policies to which you have permissions in the currently-selected folder selected in the tree pane can be unpublished.

To unpublish a policy

1. In the Policies view, click a folder in the tree pane, and do one of the following:
   - Click Workflow Tasks > Unpublish Policy.
   - Right-click an object in the tree, then click Unpublish Policy.

2. In the Unpublish Policy dialog box, click the check box beside the name of the policies to unpublish, then click Unpublish.

See “About the policy life cycle” on page 684.
See “About policy versioning” on page 684.
See “About policy status” on page 685.
See “Publishing and unpublishing policies” on page 704.
See “Publishing a policy” on page 704.

How audiences interact with policies

When you create a policy, you can assign an audience to the policy.
The policy audience uses the Control Compliance Suite Web Console to do the following:
■ Accept the policy.
■ Reject the policy.
■ Request a clarification of the policy.
■ Request an exception to the policy.
■ Review the status of clarification and exception requests.
When a policy is published, the Control Compliance Suite sends an email notification to the members of the policy audience. In addition, if an audience member requests a clarification, the Control Compliance Suite notifies the requestor when the policy administrator responds to the request.
For complete information about using the Web console, see the Control Compliance Suite Web Console Help.
See “About the policy audience” on page 688.

Managing clarifications

Clarifications let members of the policy audience request more information about a policy that they do not understand. Users can also request clarification for any policies which they may not be able to accept without further information. You manage clarifications in the policy clarifications view. You open the policy clarifications view by clicking Manage > Policies > Clarifications.
See “About clarifications” on page 706.
See “Managing clarification requests” on page 708.

About clarifications

The clarification feature lets members of the policy audience request any clarification on the policies that they have questions about, using the Control Compliance Suite Web Console home page. More than one clarification request can be made to a policy. Users can view the status of the clarification requests.
that they have made. When the policy administrator responds to the request, the user can view the response as well.

The following clarification statuses exist:

Open
A clarification request that is submitted, but for which no response exists

Closed
A policy administrator has responded

See “Managing clarifications” on page 706.
See “Managing clarification requests” on page 708.

About the Clarifications view

The Clarifications view lets you manage and respond to the policy clarification requests from users. The Clarifications view displays all policy clarification requests. The Clarifications view lets you view the attributes of a selected policy clarification or filter the displayed policy clarifications.

You can access the Clarifications view from Manage > Policies > Clarifications.

The Clarifications view contains the following panes:

Tree pane
The Tree pane appears on the left side of the console window under the navigation bar.

This pane is not used in the policy clarifications view.

Filter by pane
The Filter by pane appears in the lower left side of the console window under the tree pane.

You can specify filters in this pane so that only the required policy clarifications are displayed in the table pane.

Table pane
The Table pane appears in the right side of the console window under the taskbar.

This pane displays the policy clarifications.

Details pane
The Details pane appears in the lower-right side of the console window under the table pane.

This pane displays the details of the policy clarification that is selected in the table pane.

You can perform the following tasks from the Clarifications view:

- Review the policy clarifications.
Respond to policy clarifications.

See “Managing clarifications” on page 706.

See “About clarifications” on page 706.

See “Managing clarification requests” on page 708.

Managing clarification requests

You use the policy clarification view to view the clarification details or to respond to the clarification request.

To manage clarification requests

1. In the policy clarification view, select the clarification to manage.
2. Click Open Clarification.
3. The clarification editor displays the following information:

   - **Submitted**: Displays the date and time when the request was created.
   - **By**: Displays the name of the user who requested the clarification.
   - **Email**: Displays the email address of the user to send a notification to. The email address is optional.
     - If you send an email, you must configure the From email address in the Email Notifications tab in the General Settings.
     - See “Configuring the email Notification Server” on page 166.
   - **Details**: Displays the question that the user submitted regarding the policy.
   - **Due By**: Displays the date by when the policy administrator should send a response.
   - **Responded (date)**: Displays the date and time of the response.
   - **By**: Displays the account name of the policy administrator who responded to the request.
   - **Details**: Displays a text box where you can enter an explanation to the clarification that the user submitted.

4. Click OK to save.

   A notification is sent to the user if an email address is provided.

See “Managing clarifications” on page 706.
See “About clarifications” on page 706.
Managing clarifications
Monitoring jobs

This chapter includes the following topics:

■ About jobs
■ Managing jobs
■ Managing job runs
■ Viewing jobs information in the details pane

About jobs

A job is a specified set of operations. These operations are performed sequentially by various components of Control Compliance Suite. A job is also called a query with a scope. For example, a query with a scope in the form of assets in a particular domain is called a job. A job is uniquely defined.

When you execute a job, the particular instance of a job is called a job run. The job run is displayed when you expand a job in the table pane.

You can perform the following operations on jobs:

■ Create a job
  See “Creating jobs” on page 721.
■ Edit a job
  See “Editing a job” on page 717.
■ Run a job now
  See “Running a job now” on page 719.
■ Schedule a job
  See “Scheduling jobs” on page 718.
■ Delete a job
  See “Deleting jobs” on page 718.
■ Refresh the jobs view
  See “Refreshing the jobs view” on page 720.

■ Cancel a job run
  See “Canceling a job run” on page 722.

■ Delete a job run
  See “Deleting a job run” on page 723.

Select the job and use the right-click option to perform the stated operations. The menu options available at the right-click option are specific to the job type. You can select multiple jobs by using check boxes.

The stated options are also available on the taskbar and the menu bar under the Tasks menu. The tasks are enabled when the check box is checked.

You can even set up a job count. When you set up the job count, you can choose the number of jobs to be displayed in the Job view. These changes are made through the Settings > General Settings. Similarly, you can even set up a job run count.

To expand all the rows of jobs, press Ctrl + Right Arrow.

To collapse all the rows of jobs, press Ctrl + Left Arrow.

Control Compliance Suite does not support the following special characters in the job name:

* () \ / , + " > < ; = #

See “About using special characters in folder and job names” on page 71.

See “About the job types” on page 712.

See “About the job filters” on page 714.

About the job types

The jobs that are automatically created by Control Compliance Suite are known as System jobs. The System jobs perform certain predefined functions. Some of the System jobs may be hidden.

The jobs that are created by the user are known as user-defined jobs.

Control Compliance Suite contains the following job types:
<table>
<thead>
<tr>
<th>Job Type</th>
<th>Description</th>
<th>Related Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset import job</td>
<td>The Asset import job imports assets. You can also add assets in the hierarchy through the job, which helps you to manage the assets. See “Importing asset-specific fields from the default data collector” on page 329. See “Importing asset-specific and common fields using the CSV data collector” on page 335.</td>
<td></td>
</tr>
<tr>
<td>Baseline job</td>
<td>Initially, the Baseline job is the same as the data collection job, as it collects data based on the query. Then a job run of this job is marked as a baseline. You can compare another job run with the job run that is marked as a baseline. Similarly, you can compare two types of assets. See “Creating a baseline job” on page 672.</td>
<td></td>
</tr>
<tr>
<td>Entitlements import job</td>
<td>The Entitlements import job fetches the entitlements for a particular control point. See “Importing the entitlements manually” on page 511.</td>
<td></td>
</tr>
<tr>
<td>Automatic entitlements import job</td>
<td>The Automatic entitlements import job is created during installation. This job fetches the entitlements for the import-required control points. See “Configuring the automatic entitlements import” on page 510.</td>
<td></td>
</tr>
<tr>
<td>Evidence collection job</td>
<td>The Evidence collection job imports third-party evidence data.</td>
<td></td>
</tr>
<tr>
<td>Tiered dashboard update job</td>
<td>The Tiered dashboard update job updates an existing Tiered dashboard through the Edit Tiered Dashboards wizard.</td>
<td></td>
</tr>
<tr>
<td>Reporting database synchronization job</td>
<td>The Report data synchronization job synchronizes between the production database and the reporting database.</td>
<td></td>
</tr>
<tr>
<td>Report data purge job</td>
<td>The Report data purge job purges data from the reporting database.</td>
<td></td>
</tr>
</tbody>
</table>
### Evaluation job
The Evaluation job evaluates a standard or a set of standards against the assets or the assets group, or the assets folder.

See “Running an evaluation job from the Standards view” on page 607.

Data collection must be performed before running an Evaluation Job.

See “About remediation” on page 661.

### Data collection job
The Data collection job collects required data for a standard or a set of standard. The job collects the data against the assets or the assets group, or the assets folder.

See “Setting up a data collection job from the Standards view” on page 609.

### Collection-Evaluation-Reporting job
The collection-evaluation-reporting lets you create a chained job to collect data for a set of assets, to evaluate the assets, and to generate reports for those assets.

You can also schedule to remediate the assets automatically at the end of the evaluation.

See “Running a collection-evaluation-reporting job from the Standards view” on page 612.

### Remediation verification job
The remediation verification job is a system job.

The remediation verification job recollects and reevaluates the asset data after the remediation action is taken on the assets. This job appears only if you enable the closed-loop remediation.

### Policy and Mandates metrics computation job
The Policy and Mandates metrics computation job is a system job.

The Policy and Mandates metrics computation job computes policy and mandate specific rollups for use by the dashboards displayed on the Web console. The job also computes metrics for Symantec Data Loss Prevention dashboard panels.

See “About jobs” on page 711.

See “Creating jobs” on page 721.

### About the job filters
The Filter by pane at the left in the Jobs view shows numerous filters. You can use these filters to display the required jobs. If none of the job type is selected then jobs of all job types are shown.

Control Compliance Suite provides the following default filters for filtering the jobs:
Job Type

Let you filter the jobs according to the type of the job.

The following types of jobs can be filtered:

- Asset import job
- Baseline job
- Entitlements import job
- Automatic entitlements import job
- Evidence collection job
- Report generation job
- Report data synchronization job
- Report data purge job
- Tiered dashboard update job
- Evaluation job
- Data collection job
- Collection-Evaluation-Reporting job
- Remediation verification job
- Policy and Mandates metrics computation job

Last Run Date

Let you filter the jobs according to the last completed job run date or time.

You can select one of the following options:

- Any
- Before
- After
- Between

Select the filter and click update to view the jobs in the table pane.

See “About jobs” on page 711.

See “About the job types” on page 712.

See “Customizing the filter options” on page 67.

About the Jobs view

The Jobs view is used to view all the jobs that are created in Control Compliance Suite.

You can access the Jobs view from Monitor > Jobs.

Manage Jobs and View all Jobs permissions are needed to navigate to jobs view.

The jobs view displays the following three panes:
Table pane  The table pane displays the list of the jobs. When you expand the jobs, you can view the job run.

Details pane  The details pane displays the details of the job. When you select the job in the table pane, the job details are displayed in the details pane.

Filter by pane  The filter by pane is used to filter the jobs. When you set the filters and update, the jobs are listed in the table pane.

The taskbar of the Jobs view is divided into the following major tasks:

Common Tasks

<table>
<thead>
<tr>
<th>Job Tasks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Run job now</td>
<td>See “Running a job now” on page 719.</td>
</tr>
<tr>
<td>- Refresh selected job</td>
<td>See “Refreshing the jobs view” on page 720.</td>
</tr>
<tr>
<td>- Delete job</td>
<td>See “Deleting jobs” on page 718.</td>
</tr>
<tr>
<td>- Edit job</td>
<td>See “Editing a job” on page 717.</td>
</tr>
<tr>
<td>- Schedule job</td>
<td>See “Scheduling jobs” on page 718.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Job Run Tasks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cancel job run</td>
<td>See “Canceling a job run” on page 722.</td>
</tr>
<tr>
<td>- Delete job runs</td>
<td>See “Deleting a job run” on page 723. See “Manual review” on page 295.</td>
</tr>
</tbody>
</table>

You can search for a job through the Jobs view.

See “Searching for a job” on page 720.

See “About jobs” on page 711.

See “About the job filters” on page 714.

See “Viewing jobs information in the details pane” on page 724.

Managing jobs

You can perform the following operations in the Jobs view:

| Create jobs | See “Creating jobs” on page 721. |
■ Edit a job
  See “Editing a job” on page 717.
■ Run a job now
  See “Running a job now” on page 719.
■ Schedule a job
  See “Scheduling jobs” on page 718.
■ Delete a job
  See “Deleting jobs” on page 718.
■ Refresh the jobs view
  See “Refreshing the jobs view” on page 720.
■ Search for a job
  See “Searching for a job” on page 720.

Editing a job

You can edit a job by using the right-click menu option available at the job. You can even edit the jobs by using the taskbar and the Tasks menu.

You can edit only one job at a time. Each job type has unique edit options. You can only edit user-defined jobs. The user who has created the job and the CCS administrator can edit the job.

To edit jobs

1  In the Monitor > Job view, select the job.
2  Right-click and select Edit Job.
3  In the wizard of the respective job, make the required changes. Complete the wizard. The job is edited.

See “About jobs” on page 711.
See “Scheduling jobs” on page 718.
See “Deleting jobs” on page 718.
See “Running a job now” on page 719.
See “Canceling a job run” on page 722.
See “Searching for a job” on page 720.
See “Refreshing the jobs view” on page 720.
See “Deleting a job run” on page 723.
See “Creating jobs” on page 721.
Scheduling jobs

You can schedule a job by using the right-click menu option available at the job. You can even schedule the jobs by using the taskbar and the **Tasks** menu.

You can schedule only one job at a time.

**To schedule a job**

1. In the **Monitor > Job** view, select the job.
2. Right-click and select **Schedule Job**.
3. In the Schedule dialog box, select either or both of the following:
   - If you want to run the job now, check **Run Now**.
   - If you want to run the job at a specified interval, check **Run Periodically** and enter the following information:
     - In the Start On box, enter the start date and time to run the job.
     - Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box.
4. Click **OK**.

See “About jobs” on page 711.

See “Editing a job” on page 717.

See “Deleting jobs” on page 718.

See “Running a job now” on page 719.

See “Canceling a job run” on page 722.

See “Searching for a job” on page 720.

See “Refreshing the jobs view” on page 720.

See “Deleting a job run” on page 723.

See “Creating jobs” on page 721.

Deleting jobs

You can delete a job by using the right-click menu option available at the job. You can even delete the jobs by using the taskbar and the **Tasks** menu.

You can delete multiple jobs. You can delete only the user-defined jobs.
To delete a job

1. In the **Monitor > Job** view, select the job.
2. Right-click and select **Delete Job**. In the confirmation message, click **Yes** and the job is deleted.

See “About jobs” on page 711.

See “Editing a job” on page 717.

See “Scheduling jobs” on page 718.

See “Running a job now” on page 719.

See “Canceling a job run” on page 722.

See “Searching for a job” on page 720.

See “Refreshing the jobs view” on page 720.

See “Deleting a job run” on page 723.

See “Creating jobs” on page 721.

---

Running a job now

You can run a job by using the right-click menu option available at the job. You can even run the jobs by using the taskbar and the **Tasks** menu.

**To run a job now**

1. In the **Monitor > Job** view, select the job.
2. Right-click and select **Run Job Now**. A corresponding Job run is created and the job starts to run. The column Last Run Status displays the last run status of the job. The column Last Run Date displays the timestamp of the last completed job run.

See “About jobs” on page 711.

See “Editing a job” on page 717.

See “Scheduling jobs” on page 718.

See “Deleting jobs” on page 718.

See “Canceling a job run” on page 722.

See “Searching for a job” on page 720.

See “Refreshing the jobs view” on page 720.

See “Deleting a job run” on page 723.

See “Creating jobs” on page 721.
Searching for a job

You can use the Search box to search for a job. You can even search by any of the columns. For example, you can type Failed and see the job runs with the Failed status.

You can even use the Filter by pane to filter the jobs. Search is performed only on the records visible in User Interface.

To search for a job

1. In the Monitor > Job view, type the name of the job in the Search box available in the table pane.
2. Click the search icon. The jobs are listed in the table pane.

See “About jobs” on page 711.
See “Editing a job” on page 717.
See “Scheduling jobs” on page 718.
See “Deleting jobs” on page 718.
See “Running a job now” on page 719.
See “Canceling a job run” on page 722.
See “Refreshing the jobs view” on page 720.
See “Deleting a job run” on page 723.
See “Creating jobs” on page 721.

Refreshing the jobs view

You can refresh the jobs view or the selected jobs.

To see the current status of the job or the job run, you can perform the refresh option manually.

To refresh the whole view, you can press F5.

To refresh a specific job

1. Select the job that you want to refresh.
2. Do one of the following:
   - On the Tasks menu, point to Job Tasks and then select Refresh Selected Job.
   - Right-click the selected job and select Refresh Selected Job.
   - On the taskbar, select Refresh Selected Job.
Creating jobs

You can create few jobs from the jobs view by using the right-click option in the table pane. You can even create the jobs through the Tasks bar.

You can create the following jobs from the jobs view:

■ Baseline job
  See “Creating a baseline job” on page 672.

■ Evaluation job
  See “Running an evaluation job from the Standards view” on page 607.

■ Data collection job
  See “Setting up a data collection job from the Standards view” on page 609.

■ Entitlements import job
  See “Importing the entitlements manually” on page 511.

■ Import assets job
  See “Importing asset-specific and common fields using the CSV data collector” on page 335.
  See “Importing asset-specific fields from the default data collector” on page 329.

To create a job from the jobs view

1. In the Monitor > Job view, right-click in the empty grid in the table pane and select the job that you want to create.
   The wizard that is associated with the respective job is launched.

2. Complete the wizard to create the job.

See “About jobs” on page 711.
See “Editing a job” on page 717.
Managing job runs

You can perform the following operations on job runs:

▪ Cancel a job run
  See “Canceling a job run” on page 722.

▪ Delete a job run
  See “Deleting a job run” on page 723.
  See “Manual review” on page 295.

Canceling a job run

You can cancel a job run by using the right-click menu option available at the job run. You can even cancel the job run by using the taskbar and the Tasks menu.

You can simultaneously cancel job runs of the same type. Job runs of the same type that belong to different jobs can also be canceled.

For example, if you select two asset import job runs, the cancel option is enabled. If you select asset import job run and data collection job run for cancelation, then the cancel option is disabled. These job runs are not canceled because the jobs are not of the same type.

You can cancel Job runs in Executing states.

You cannot cancel Job runs in the following states:

▪ Aborted
▪ Complete
▪ Faulted
▪ Custom
To cancel a job run

1. In the **Monitor > Job** view, expand the job container under which the job run resides.
2. Select the job run you want to cancel, right-click, and then click **Cancel Job**. The job run is canceled.

See “About jobs” on page 711.
See “Editing a job” on page 717.
See “Scheduling jobs” on page 718.
See “Deleting jobs” on page 718.
See “Running a job now” on page 719.
See “Searching for a job” on page 720.
See “Refreshing the jobs view” on page 720.
See “Deleting a job run” on page 723.
See “Creating jobs” on page 721.

Deleting a job run

You can delete a job run by using the right-click menu option that is available at the job run. You can even delete the job runs by using the taskbar and the **Tasks** menu.

You can delete only the job runs in completed, aborted, and faulted states.

To delete a job run

1. In the **Monitor > Job** view, expand the job in the table pane.
2. Select the job run, right-click, and select **DeleteJobRun**. The job run is deleted.

See “About jobs” on page 711.
See “Editing a job” on page 717.
See “Scheduling jobs” on page 718.
See “Deleting jobs” on page 718.
See “Running a job now” on page 719.
See “Canceling a job run” on page 722.
See “Searching for a job” on page 720.
See “Refreshing the jobs view” on page 720.
See “Creating jobs” on page 721.
Viewing jobs information in the details pane

You can view the information about the jobs through the details pane. The details pane displays all the information about the selected job or the job run in the following tabs:

- General tab
  See “Jobs details pane- General tab” on page 724.

- Schedule tab
  See “Jobs details pane- Schedule tab” on page 725.

- Wizard Summary tab
  See “Jobs details pane - Wizard Summary” on page 725.

- Summary tab
  See “Job run details pane- Summary tab” on page 725.

- Failures tab
  See “Job run details pane- Failures tab” on page 725.

- Templates tab
  See “Jobs details pane- Template tab” on page 725.

To view jobs information

1. In the Monitor > Jobs view, select the job or the job run in the table pane for which you want to view the information.

2. View the information for the selected job or the job run in the details pane.

Jobs details pane- General tab

The General tab of the Jobs details pane provides general information about the selected job. The information in this tab is read-only.

The General tab contains the following details about the jobs:

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job type</td>
<td>Displays the job type</td>
</tr>
<tr>
<td>Created by</td>
<td>Displays the identity of who has created the job</td>
</tr>
<tr>
<td>Next run date</td>
<td>Displays the date and the time when the job runs next</td>
</tr>
<tr>
<td>Created on</td>
<td>Displays the date and the time when the job was created</td>
</tr>
<tr>
<td>Last run status</td>
<td>Displays the status of the latest job run</td>
</tr>
<tr>
<td>Last run date</td>
<td>Displays the last completed job run date and time</td>
</tr>
</tbody>
</table>
Jobs details pane - Schedule tab

The Schedule tab of the Jobs details pane provides information about the scheduling of the selected job. The information in this tab is read-only.

The Schedule tab contains the following details about the jobs:

- **Run on**: Displays the date and time for the job to run or displays the next job execution time.
- **Recurring**: Displays the status for a recurring job.
- **Run every**: Displays the duration between two scheduled runs.

Jobs details pane - Wizard Summary

This tab shows the configuration details of the job. The data that is displayed in this tab varies with the job type.

Job run details pane - Summary tab

The Summary tab provides details about the selected job run. The information that is displayed in the tab pertains to the type of the job. The information in this tab is read-only.

Job run details pane - Failures tab

The Failures tab provides information about the data collector errors of the selected job run. The information in this tab is read-only.

The Failure Details column of the job run in the tables pane displays the details about other errors.

You can launch a new window that displays the errors. The Job Run error window provides information about the data collector errors of the selected job run. The information in this window is read-only. You can export the grid to the desired location with the desired file format.

Jobs details pane - Template tab

The Template tab of the Jobs details pane specifies the template that is used for creating the report. The information in this tab is read-only.
The **Template** tab contains the following information of the report:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report title</td>
<td>Displays the name of the report</td>
</tr>
<tr>
<td>Report type</td>
<td>Displays the type of report</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description of the report</td>
</tr>
<tr>
<td>Author</td>
<td>Displays the name of the author of the report</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the version of the report</td>
</tr>
</tbody>
</table>
Monitoring evaluation results

This chapter includes the following topics:

- About the Evaluation Results view
- About the evaluation result filters
- Viewing evaluation jobs in the details pane

About the Evaluation Results view

The Evaluation Results view is used to view the details of each evaluation job run. For example, assume that you have evaluation jobs A and B. You run the job A two times and the job B three times. The Evaluation Results view lists the details of each job run. In this case, job A is listed twice and job B is listed three times.

Note: You must have the Standard Administrator or Standard Evaluator role to view the evaluation results.

The Evaluation Results view displays content in the following panes:

- **Tables pane**: Lists each instance of the job run for all the evaluation jobs.
- **Details pane**: Provides the details of each evaluation job run.
- **Filter by pane**: Provides the filters to display only selected evaluation jobs in the table pane.

See “Evaluation Results details pane - General tab” on page 729.
See “Evaluation Results details pane - Evaluation Summary tab” on page 729.

See “Evaluation Results details pane - Assets Evaluated tab” on page 729.

About the evaluation result filters

The filter by pane contains the Last Run Date filter that you can use to display only the required evaluation jobs.

The Last Run Date filter contains the following options for filtering the evaluation jobs:

- **All**: Lists all the evaluation jobs.
- **Last One Day**: Lists all the evaluation jobs that were run during the last one day.
- **Last One Week**: Lists all the evaluation jobs that were run during the last one week.
- **Last One Month**: Lists all the evaluation jobs that were run during the last one month.
- **Between** and **And**: Lists all the evaluation jobs that were run during a specific time period. Provide the start date and time in the Between box. Provide the end date and time in the And box.

The time that is used to calculate the specified options is 12:00 am.

For example, consider that on 23 Aug 2008 at 4:00 p.m. you select the Last One Day option for filtering the jobs. Then all the jobs that were run from 22 Aug 2008 (at 12:00 a.m.) to 23 Aug 008 (at 4:00 p.m.) are displayed.

Viewing evaluation jobs in the details pane

You can view the information about an evaluation job through the details pane of the Evaluation Results view.

**To view the evaluation job information**

1. In the table pane, select the evaluation job for which you want to display the information.
2. View the information for the selected evaluation job in the details pane.

   The evaluation job details are contained in the following tabs:
■ General
  See “Evaluation Results details pane - General tab” on page 729.

■ Evaluation Summary
  See “Evaluation Results details pane - Evaluation Summary tab” on page 729.

■ Assets Evaluated
  See “Evaluation Results details pane - Assets Evaluated tab” on page 729.

See “About the details pane” on page 62.

Evaluation Results details pane - General tab

The General tab of the Evaluation Results details pane provides general information about the selected evaluation job.

The General tab contains the following information:

- Name  The name of the evaluation job. This value is editable.
- Description  The description of the evaluation job.
- Evaluation Date  The date when the job was evaluated.
- Submitted by  The user name of the user who submitted the job.

Evaluation Results details pane - Evaluation Summary tab

The Evaluation Summary tab of the Evaluation Results details pane provides information about the standards that were evaluated in the evaluation job.

The Evaluation Summary tab contains the following information:

- Name  Lists the name of the standards that were evaluated in the evaluation job.
- Version  Lists the version of the standards.
- Risk Score  Lists the risk score of the standard.
- Compliance Score  Lists the compliance score of the standard.

Evaluation Results details pane - Assets Evaluated tab

The Assets Evaluated tab of the Evaluation Results details pane provides information about the assets that are evaluated in the evaluation job. This tab contains a list of the names of the assets that were evaluated.
Monitoring evaluation results

Viewing evaluation jobs in the details pane
Managing reports and dashboards

This chapter includes the following topics:

- About the reports and dashboards
- Working with reports
- Working with tiered dashboards

About the reports and dashboards

Control Compliance Suite (CCS) provides a rich set of presentation-level reports. A report lets you collect and present the data in a format that conforms to the organizational needs. A report is a business document that contains a predefined, organized collection of data. A report can be viewed, printed, or analyzed. You can create and customize reports from the Reporting view. You can schedule the report generation or dashboard update jobs from the Jobs view. You can schedule reports and dashboard jobs to run at a specified time. If the report supports the feature, you can export a report in several formats. Dashboards that are created in the Web Console are real-time, visual representations of selected key elements for an organization. Dashboards that are created in the Web Console are not scheduled.

Organizations collect vast amounts of information in the course of completing business transactions. Management studies the data to make decisions. The Reporting feature gives you the timely information that you need to make informed decisions about the organization.

The reporting database stores the data that is needed for the reports and dashboards.
About the Reports Templates view

The Reports Templates view lists the report templates that you can access. The Reports folder has the Predefined subfolder. You can create a user-defined subfolder to store the customized report templates. You can copy the predefined templates to the user-defined folder. If the report template supports the feature, you can customize the predefined report template.

The Report Templates view has the following panes:

- Folder
- Filter by
- Table
- Details

In the folder pane, you can do the following:

- Add user-defined subfolders
- Select a folder to view the report templates in the table pane

In the Filter by pane, you can do the following:

- Create a report type filter.
- Create a tag filter.

In the table pane, you can do the following:

- Schedule a selected template
- Copy and paste a predefined template to the user-defined folder
- Customize a report template, if the report template supports the feature
- Apply a filter to the template list
- View the name, description, and version number of each report template
- Verify if a report supports customization and can be generated using the chained job
- In a user-defined folder, you can delete a report template
- Add or update a report template
- Export a report template
Move a report template

In the details pane > General tab, you can view the following information about a selected report template:

- Report title
- Report type
- Description
- Author
- Version

In the details pane > Tags tab, you can add a tag to a report.

- Add a tag.
- Remove a tag.

See “Copying a report template” on page 750.
See “Customizing a report template” on page 750.
See “Deleting a user-defined report template” on page 753.
See “About the Reporting view” on page 65.
See “Exporting a report” on page 749.
See “Adding a user-defined report template” on page 752.
See “Updating a report template” on page 754.
See “Exporting a report template” on page 753.
See “Moving a report template” on page 755.

About the My Reports view

The My Reports view lists the successful report runs that you can access. The view displays only the successful report runs. These reports are only accessible by the user who created the report. The Report Viewer role can only see reports in the My Reports view.

Members of the CCS Administrators role cannot remove a report. If you are assigned as a viewer for the report, you can remove the report from the My Reports view.

The My Reports view has the following panes:

- Filter by
- Table
In the **Filter by** pane, you can filter the reports by the following: by using a last run date and the selected type of report.

- Last run date
- Report type

The last run date can be one of the following:

- Any date
- Before a selected date
- After a selected date
- Within a specific date range

The report type can be one of the following:

- Assets
- Standards
- Entitlements
- Policy
- Audit

You can do the following in the table pane:

- View a selected report.
- Remove a report.
- Apply a filter to the report list.
  
  You can base the filter on the report template type or date run.

When you view a report, you can export the report to a supported format.

See “**About the Reporting view**” on page 65.

---

**About the My Dashboards view**

The **My Dashboards** view lists the tiered dashboards that you can access. A tiered dashboard is listed in the table pane after you create the dashboard job using the **Create Tiered Dashboard** wizard.

If you are assigned as a viewer for the dashboard, you can remove any tiered dashboard from the **My Dashboards** view.

In the taskbar, you can select the following:

- **View**
- **Dashboard Tasks**
Create Tiered Dashboard

Delete

Manage Tiered Dashboards

View Details Report

View Trends Report

Tiered Dashboards Reports

The My Dashboards view has the following panes:

Filter by

Table

In the Filter by pane, you can create a filter on the Last Run Date.

You can have the following options for the Last Run Date:

- Any
- Before a selected date
- After a selected date
- Between selected dates

The table pane columns are as follows:

- Dashboard Name
- Last Run Date
- Status

You can select a column and drag the column name to the header to group the remaining columns by that column.

You can Search by any of the table pane columns.

In the table pane, you can do the following with a selected dashboard:

- View
- Delete
- Rename
- Copy
- Edit
- Edit Schedule
- Edit Dashboard Job Notification
About types of dashboards

Control Compliance Suite has the following types of dashboards:

Table 18-1  Dashboard types and descriptions

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Available in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tiered</td>
<td>A dashboard that is based on hierarchical dashboards with the sections and the nodes that logically represent your organization in different ways.</td>
<td>Control Compliance Suite Console</td>
</tr>
<tr>
<td>Web-based</td>
<td>A dashboard that is based on selected key elements of an organization and can be adapted for each viewer.</td>
<td>Control Compliance Suite Web Console</td>
</tr>
</tbody>
</table>

You can do the following for a tiered dashboard:

- Create the dashboards that contain evaluation sections and nodes.
- Schedule and execute the tiered dashboard update jobs.
- Edit a tiered dashboard and the evaluation sections and nodes.
- Delete a tiered dashboard.

A dashboard that is created in the Web Console has the following features:

- Web-based
- Real time
- May be able to collate data from various sources, if needed

The dashboard that is created in the Web Console is not based on a scheduled job. A dashboard that is created in the Web Console consists of independent elements, called panels. Each panel has two levels. The top level is typically a chart or a grid. You can drill down to see the detail in a second-level grid.

You can only access dashboards from the Web Console.

See “Managing tiered dashboards” on page 756.
About predefined report templates

The predefined report templates are installed with the Control Compliance Suite. The predefined report templates are in the Predefined folder in the tree pane of the Report Template view. You can schedule a report template. You can customize a template, if the template supports the feature. You can customize a report template in the predefined node or copy the report template to a user-defined folder in the Report Templates view.

You cannot delete a predefined report template.

See “Scheduling a report” on page 746.

See “Copying a report template” on page 750.

See “Customizing a report template” on page 750.

See “Predefined report descriptions” on page 741.

About data synchronization

Reports and dashboards use the data that is stored in the reporting database. The data that is required for reports and dashboards is synchronized with the production database using the synchronization job. The reporting database synchronization job is located in the Job Management view.

The synchronization job operates in the following modes:

- Automatic
- Scheduled

The automatic mode synchronizes data between the production and reporting databases after the completion of selected jobs. You can select the jobs in the Settings > General > System Configuration > Reporting Synchronization.

The synchronization job can be set to start at a specific time. You can request an administrator to schedule a synchronization job to run immediately. Only administrators run the synchronization job. You must run a synchronization job before you schedule a report or dashboard.

See “About the Report Management jobs” on page 741.

See “Synchronizing the reporting database” on page 167.

About creating user-defined templates

You can create a template with Crystal Reports 2008 SP1 and then add the template into Control Compliance Suite. You can also update an existing template by
exporting the template to Crystal Reports 2008 SP1. To add or update a template, you must be a Report Administrator.

An installation of the Crystal Reports 2008 SP1 is required. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

You can find more information on developing your reports at:

http://www.symantec.com/business/support/overview.jsp?pid=53741

See “Adding a user-defined report template” on page 752.

See “About the prerequisites for user-defined report templates” on page 738.

About the prerequisites for user-defined report templates

You can register user-defined reports. User-defined reports are reports created with Crystal Reports 2008 SP1. To create a user-defined report, you must have access to the reporting database.

You must have the following permissions:

- Access to the SQL Server instance
- Read-only access to the Reporting database
- An installation of the Crystal Reports 2008 SP1 is required. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

If you create a report that combines business objects, you must add all of the required parameters. The report template is validated based on the type of business objects. For example, if you create a report template for assets and standards, then you must add the required asset parameters and the required standards parameters to the report template. You do not add a required parameter twice. The ReportRunBy parameter and the ReportRunDate parameter must appear only once in the report.

If you create a report that needs information from RMS, the legacy default RMS database name is ComplianceManager.

To create a new asset or asset group report template in Crystal Reports 2008 SP1, you must have the following parameters:

- **AssetJobID** - The unique identifier joins related tables to the ReportJob table in the CSM_Reports database.
- **AssetGroup** - The unique identifier of the asset group present in the report scope.
- **Folders** - The unique identifier of the asset system folder within the report scope.
To create a new standards report template in Crystal Reports 2008 SP1, you must have the following parameters:

- **StandardJobID**: The unique identifier joins related tables to the ReportStandardJob table in the CSM_Reports database.
- **ReportRunBy**: The user who executes the reporting job for the report.
- **ReportRunDate**: The date for the reporting job

To create a new entitlements control points report template in Crystal Reports 2008 SP1, you must have the following parameters:

- **ControlPointType**: The display name of the control point type.
- **Status**: The control point status
- **DataOwner**: The control point owner
- **Tags**: The tags that are associated with the control point
- **EntitlementControlPointJobID**: The unique identifier joins related tables to the ReportJob table in the CSM_Reports database. The parameter is a part of the filter set definition XML. The definition filters control point types.
- **ReportRunBy**: The user who executes the reporting job for the report.
- **ReportRunDate**: The date for the reporting job
- **AssetGroup**: The unique identifier of the asset group present in the report scope.
- **Folders**: The unique identifier of the asset system folder within the report scope.

To create a new entitlements review cycles report template in Crystal Reports 2008 SP1, you must have the following parameters:
CurrentOrSnapshotted

The parameter determines if the report scope contains current review cycles or snapshot review cycles

Status

The status of the review cycle

ReviewCycleID

The unique identifier of the review cycle

ControlPointType

The display name of the control point type.

DataOwner

The control point owner

Tags

The tags that are associated with the control point

EntitlementsReviewCycleJobID

The unique identifier joins related tables to the ReportJob table in the CSM_Reports database. The parameter is a part of the filter set definition XML. The definition filters control point types.

ReportRunBy

The user who executes the reporting job for the report.

ReportRunDate

The date for the reporting job

AssetGroup

The unique identifier of the asset group present in the report scope.

Folders

The unique identifier of the asset system folder within the report scope.

To create a new policy report template in Crystal Reports 2008 SP1, you must have the following parameters:

PolicyJobID

The unique identifier joins related tables to the PM_PolicyUser table in the CSM_Reports database.

ReportRunBy

The user who executes the reporting job for the report.

ReportRunDate

The date for the reporting job

See “About creating user-defined templates” on page 737.
See “Adding a user-defined report template” on page 752.
About the Report Management jobs

In the Monitor >Jobs view, you can view the run status and details for the Report Management jobs.

The Report Management jobs are the following:

- Report generation: The job schedules a report.
- Dashboard update: The job schedules a dashboard.
- Scheduled Reporting Database Purge: The job purges historical and summary data from the reporting database.
- Reporting Database Synchronization: The job synchronizes the data from the production database into the reporting database.

See “Scheduling a report” on page 746.
See “Viewing a report” on page 747.

About the View My Reports filter option

If the report supports the filter option, you can filter a report in the View My Report - Reporting. A report may not support the filter option. The types of filter that you can apply to a report are different and based on the report.

Predefined report descriptions

The Control Compliance Suite Reports include the default reports that let you determine the state of the installation. Settings are selected before the report is run.

The result of a report may vary based on your permission level.

Table 18-2 Report Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Location</th>
<th>Customization Support</th>
<th>Job Chaining Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Evaluation Result</td>
<td>The report lets the user compare the two most recent compliance results and display the differences in values.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Location</td>
<td>Customization Support</td>
<td>Job Chaining support</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-----------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Asset Group Compliance</td>
<td>The report displays risk scores and compliance status of technical checks for an asset group or folder for the latest evaluation.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Asset Details</td>
<td>The report displays detailed information about the user's managed assets.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Asset Exception Status</td>
<td>The report displays a summary of exceptions that are in place across the IT infrastructure.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Asset Risk Summary</td>
<td>The report displays asset type, risk level, and related technical controls for a standard.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Assets at Highest Risk</td>
<td>The report displays the assets ranked by remediation order (based on risk score).</td>
<td>Report Templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Compliance by Technical Check</td>
<td>The report lets users filter the failed, passed, unknown, Not applicable, and errored technical checks.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Compliance by Asset</td>
<td>The report displays the individual check results for a set of assets.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Compliance Summary</td>
<td>The report lets users view risk scores and compliance status for a set of assets.</td>
<td>Report Templates</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Control Point Effective Permissions</td>
<td>The report generates detailed information about the effective permissions for one or more control points.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Location</td>
<td>Customization Support</td>
<td>Job Chaining support</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Control Point Simple Permissions</td>
<td>The report displays Simple permissions on the control point.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Control Point Permissions by Trustee</td>
<td>The report displays information about the permissions of a trustee for control points in the Entitlements module.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CCS System Auditing</td>
<td>The report displays key events related to Assets, Standards, Policies, and Entitlements in the CCS system.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Comparison of Control Statement Mappings</td>
<td>The report lets the user compare control statement mappings between policies or between a mandate and a policy.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Entitlement Change Requests</td>
<td>A report of the change requests made for the control points in the review cycle.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Evaluation Results Asset view</td>
<td>The report displays evaluation results by Asset for selected evaluation job/run.</td>
<td>Report Templates</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Entitlement Changes</td>
<td>The report lets the user access information for the entitlements or group memberships from the current and most recently approved entitlements.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Evaluation Results Standard View</td>
<td>The report displays evaluation results by Standard for selected evaluation job/run.</td>
<td>Report Templates</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Table 18-2  
Report Descriptions (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Location</th>
<th>Customization Support</th>
<th>Job Chaining support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Compliance by Asset</td>
<td>The report lets users view roll-up compliance scores for the assets assessed against technical and procedural controls.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policy Results by Control</td>
<td>The report displays asset information for selected policies like risk score, risk rating, technical checks, and procedural controls against which the asset is assessed.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policy Control Statement Mappings</td>
<td>The report lets you view the policy and the controls mapped to its control statements.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policy Summary</td>
<td>The report displays the assets, control statements, and audience for the selected policies.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policy Acceptance Status</td>
<td>The report displays the policy acceptance status.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Remediation Asset View</td>
<td>The report displays remediation information for one or more asset groups or containers for latest evaluation grouped by Asset.</td>
<td>Report Templates</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Remediation Standard View</td>
<td>The report displays the remediation information for one or more assets groups or containers, for latest evaluation grouped by Standard.</td>
<td>Report Templates</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 18-2  Report Descriptions (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Location</th>
<th>Customization Support</th>
<th>Job Chaining support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Details</td>
<td>The report reviews the technical checks that are applied to the IT infrastructure.</td>
<td>Report Templates</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Top Failed Technical Checks</td>
<td>The report identifies the checks that failed most frequently across a set of assets for the latest evaluation during the date range.</td>
<td>Report Templates</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Working with reports

You can do the following with a report template:

- Schedule a report template to create a report
  See “Scheduling a report” on page 746.

- View a report
  See “Viewing a report” on page 747.

- Copy a report template
  See “Copying a report template” on page 750.

- Customize a user-defined report template
  See “Customizing a report template” on page 750.

- Customize a report in the report viewer
  See “Customizing a report in report viewer” on page 751.

- Refresh a report in the report viewer
  See “Refreshing a report” on page 748.

- Export a report in the report viewer
  See “Exporting a report” on page 749.

- Print a report in the report viewer
  See “Printing a report” on page 748.

- Delete a user-defined report template
  See “Deleting a user-defined report template” on page 753.

- Add a user-defined report template
See “Adding a user-defined report template” on page 752.

- Export a user-defined report template
  See “Exporting a report template” on page 753.

- Update a user-defined report template
  See “Updating a report template” on page 754.

- Move a report template
  See “Moving a report template” on page 755.

- Remove a report
  See “Removing a report” on page 748.

### Scheduling a report

The Schedule Report wizard generates a report by creating a report generation job. A report is generated on the current data in the reporting database. The reports are generated only on the evaluated assets and standards. After you have created the job, you can view the current job status in Monitor > Jobs view. You can view the report in My Reports.

You must run the Reporting Database Synchronization job before you schedule the report. The synchronization job populates the database with the data in the production database. The synchronization job is an existing job and is in the Monitor > Jobs view. If you create the report before the synchronization job completes its run, you may see a blank report.

If you attach a report, the report displays the date and time of the operating system where the Application Server is installed. In a remote console, the report displays the date and time of the operating system where the Application Server is installed.

Each report has different scalability limitations. For example, the remediation report is designed to handle large result sets. For most of the predefined reports, you should be sure that your report fits within the limitation. A report may fail or cause a system slowdown if the limitation is exceeded.

If you have changed the locale or the time zone on the Application Server, you must restart the Application Server. After you have restarted the service, you should launch the Control Compliance Suite. You should run the Reporting Database Synchronization job and then run your report generation jobs.

The report generation job may send an email to selected users when the report is ready. Report notification must be implemented as a part of the reporting job workflow. The report notification has SMTP requirements.

Each schedule report wizard has a different sequence of panels. The panels that you complete depend on the business logic of the report.
Note: As a prerequisite for the CCS System Auditing report, you must enable auditing from the Settings > General > System Configuration area.

See “Running a job now” on page 719.

See “Viewing a report” on page 747.

To schedule a report

1. In the Report Templates view, select a report template.
2. Right-click and select Schedule Report.
   The wizard that is associated with that report is launched.
3. Complete the wizard to create the report generation job.
4. You can monitor the status in the Jobs view.

Viewing a report

After a successful report generation job run, the report is listed in My Reports view. The result of a report may vary based on your permission level.

You must synchronize data in the reporting database by running the sync report job before you run the report. The sync report job is in the Jobs > Monitor view.

The report process takes several minutes to generate a view if the selected report has large numbers of the following:

- Assets
- Checks
- Control points
- Policies

You must have sufficient disk space available in the user temp folder on the computer that runs the CCS console in the following conditions:

- You select a report that has a large number of assets, checks, control points, or policies
- You select multiple reports simultaneously

See “Working with reports” on page 745.

See “About the My Reports view” on page 733.
To view a report

1. In Reporting > My Reports, select a report.
2. Right-click and select View.
   
   The selected report opens in the viewer.

Refreshing a report

You refresh a report in the report viewer. The report must support the refresh option.

See “Viewing a report” on page 747.
See “Printing a report” on page 748.
See “About the My Reports view” on page 733.

To refresh a report

1. In the Reporting view, click My Reports.
2. Select a report and right-click.
3. Click View.
4. In the report viewer, click the Refresh icon.
5. In the Enter Parameter Values dialog box, provide the required information.
6. Select OK.

Removing a report

You can remove a report from the My Reports view.

Members of the CCS Administrators role cannot remove a report. If you are assigned as a viewer for the report, you can remove the report from the My Reports view.

See “Working with reports” on page 745.

To remove a report

1. In the table pane of Reporting > My Reports, select a report.
2. Right-click and select Remove.
3. In the Confirm message box, click Yes.

Printing a report

To print a report
1. In Reporting > My Reports, select a report in the table pane.
2. Right-click and select **View**.
3. In the report viewer, click the **Print Report** icon.
4. In the **Print** dialog, select the options and click **OK**.

Exporting a report

After a report generation job run has completed, you can export a report. You can export the report in the following formats:

- Crystal Reports (.rpt)
- Adobe Reader (.pdf)
- Microsoft Excel 97 - 2003 (.xls)
- Microsoft Excel 97 - 2003 Data-Only (.xls)
- Microsoft Word 97 - 2003 (.doc)
- Microsoft Word 97 - 2003 Editable (.rtf)
- Rich Text (.rtf)
- XML (.xml)

To export a report
1. In the Reporting view, click **My Reports**.
2. Select a report and right-click.
3. Select **View**.
4. In the report viewer, click the Export Report icon.
5. In the **Export Report** dialog box, browse to a folder, if needed.
6  Select a format, if needed.
7  Click Save.

Copying a report template

You can copy a report template to a user-defined folder. If the report template supports customization, you can customize a predefined report template or a user-defined report template.

See “Working with reports” on page 745.

See “Customizing a report template” on page 750.

To copy a report template
1  In the table pane of the Report Templates view, select a template.
2  Right-click the report template and select Copy.
3  Navigate to a user-defined folder.
4  Right-click in the table panel, and select Paste to add the template to the folder.

Customizing a report template

You can customize a report in the user-defined folder or predefined folder. Only certain report templates support customization.

Based on your permission level, you can customize the following report templates in the predefined folder:

- Asset Evaluation Result Change
- Compliance by Technical Check
- Assets at Highest Risk
- Asset Exceptions Status
- Asset Risk Summary
- Compliance by Asset
- CCS System Auditing
- Asset Group Compliance
- Top Failed Technical Checks

See “Copying a report template” on page 750.
To customize a report template

1. Select a template.
2. Right-click and select **Customize**.
3. In the **Specify Report Title, Company Name, and Logo** panel, provide a report title for the report. Click **Next**.

   You can add a company name and logo, if they are available in the Settings > General view.
4. In the **Specify Report Content** panel, you can add or remove the fields from the report. You can reorder the fields.
5. Click **Add Fields** to add fields to the report.

   The report template must support the feature.
6. In the **Add Fields** dialog box, select the fields. Click **OK**.

   You can add a maximum of 10 fields.
7. Click **Next**.
8. In the **Specify Report Group By Information** panel, select the fields that are used to group the displayed results. Click **Next**.
9. In the **Select the Location for the Saved Report** panel, navigate to the folder where you want to save the report. Click **Next**.
10. In the **Summary** panel, click **Finish**.

Customizing a report in report viewer

You can customize certain reports in the **My Reports** view in **Reporting**. You can find which reports support customization in the Predefined report and dashboard descriptions section. Every report does not support customization. Using the viewer, you may be able to interact with the report by drilling down into charts and table summaries.

When a report is customized in the report viewer, a report is not generated. The selected report is updated with the customized settings. This process is known as Post Customization. If you want to save the settings that you have customized, you must export the report. If you close and relaunch the report, the customized settings are not saved.

See “**Predefined report descriptions**” on page 741.

To customize a report in report viewer

1. In the **My Reports** view, select a report.
2. Right-click and select **View**.
3 In the report viewer, click **Customize**.

4 In the **Specify Report Title, Description, and Logo** page, provide a name for the report.

   You can add a company name and logo, if they are available in the Settings > General view.

5 In the **Specify Report Content** page, you select the fields for the report. Click **Add** to add fields.

6 In the **Add Fields** message box, select a maximum of 10 fields to add to the report.

7 Click **OK**.

8 Click **Next**

   In the **Specify Grouping of Information** page, and then select the groups that should be displayed.

9 In the **Summary** page, click **Finish**.

---

**Adding a user-defined report template**

With Crystal Reports 2008 SP1, you can create a report and then add the report to the Control Compliance Suite. You must be a member of the Report Administrator role to add a template.

An installation of the Crystal Reports 2008 SP1 is required to create the template. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

**To add a user-defined report template**

1 In the Reports view, select **Common Tasks**. Click **Add or Update** to open the **Add or Update a report template** wizard.

2 In the **Choose an Option - Add or Update a Report Template** panel, select **Add a report template**.

3 In the **Specify the Name, Description, and other Properties of the New, User-Defined Report Template** panel, provide the **Report template name**.

4 Provide the **Report template description**

5 In the **Import template from** box, navigate to and select the report template location.

6 In the **Save template to** box, navigate to and then select the folder to save the template.

7 Click **Next**.
In the Select the Business Objects panel, select the business objects that are included in the template.

Check Allow multiple if the template supports multiple instances of a business object.

Select the category type from the Report template category drop-down box. The category type is based on the selected business object.

Click Next.

In the Summary panel, click Finish.

Deleting a user-defined report template

You can delete a user-defined report template. A report template is not saved before deletion. If you delete the template, you must recreate the template if you want to use the template again. You can only delete a template in the user-defined folder.

You must have the appropriate permissions on the user folder to delete a template. If you delete a user-defined template, the deletion does not affect the predefined report template.

You cannot delete a predefined report template.

See “Working with reports” on page 745.

See “Copying a report template” on page 750.

See “Customizing a report template” on page 750.

To delete a user-defined report template

1. In the Report Templates tree view, navigate to a user-defined folder
2. In the table pane, select a template.
3. Right-click and select Delete.
4. In the Confirm message box, click Yes.

Exporting a report template

You can export a report template to an RPT file. You can open the file in Crystal Reports 2008 SP1 to modify the file. You can export either user-defined templates or predefined templates.

An installation of the Crystal Reports 2008 SP1 is required to view the exported file. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.
To export a report template

1. In the table pane, right-click a report template.
3. In the Save As dialog box, select the destination and provide a file name.
4. Click Save.

Updating a report template

You can update an existing report template in the user-defined folder using the Add or Update a Report Template wizard. The wizard validates the template's mandatory parameters for each update. A successful validation overwrites the existing template.

We recommend that you should update a template only if you make the following changes:

- Change the field labels
- Change header and footer information
- Add static text
- Change the layout
- Add fields
- Remove fields

The update fails if you alter the template's mandatory parameters. The template update process validates the number of mandatory parameters and the type of mandatory parameters. Parameters that are not mandatory are not checked. If the number of mandatory parameters is incorrect or if you have added mandatory parameters then the update fails.

If you want to change the template's mandatory parameters or if you want to add information to the report we recommend that you create a new template.

The validation only checks the report template's mandatory parameters. If you have two report templates with different information but the same mandatory parameters, you may overwrite the template. For example, if you have two asset reports, report A and report B, and you modify report A. You select report B when you do the update. Report B is overwritten. The report contents may be different but the validation succeeds and one template overwrites the selected template.

An installation of the Crystal Reports 2008 SP1 is required to modify the template. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.
To update a user-defined report template

1. In the Reports view, select **Common Tasks**. Click **Add or Update** to open the **Add or Update a report template** wizard.

2. In the **Choose an Option - Add or Update a Report Template** panel, select **Update a report template**.

3. In the **Browse for the Updated .RPT and Choose the Template to Update** panel, navigate to the modified RPT file.

4. Select a folder and add the report template to be updated.

5. Click **Next**.

6. In the **Summary** panel, click **Finish**.

7. In the message, click **OK**.

Moving a report template

You can move a user-defined report template from one location to another location. You can move a user-defined template from one user-defined folder to another user-defined folder.

To move a report template

1. In the table pane, right-click a report template.

2. Select **Move**.

3. In the **Move Report Template** dialog box, select the destination folder.

4. Click **OK**.

5. In the **Reporting** message box, click **OK**.

Editing a report generation job

You can edit a report generation job in the Job view. The job can have only one scheduled run in a 24 hour period. Any changes to the schedule overwrite the existing schedule. If you select the **Run now** option, the option does not affect the scheduled job run. By default, the schedules begin on the current date and the current time.

The Report type determines which steps are available.
To edit a report generation job

1. In the Monitor > Jobs view, existing jobs are shown in the table pane. Select a report generation job.

2. Right-click and select **Edit job**

   The wizard that is associated with that report is launched.

3. Complete the wizard to edit the report generation job.

**Working with tiered dashboards**

Dashboards are a visual analysis that provides a summary of your organization’s compliance. Dashboards provide the capability to view the security posture and assessment trends at a glance. You can also drill down through the hierarchy that represents your organization to see the compliance percentage of each level.

You can also create the dashboards that contain roll-up data, which is a summary result of the standards' checks and the bv-Control query results. Dashboards consume the summary data from the bv-Control XML export format and the evaluation results of the standards. The dashboard jobs that are created from the roll-up data are known as tiered dashboards.

**Note:** Tiered dashboards do not summarize results of ESM message data for display.

In the My Dashboards view, you can view the dashboards. In the **Monitor > Jobs** view, you can edit a dashboard update job.

- Viewing a dashboard
  
  See “Viewing a tiered dashboard” on page 758.

**Managing tiered dashboards**

Tiered dashboard is the hierarchical representation of roll-up data. The roll-up data is a summary of the evaluation results of the Standards checks and the bv-Control query results. Hierarchy in tiered dashboards refers to the creation of sections and nodes, which are scopes representing either a geographical location or a business unit. A tiered dashboard consumes the summary data from the bv-Control reports that are in XML format and the Standards evaluation results.

You can configure multiple dashboards to define the hierarchy that logically represents your organization in different ways. For example, you can configure the dashboards that are based on your corporate network topology, department structures, or geographical locations.
Getting started with tiered dashboards

Tiered dashboard collects data from either an evaluation result of the Standards module or from an export file of the bv-Control snap-in. Before you create a tiered dashboard, you must have either of the following completed:

- Evaluation results of assets that are evaluated against a standard
- Query results of any bv-Control snap-in

All users of dashboards must be assigned a role before they can use the application. Use the following table to get you started quickly with dashboards:

<table>
<thead>
<tr>
<th>Assigning roles</th>
<th>Assign appropriate roles and permission to the users of dashboards. See “About roles and permissions in tiered dashboard” on page 768.</th>
</tr>
</thead>
</table>
| Collecting data  | Do one of the following:  
  - For bv-Control query results data that are exported to an XML file, you need to set up a data location where the file is stored. The data location must be a network share path of the computer from where the export file is accessed by the dashboard. See “Configuring the data locations” on page 165.  
  - For the Standards module evaluation data, create and run a scheduled evaluation job. Dashboard update jobs that are scheduled for evaluation nodes of standards module evaluate the assets based on the selected standard at run time. The evaluation results are used for data collection by the dashboard. |
| Creating dashboard | Create a new dashboard. When you create a dashboard you first configure the settings for the dashboard that define the evaluation criteria for the assessment. See “Creating a tiered dashboard” on page 763. |
Configuring an evaluation node

Configuration settings for an evaluation node include selecting the following:

- Select the evaluation results for the Standards Evaluation Results node or the export file for the bv-Control Query Results node.
- Set the thresholds for the evaluation node.
- Schedule the collection of summary results for assessment.

See “Adding an evaluation node” on page 777.

Assessing and analyzing

After the data is collected and is available to the dashboard, you can begin to view, assess, and analyze the information.

See “Viewing a tiered dashboard” on page 758.

Viewing a tiered dashboard

All the tiered dashboards that you create are listed in the My Dashboards view. You can view the status and details of the dashboard sections provided you have the requisite view permissions.

You must synchronize data in the reporting database by running the Reporting Database Synchronization Job before you run the dashboard. The job is in the Jobs > Monitor view.

To view a tiered dashboard

1. Go to Reporting > My Dashboards view of the console.
2. In the My Dashboards view, select a tiered dashboard from the list, right-click it, and select View.
3. In the View Dashboard-Reporting window, you can find the following tabs for the selected tiered dashboard:
   - Status
   - Details
   - Evaluation Results
     This tab is displayed only when you select a Standards Evaluation Results evaluation node.

See “About the Status tab view” on page 759.

See “About the Details tab view” on page 761.
About the Status tab view

The **Status** tab of the **View Dashboard - Reporting** window captures the essence of the security assessment information. You can view the current roll-up of the security assessment status in the graphical form for a specific dashboard.

The status of the evaluation node is automatically updated at the time the Standards module evaluation job completes its execution. The status is also updated when the bv-Control schedule is completed.

The dashboard and the section status are also updated if the data collected crosses any threshold values. The last evaluated date-time stamp is displayed for an evaluation node.

When you select a dashboard or an evaluation section on the left pane of the window, the Status tab displays the following information:

- **Current Overall Status**
  - The dashboard analyzes and summarizes the lower level security assessment details. The dashboard provides a roll-up of the security assessment of the organization that is based on all data that is collected for this dashboard or for individual sections.
  - The overall status display indicate the following security assessment status levels:
    - Critical
    - Danger
    - Warning
    - Normal
    - No Data
    - Information

- **Status Trend**
  - This bar chart indicates the security posture of your organization, showing improvement or degradation over a time period. The status is based on the maximum status that the evaluation nodes have attained in a time interval. If there are multiple evaluations in a day, the latest status on that day is considered. The time scale can be changed to suit the needs of your analysis period.

- **Current Evaluations by Status**
  - This bar chart depicts the security assessment status of all evaluation nodes in this dashboard or the evaluation sections. The evaluation nodes are grouped based on criticality. By grouping, you can quickly determine if there are too many evaluation nodes in the critical or danger status that require immediate attention. The threshold conditions determine the status of the evaluation nodes.
Evaluations Trend  The line graph indicates the number of evaluation nodes that have attained a specific assessment status for a time period. The time period is based on the Trend Window option. The specific assessment status is the average status that the evaluation nodes have attained in a time interval. The average is used because data collection schedules can be different for different evaluation nodes.

**Note:** If an evaluation node does not exist or contains no data then the status, No Data is displayed for the dashboard or the section.

When you select an evaluation node in the left-side pane of the window, the Status tab displays the following information:

**Trend Window**  Select a trend from the Trend window option, which determines the amount of historical data that is to be displayed in the dashboard.

**Node Details**  Review the details of the node that you have selected.

The following Node Details are displayed for both the bv-Control Query Results and Standards Evaluation Results node.

- **Type**  Displays the type of the selected node.

- **Status**  Displays the status such as critical, warning, danger, and normal of the selected node.

- **Scope**  Displays the scope for the selected node. For example, for a bv-Control node, the path of location for the XML file is displayed.
Review the summary data that is collected for the selected node.

For the bv-Control Query Results node, the details are as follows:

- Not Found Percent
  - Refers to data of the selected node that is not found
- Found Percent
- Objects Not Found
  - Refers to not retrieving the target computers on which bv-Control queries are executed.
- Objects Found
  - Refers to retrieving the target computers on which bv-Control queries are executed.
- Objects in Scope
  - Refers to the scope for target computers on which bv-Control queries are executed.

For the Standards Evaluation Results node, the details are as follows:

- Compliance Score
- Risk Score
- Total Checks
- Checks Unknown
- Checks Passed
- Checks Failed

Review the value of the custom threshold that you have set for the node.

Review the bar chart that shows the status trend of the selected node.

Select the time period for which you want to view the status trend from the Time Scale drop-down box.

See “About trends configuration” on page 781.

Review the bar chart that shows the current status of the evaluation data for the node.

Select the time period for which you want to view the summary results trend from the Time Scale drop-down box.

See “About the Details tab view” on page 761.

### About the Details tab view

The Details tab displays the evaluation results of the Standards and the bv-Control query results. You can print or export the grid information to a file.
When you select a dashboard or an evaluation section on the left pane of the View Dashboard - Reporting window, the Details tab displays the following:

- The roll-up of the evaluation results from all the nodes or sections in the dashboard or evaluation section.
- The evaluation node name, hierarchical path, and the time when the evaluation node was last updated.
- The results that are grouped based on the security assessment status. You can regroup the evaluation nodes based on the status or the type of evaluation node. You can drag the columns to group the evaluation nodes in the window.

When you select an evaluation node on the left pane of the window, the tab displays the assets in the evaluation results. The predefined assigned attributes and values of the assets are also displayed for the evaluation node. If you add new attributes to an asset, then the details of the new fields are also listed for the evaluation node.

You can click on the column chooser icon to select or unselect the attribute columns.

**Note:** You can view the data of only those assets for which you have the requisite permission.

See “About the Status tab view” on page 759.

See “Viewing a tiered dashboard” on page 758.

### About the Evaluation Results tab view

The Evaluation Results tab displays the evaluation results of a standard that is evaluated on an asset. The tab displays the details of the number of assets that are evaluated and the properties of the checks that are executed on the assets. The tab also contains a graphical representation of the risk score, compliance score, and the result summary of the assets.

The various fields of the tab and their descriptions are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Evaluated</td>
<td>Name of the standard that evaluated the asset.</td>
</tr>
<tr>
<td>Asset Name</td>
<td>Name of the asset.</td>
</tr>
<tr>
<td>Data Collection Date</td>
<td>Date when data is collected from the assets for the selected standard.</td>
</tr>
</tbody>
</table>
Evaluation Date  
Date when evaluation of the collected data for the selected standard is performed.

Column Chooser  
Lets you select the properties of the checks to display at the bottom pane of the view.

You can right-click a check and select Export to export the check details to a file.

Click the column chooser icon to display the dialog box.

See “Working with Evaluation Results” on page 653.

Creating a tiered dashboard

A tiered dashboard can be created and listed in the My Dashboards view of the console. A tiered dashboard is executed as a tiered dashboard update job from the My Dashboards or from the Monitor> Jobs view of the console.

Note: You must synchronize data in the reporting database by running the Reporting Database Synchronization Job before you run the tiered dashboard update job. The job is in the Monitor> Jobs view.

To create a tiered dashboard

1  Go to Reporting > My Dashboards in the console.
2  In the My Dashboards view, right-click on the table pane and select Create Tiered Dashboard.
3  In the Specify Name and Description panel of the Create Tiered Dashboard wizard, enter the name and description and then click Next.

   The Description is optional.

4  In the Create Dashboard Nodes panel, you can do the following and then click Next.
   ■  Create a section.
   ■  Create and edit node.
   ■  Add and manage a trustee.
   ■  Set up a notification for the dashboard.
   ■  Copy, paste, rename, and delete a dashboard.

5  In the Job Schedule panel, select an option of scheduling the dashboard job that you create and then click Next.
6 In the **Job Notification** panel, setup the notification for the success or failure of the scheduled dashboard job and then click **Next**.

7 In the Summary panel, review the details of the dashboard job that you create and then click **Finish**.

See “Editing a tiered dashboard” on page 764.

See “Configuring an email notification alert for tiered dashboards” on page 780.

**Editing a tiered dashboard**

You can edit a tiered dashboard from the My Dashboards view of the console.

**To edit a tiered dashboard**

1 Go to **Reporting > My Dashboards** view in the console.

2 In the My Dashboards view, do one of the following:
   - Right-click on the selected tiered dashboard and select **Edit**.
   - Click **Manage Tiered Dashboards > Edit**

3 In the **Edit Dashboard** dialog box you can edit any of the following and then click **OK**.
   - Create and edit an evaluation node.
   - Add and manage a trustee.
   - Set up a notification for the dashboard.
   - Copy, paste, and delete a dashboard.

See “Creating a tiered dashboard” on page 763.

See “Viewing a tiered dashboard” on page 758.

**Copying and pasting a tiered dashboard**

You can create a copy of an existing tiered dashboard that is displayed in the **My Dashboards** view. When you copy and paste a dashboard, all the permissions assigned to the user are also copied.

**Note:** On copying a tiered dashboard, the permissions stamped on the dashboard are also copied.
To copy a tiered dashboard

1. Go to Reporting > My Dashboards view and select a tiered dashboard.
2. In the My Dashboards view, do one of the following:
   - Right-click on the selected tiered dashboard and select Copy.
   - Click Manage Tiered Dashboards > Copy.
3. On the same My Dashboards view do one of the following to paste the copied dashboard:
   - Right-click on the workspace and select Paste Tiered Dashboard
   - Click Manage Tiered Dashboards > Paste Tiered Dashboard

See “Copying and pasting an evaluation section” on page 779.
See “Copying and pasting an evaluation node” on page 779.

Renaming a tiered dashboard

You can change the current name of a tiered dashboard by renaming it in the My Dashboards view.

To rename a tiered dashboard

1. Go to Reporting > My Dashboards view of the console.
2. In the My Dashboards view, do one of the following:
   - Select a tiered dashboard to rename and click Rename.
   - Click Manage Tiered Dashboards > Rename.
3. In the Rename Dashboard dialog box, provide the new name.

See “Managing tiered dashboards” on page 756.

Editing a tiered dashboard job schedule

You can edit the job schedule of a tiered dashboard from the My Dashboards view of the console. Initially, you can schedule the dashboard update job when creating it using the Create Tiered Dashboards wizard.

To edit a tiered dashboard job schedule

1. Go to Reporting > My Dashboards view of the console.
2. In the My Dashboards view, do one of the following:
   - Select a tiered dashboard and then click Edit Schedule.
Click Manage Tiered Dashboards > Edit Schedule

3 In the Schedule Dashboard dialog box, edit the job schedule options, and then click OK.

**Editing a tiered dashboard job notification**

You can edit the job notification of a tiered dashboard from the My Dashboards view of the console. Initially, you can set the dashboard update job notification when creating it using the Create Tiered Dashboards wizard. Control Compliance Suite sends an email notification whenever a dashboard job succeeds or fails.

**To edit a tiered dashboard job notification**

1 Go to Reporting > My Dashboards.
2 In the My Dashboards view, do one of the following:
   - Select a tiered dashboard and then click Edit Dashboard Job Notification
   - Click Manage Tiered Dashboards > Edit Dashboard Job Notification
3 In the Job Notification dialog box, edit the job notification for the Success and the Failure tabs, and click OK.

**Importing a tiered dashboard**

You can import a tiered dashboard from an XML file into the My Dashboards view. The XML file must adhere to a specific schema. A new dashboard is created after you import an XML file provided that no dashboard of the same name already exists.

You can import multiple XML files to create multiple dashboards. An hourglass icon appears during the import operation of the selected dashboard. A status dialog box appears when the import operation completes.

**Note:** Depending on the type of XML editor, the threshold operators, < or > might appear in the exported XML file as &lt or &gt, respectively. You must retain the operators as, &lt or &gt in the XML file during dashboard import.

**To import a tiered dashboard**

1 Go to Reporting > My Dashboards view of the console.
2 In the My Dashboards view, do one of the following:
   - Right-click on the table pane and select Import Tiered Dashboard.
Click Manage Tiered Dashboards > Import Tiered Dashboard.

3 In the Select File to Import dialog box, select the xml file, and then click Open.

See “Exporting a tiered dashboard” on page 767.

Exporting a tiered dashboard

You can export a tiered dashboard to an XML file. You can use an XML editor to read and edit the file later. The exported dashboard XML file contains all the required and mandatory information to recreate a dashboard. The XML file contains comments for each element for you to edit the XML file. You must have the appropriate permissions to export specific evaluation sections of a dashboard.

An XML file is saved in the location that you select. An hour glass appears while the export operation is in progress. A status dialog box appears when the export operation completes.

Note: Depending on the type of XML editor, the threshold operators, < or > might appear in the exported XML file as, &lt or &gt respectively. You must retain the operators as &lt or &gt in the XML file during dashboard import.

The exported XML file contains the following information:

- Dashboard attributes
- Event notification
- View permissions
- Evaluation node and evaluation section attributes

To export a tiered dashboard

1 Go to Reporting > My Dashboards view.
2 In the My Dashboards view, do one of the following:
   - Click Manage Tiered Dashboards > Export.
   - right-click a dashboard and select Export
3 Save the dashboard as an XML file when the File Save dialog box opens.

See “Importing a tiered dashboard” on page 766.

Editing a tiered dashboard update job

You can edit a tiered dashboard update job from the Monitor > Jobs view.
To edit a tiered dashboard update job

1. Go to Monitor > Jobs view of the console.
2. In the Jobs view, right-click a dashboard update job and select Edit Job.
3. In the Edit Tiered Dashboards wizard, edit the properties of the job and reschedule it.

About roles and permissions in tiered dashboard

Control Compliance Suite can restrict permission for any user or group to any specific network data. This restriction of permission is leveraged in tiered dashboards through roles that are defined with permission to perform specific tasks.

The following default roles are defined for the tiered dashboard:

- Report Result Viewer
- Reporting Administrator
- CCS Administrator

Using the role-based access control feature, permissions can be given at the dashboard level or at the section level of a dashboard.

By default, view permissions over dashboards and sections are assigned to all users who belong to any of the default roles. Dashboard trustees are created to assign permissions to few selected users to view a dashboard or a dashboard section. The Manage Trustees option of the Edit Dashboard dialog box creates the dashboard trustee for the tiered dashboard.

Users with the following roles can modify the View permissions:

- CCS Administrator role
- Report Result Viewer role
- Reporting Administrator role

See “About the predefined roles in tiered dashboards” on page 769.
See “About view permissions for users in Report Result Viewer role” on page 770.
See “About manage permission for users in Reporting Administrator role” on page 771.
About the predefined roles in tiered dashboards

The tiered dashboards provide predefined roles that you can use to delegate permissions for your users.

The tiered dashboards related tasks that a user of a specific role can perform are as follows:

<table>
<thead>
<tr>
<th>Report Result Viewer</th>
<th>User who is added in the Report Result Viewer role can do the following at the dashboard and section level:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ View the tiered dashboard</td>
</tr>
<tr>
<td></td>
<td>■ View the dashboard details report</td>
</tr>
<tr>
<td></td>
<td>■ View the dashboard trends report</td>
</tr>
<tr>
<td></td>
<td>■ View the jobs, the job runs, and the details of a job in the Job Management view of the console.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reporting Administrator</th>
<th>User who is added in the Reporting Administrator role and is the creator of a dashboard can do the following at the dashboard and section level:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Create a dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Edit a dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Rename a dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Copy and paste a dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Edit the dashboard job notification</td>
</tr>
<tr>
<td></td>
<td>■ Import and export a dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Setup a dashboard status notification</td>
</tr>
<tr>
<td></td>
<td>■ View the dashboard details and trends report</td>
</tr>
<tr>
<td></td>
<td>■ View the dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Assign permission to another user to manage the dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Run and schedule the tiered dashboard update job</td>
</tr>
</tbody>
</table>

User who is added in the Reporting Administrator role and assigned permission on a dashboard or a section can do the following:

■ Create a dashboard
■ Edit a dashboard or a section
■ View the dashboard
  You can view the section of the dashboard for which you have the permission.
■ View the dashboard details and trends report
  You can view the reports for the section of the dashboard for which you have the permission.
■ Import and export a dashboard
■ Run a tiered dashboard update job
See “Predefined roles” on page 97.

**About view permissions for users in Report Result Viewer role**

A CCS Administrator or a Reporting Administrator user can edit the view permission of a user that belongs to the Report Result Viewer role. You can edit the view permission of a tiered dashboard user using the Manage Trustees option of the Edit Dashboard dialog box.

The user with view permission at the dashboard level can do the following:

- View the dashboard details report and the dashboard trends report for a tiered dashboard.
  The dashboard details and trends report are accessed for a Tiered dashboard that is selected in the My Dashboards view.

- Require requisite permission to view the assets and standards for a Standards Evaluation Results node in the View Dashboard - Reporting window.
  The user must have read permission on assets and standards to view the Details and the Evaluation Results tabs of the Standard Evaluation Results node.
  See “Predefined roles” on page 97.

  | Status tab |
  | Details tab |
  | Evaluation Results tab |

The user with view permission at the section level of a dashboard can do the following:

- View the section and its evaluation nodes in the View Dashboard-Reporting window. The child sections can also be viewed.
  The user cannot view the evaluation nodes of the parent dashboard or the parent section.

- The user must have read permission on assets and standards to view the Details and the Evaluation Results tabs of the Standard Evaluation Results node.

See “About manage permission for users in Reporting Administrator role” on page 771.

See “About the predefined roles in tiered dashboards” on page 769.
About manage permission for users in Reporting Administrator role

A CCS Administrator or a Reporting Administrator user can assign permission to users to manage a tiered dashboard. You can assign permission to a user using the Manage Trustees option of the Create or Edit Tiered Dashboards wizard.

The following points apply to the user with permission to manage a tiered dashboard:

- Create a new dashboard and have permission on all the tasks that are related to the dashboard and the dashboard update job.
- The following tasks cannot be performed by the user who is not a creator of the dashboard but is assigned permission to manage the tiered dashboard:
  - Edit Dashboard Job Notification
  - Edit Schedule
  - Delete
  - Rename
  - Set up notification

The following points apply to the user with permission to manage at the section level of a dashboard:

- Create a new dashboard and have permission on all the tasks that are related to the dashboard and the dashboard update job.
- The following tasks cannot be performed by the user who is not a creator of the dashboard but is assigned permission to manage the section of a tiered dashboard:
  - Edit Dashboard Job Notification
  - Edit Schedule
  - Delete a dashboard
  - Rename a dashboard
  - Setup dashboard notification
  - Any tasks that are to be performed for the parent section or dashboard

See “About view permissions for users in Report Result Viewer role” on page 770.
See “About the predefined roles in tiered dashboards” on page 769.
About threshold settings in tiered dashboard

You can define thresholds for all the security assessment status levels of a Tiered dashboard's evaluation node. If the set threshold condition for an evaluation node does not evaluate to true, then the node's security assessment status is Normal. If the set threshold condition for an evaluation node evaluates to true, then the associated status level is the security assessment status of the evaluation node.

Configuring the threshold for a status level involves defining the check fields, relational operator, and the check reference value. The check fields vary depending on whether you have selected a Standards Evaluation Results node or a bv-Control Query Results node. The check field values are derived from the evaluation results of the Standards module and the summary results' data fields of the bv-Control queries.

We recommend that you use the same check field for the different status levels that are defined for the evaluation node. Also, define thresholds in such a way that one of them always evaluates to true.

See “About the threshold types” on page 772.

See “About status calculation” on page 774.

About the threshold types

Threshold conditions are configured for the evaluation nodes to generate customized dashboard reports and information about the dashboard status. The types of thresholds that can be configured for an evaluation node are Global Threshold, Custom Threshold and No Thresholds (Information only node). All the threshold types can be set and associated with the evaluation nodes when you create the nodes through the Create Tiered Dashboards wizard.

The types of thresholds and their descriptions are as follows:

- **Global Threshold**: Use this threshold type to set conditions and apply them to all the evaluation nodes of the same type.

  You can set the global thresholds from the General view of the console. You can access the option, **Settings > General > Tiered Dashboards > Global Thresholds Settings** to configure the global thresholds.

- **Custom Threshold**: Use this threshold type to set the threshold conditions specific to an evaluation node. You can set the threshold conditions for the evaluation node through the Create Tiered Dashboards wizard.
No Thresholds Use this threshold type when you want to retrieve summary data of evaluation nodes for which no threshold conditions are set.

See “About the threshold check fields” on page 773.
See “About status calculation” on page 774.

About the threshold check fields
Check fields are threshold parameters for which the threshold values are set for a node.

The following check fields are available for the Standards Evaluation Results node:

- Compliance Score (%)
- Total Checks
- Checks Passed
- Checks Failed
- Checks Unknown
- Risk Score

The following check fields are available for the bv-Control Query Results node:

- Objects in Scope
- Objects Found
- Objects Not Found
- Found Percent
- Not Found Percent

See “About the relational operators” on page 773.

About the relational operators
The dashboard evaluation node configuration supports the following relational operators for comparing the check field values and the reference:

- < (Less Than) Values that are smaller than the user-selected value.
- > (Greater Than) Values that exceed the user-selected value
- <= (Less Than or Equal To) Values that are smaller than or are equal to the user-selected value.
Values that match the user-selected value.

Values that exceed or are equal to the user-selected value.

See “About status calculation” on page 774.

**About status calculation**

The summary data collected by an evaluation node is evaluated against the reference values as configured in the threshold settings. If a threshold condition does not evaluate to true, then the evaluation node's security assessment status is Normal. If a threshold condition evaluates to true, then the associated status level is the security assessment status of the evaluation node.

See “Example of status calculation for Standards Evaluation Results node” on page 774.

See “Example of status calculation for bv-Control Query Results node” on page 775.

**Example of status calculation for Standards Evaluation Results node**

You can set the criticality of your environment in different ways. For example, you can define the criticality for your environment, based on a percentage of compliance.

To set the status condition that is based on 85% compliance, you can use the Standards evaluation results.

<table>
<thead>
<tr>
<th>Status</th>
<th>Condition</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Compliance Score (%)</td>
<td>&lt;</td>
<td>50.00</td>
</tr>
<tr>
<td>Danger</td>
<td>Compliance Score (%)</td>
<td>&lt;</td>
<td>70.00</td>
</tr>
<tr>
<td>Warning</td>
<td>Compliance Score (%)</td>
<td>&lt;</td>
<td>85.00</td>
</tr>
<tr>
<td>Normal</td>
<td>Compliance Score (%)</td>
<td>&gt;=</td>
<td>85.00</td>
</tr>
</tbody>
</table>

To set the status condition that is based on the total number of checks that are passed, you can use the Standards evaluation results.
Table 18-4  Criticality status based on the total number of checks passed

<table>
<thead>
<tr>
<th>Status</th>
<th>Condition</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Compliance Score</td>
<td>&lt;</td>
<td>50.00</td>
</tr>
<tr>
<td></td>
<td>(%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Danger</td>
<td>Checks Failed</td>
<td>&gt;=</td>
<td>50.00</td>
</tr>
<tr>
<td>Warning</td>
<td>Check Unknown</td>
<td>&gt;=</td>
<td>20.00</td>
</tr>
<tr>
<td>Normal</td>
<td>Checks Passed</td>
<td>&gt;=</td>
<td>50.00</td>
</tr>
</tbody>
</table>

See “Managing tiered dashboards” on page 756.

**Example of status calculation for bv-Control Query Results node**

You can use bv-Control query results to set the status condition that is based on 85% of found objects.

Table 18-5  bv-Control query configuration

<table>
<thead>
<tr>
<th>Status</th>
<th>Condition</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Objects Found</td>
<td>&lt;</td>
<td>15.00</td>
</tr>
<tr>
<td>Danger</td>
<td>not used</td>
<td>not used</td>
<td>not used</td>
</tr>
<tr>
<td>Warning</td>
<td>not used</td>
<td>not used</td>
<td>not used</td>
</tr>
<tr>
<td>Normal</td>
<td>Objects Found</td>
<td>&gt;=</td>
<td>85.00</td>
</tr>
</tbody>
</table>

See “Managing tiered dashboards” on page 756.

**Configuring tiered dashboards**

Dashboard configuration involves tasks that are related to creating and modifying the sections and nodes of the dashboard.

Dashboard configuration includes the following:

- Adding a node
  See “Adding an evaluation node” on page 777.

- Editing a node
  See “Editing an evaluation node” on page 778.

- Deleting a node
See “Deleting an evaluation node” on page 778.

- Copying and pasting an evaluation section
  See “Copying and pasting an evaluation section” on page 779.

- Copying and pasting an evaluation node
  See “Copying and pasting an evaluation node” on page 779.

- Configuring the email alerts
  See “Configuring an email notification alert for tiered dashboards” on page 780.

See “Managing tiered dashboards” on page 756.

**About types of evaluation nodes**

An evaluation node represents a scope of assets or query reports, which are to be assessed by Control Compliance Suite.

A Standards Evaluation Results node represents a scope of assets that are evaluated against a specific standard.

A bv-Control Query Results node represents a scope of query reports. The query reports are exported into the XML files after executing the bv-Control queries on the assets.

See “Adding an evaluation node” on page 777.

**Assigning roles and permissions to users of tiered dashboard**

You can associate a user or group with any predefined role that is specific to dashboard and assign permissions. The predefined roles that are specific to dashboard are Report Result viewer and Reporting Administrator. You can assign or revoke permission to a user or a group using the Manage Trustee option of the Create Tiered Dashboards wizard. You can edit the permissions in the Edit Dashboard dialog box.

To revoke permission completely for a user, you must remove the user from the dashboard specific role in the Roles view of the console.

**To assign permission to users or groups on a specific dashboard or an evaluation section**

1. Go to Settings > Roles view of the console.

2. In the Roles view, right-click any of the dashboard related roles and select Add Users and Groups and add a user or group.

   See “Adding users and groups to a role” on page 107.

3. Go to Reporting > My Dashboards view of the console
In the My Dashboards view, right-click a dashboard and select Edit.

In the Edit Dashboard dialog box select the dashboard or section and then click Manage Trustees.

In the Manage Trustees dialog box, click Add Users and Groups to assign a user or group to a role.

In the Manage Trustees dialog box, you can view the list of users and groups that are associated with a role.

In the Select Users or Groups dialog box, select a role name and associate the users or groups that are configured for the role and click Update Users and Groups.

In the Manage Trustees dialog box, click Update Permissions.

In the Edit Dashboard dialog box, click OK.

To revoke permission for a user or group from a specific dashboard or an evaluation section

1. Go to Reporting > My Dashboards view of the console
2. In the My Dashboards view, right-click a dashboard and select Edit.
3. In the Edit Dashboard dialog box select the dashboard or section for which you want to revoke permission and click Manage Trustees.
4. In the Manage Trustees dialog box, select the user name or group name and the corresponding role name and click Remove.
5. In the Manage Trustees dialog box, click Update Permissions.
6. In the Edit Dashboard dialog box, click OK.

Adding an evaluation node

You can use the Edit Dashboard dialog box to add evaluation nodes to an existing tiered dashboard. You can also use the Create Tiered Dashboards wizard to add a new evaluation node to the tiered dashboard.

A tiered dashboard can contain evaluation nodes of the following types:

- Standards Evaluation Results
- bv-Control Query Results

To add an evaluation node

1. Go to Reporting > My Dashboards view of the console.
2. In the My Dashboards view, right-click a dashboard and select Edit.
3 In the **Edit Dashboard** wizard, select the type of node from the drop-down box, and click **Add Node**.

You can select either **bv-Control Query Results** node or **Standards Evaluation Results** node from the drop-down box.

4 In the displayed dialog box, enter the required values to create the following nodes:

- For a Standards Evaluation Results node, enter the required values in the dialog box.
- For a bv-Control Query Results node, enter the required values in the dialog box.

See “**Editing an evaluation node**” on page 778.

**Editing an evaluation node**

You can edit either the bv-Control Query Results node or the Standards Evaluation Results node of a tiered dashboard.

To edit an evaluation node

1 Go to **Reporting > My Dashboards** view of the console.
2 In the **My Dashboards** view, right-click a dashboard, and select **Edit**.
3 In the **Edit Dashboard** dialog box, select and expand the dashboard to the level of the evaluation node.
4 Select the evaluation node and click **Edit Node**.

A dialog box corresponding to the selected node type is displayed.

5 In the displayed dialog box, edit the required values for the following evaluation nodes:

- For a Standards Evaluation Results node, enter the required values in the dialog box.
- For a bv-Control Query Results evaluation node, enter the required values in the dialog box.

See “**Adding an evaluation node**” on page 777.

See “**Deleting an evaluation node**” on page 778.

**Deleting an evaluation node**

You can delete an evaluation node that is added to a tiered dashboard. When creating a tiered dashboard, you can delete an evaluation node from the **Create**
Tiered Dashboards wizard. You can also delete an existing evaluation node through the Edit Dashboard dialog box.

**Note:** Data of the evaluation node is deleted once you delete the evaluation node.

**To delete an evaluation node**

1. Go to Reporting > My Dashboards view of the console.
2. In the My Dashboards view, right-click a dashboard and select Edit.
3. In the Edit Dashboard dialog box, select and expand the dashboard to the level of the evaluation node.
4. Select the evaluation node and click Delete.

See “Editing an evaluation node” on page 778.

**Copying and pasting an evaluation section**

You can copy and paste an evaluation section when creating a tiered dashboard using the Create Tiered Dashboards wizard. You can also copy and paste a section when editing the tiered dashboard using the Edit Dashboard dialog box.

**Note:** On copying a section of the dashboard, all the permissions that are stamped on the section are also copied.

**To copy and paste an evaluation section**

1. Go to Reporting > My Dashboards view of the console.
2. In the My Dashboards view, do one of the following:
   - Click Create Tiered Dashboards to create a dashboard.
   - Right-click a dashboard and select Edit to edit a dashboard.
3. In the wizard or the Edit Dashboard dialog box, select the section of a dashboard that you want to copy and click Copy.
4. Navigate to the level of a dashboard and then click Paste.

See “Copying and pasting an evaluation node” on page 779.

**Copying and pasting an evaluation node**

You can copy and paste an evaluation node of a tiered dashboard through the Create Tiered Dashboard wizard and the Edit Dashboard dialog box.
To copy and paste an evaluation node

1. Go to Reporting > My Dashboards view of the console.
2. In the My Dashboards view, right-click a dashboard and then select Edit.
3. In the Edit Dashboard dialog box, select a section of a dashboard and navigate to the node that you want to copy and click Copy.
4. Navigate to the level of a section and then click Paste.

See “Copying and pasting an evaluation section” on page 779.

Configuring an email notification alert for tiered dashboards

You can configure an email notification alert for the tiered dashboards.

You can configure an email notification for the following tasks:

- Status change of a tiered dashboard update job
  The status of the tiered dashboard update job can change to either success or failure.

- Status change of a dashboard.
  A dashboard's status can change if the status of a section or an evaluation nodes changes.

To configure email notification for a tiered dashboard job

1. Go to Reporting > My Dashboards in the console.
2. In the My Dashboards view, right-click a dashboard and select Edit Dashboard Job Notification.
3. In the Job Notification dialog box, enter the values for the required fields.

To configure email notification for a tiered dashboard

1. Go to Reporting > My Dashboards in the console.
2. In the My Dashboards view, select Manage Tiered Dashboards > Create Tiered Dashboards or Manage Tiered Dashboards > Edit.
3. In the Create Tiered Dashboards wizard or Edit Dashboard dialog box navigate to the Create Dashboards Node panel and click Setup Notification.
4. In the Setup Notification dialog box, enter the values of the fields for setting an email notification.
About trends configuration

The tiered dashboard lets you view the trends in the security assessment posture of your organization over a period of time. To view the trends, you must add an evaluation node and schedule data collection for a tiered dashboard.

See “Adding an evaluation node” on page 777.

Trends define the amount of historical data that is displayed for an evaluation node. You can set the default trends for an evaluation node when creating it using the Create Tiered Dashboards wizard. The trends are displayed based on the time scale that is set for the evaluation node. The time-scale setting defines the frequency of display of the data. You can configure various types of trends and time-scale for an evaluation node.

By default, in the tiered dashboard's reporting view, all data that you collect from the dashboard's creation date to the current date are displayed. You can view the status trends of the evaluation node for the selected time scale in the Status tab of the View Dashboard-Reporting window.

Dashboard details and trends reports can also be generated and viewed for the configured trends.

See “About configuring trends for evaluation nodes” on page 781.

See “Calculation of time interval - Example 1” on page 782.

See “Calculation of time interval - Example 2” on page 783.

About configuring trends for evaluation nodes

Evaluation node trends are the latest evaluation data that is collected by the evaluation node. For example, if you want to view the trends for the last week on a daily basis, then the latest data that is collected in the week is displayed.

You can configure trends for an evaluation node of the tiered dashboard in the following ways:

- Set the default trends and time scale for the evaluation nodes when creating it through the Create Tiered Dashboards wizard.
  You can set the default trend and time scale in the Create Dashboard Nodes panel of the wizard. Data is collected for the evaluation node based on this default trends and time-scale configuration.

- Set the trends for the evaluation nodes when viewing it in the View Dashboard-Reporting window.
  You can modify the status trends of the evaluation node when viewing the dashboard in the View Dashboard-Reporting window. In the View Dashboard
- **Reporting** window, the view at the dashboard or section level displays the status trends of the latest updated evaluation node.

- Set the trends and time scale of the evaluation nodes in the Dashboard Details and Trends report.
  
The Dashboard Details and Trends reports updates and displays the report instantly as per the configured trends.

See “**Viewing the tiered dashboard reports**” on page 784.

See “**Calculation of time interval - Example 1**” on page 782.

See “**Calculation of time interval - Example 2**” on page 783.

**Calculation of time interval - Example 1**

The Trend Window is given as the Last Month, with the Current Date given as the date of entry, in this example 3/1/2007. The Trend Start Date would then be 2/1/2007 and the Trend End Date would be 2/28/2007.

If the Time Scale value is Weekly, the time intervals are based on the days in the week. For calculation purposes, Weekly starts on Sunday and ends on Saturday. The first date is the Trend Start Date, which is as per this example is 2/1/2007(Thursday). The last date is Trend End Date, which as per this example is 2/28/2007 (Wednesday). The complete calendar weeks between the first and the last date start on Sundays and end on Saturdays.

Based on the example the five time intervals and their display dates are as follows:


The time interval shows the time period in the **Trend Window** for which data is grouped and the trends are calculated. The display value is the value shown as X-axis labels.
If the Time scale value is Daily, then the time intervals are based on the days in the month.

The 28 time intervals and their display dates are the following:

2/2/2007 Displays as 2/2/2007
...

The time interval shows the time period in the Trend Window for which data is grouped and the trends are calculated. The display value is the value shown as X-axis labels.

See “Managing tiered dashboards” on page 756.

**Calculation of time interval - Example 2**

The Trend Window is given as Last 30 Days, with the Current Date given as the date of entry, in this case 3/1/2007. The Trend Start Date would then be 1/31/2007 and the Trend End Date would be 3/1/2007.

If the time scale value is Monthly, the three time intervals and their display dates are as follows:

1/31/2007 - 1/31/2007 Displays as Jan 2007

The time interval shows the time period in the Trend Window for which data is grouped and the trends are calculated. The display value is the value shown as X-axis labels.

See “Managing tiered dashboards” on page 756.
Viewing the tiered dashboard reports

Tiered dashboard reports show the trends and the summary details of the evaluation nodes. The dashboard reports are displayed in a new window. You can export the details and the trends report to any format such as a PDF, XLS, RTF.

The following are the types of tiered dashboards reports:

- **Dashboard Details report**
  Displays the details of the evaluation node, the summary results data and the assessment status for the node. The information is in a graphical format.

- **Dashboard Trends report**
  Displays the graphical view of the security assessment posture of your organization for the specified time period.
  Prints the Status Trend and the Evaluations Trends for all the levels of the dashboard.

See “Viewing the dashboard details report” on page 784.
See “Viewing the dashboard trends report” on page 785.

Viewing the dashboard details report

You can view the dashboard details report for a tiered dashboard from the **My Dashboards** view.

The details report is displayed in the **Dashboard Details Report** window.

You can view the following details in the window:

- Current overall status
- Status trends
- Current evaluation by status
- Evaluation trends

To view the dashboard details report

1. Go to Reporting > **My Dashboards** view of the console.
2. In the **My Dashboards** view, select a tiered dashboard and then right-click to select **View Details Report**.
3. In the **Dashboard Details Report** view, select the following options and check Show Details.
   - Set the trend of the data collection from the **Trend window** drop-down box.
Set the frequency scale of displaying the data in the **Time scale** drop-down box.

4 Click **Apply**.

See “**Viewing the dashboard trends report**” on page 785.

**Viewing the dashboard trends report**

You can view the dashboard trends report for a tiered dashboard from the **My Dashboards** view.

The trends report is displayed in the **Dashboard Trends Report** window in which you can view the following details of the dashboard:

- **Status trends**
  The status trends are displayed for the dashboard, section, and the evaluation node levels.

- **Evaluation trends**
  The evaluation trends are displayed for the dashboard and the section level only.

To view the dashboard trends report

1 Go to **Reporting > My Dashboards** view of the console.
2 In the **My Dashboards** view, select a tiered dashboard and right-click to select **View Trends Report**.
3 In the **Dashboard Trends Report** window select the following options and click **Apply**
   - Set the trend of the data collection from the **Trend window** drop-down box.
   - Set the frequency scale of displaying the data in the **Time scale** drop-down box.

See “**Viewing the dashboard details report**” on page 784.
Working with tiered dashboards
Managing custom content

This chapter includes the following topics:

- About the Content view
- About custom content
- Creating custom content
- Performing policy analysis

About the Content view

The Content view let you create and manage custom content in the Control Compliance Suite. It also lets you map your policies to control statements and control statements to checks, questions, and third-party controls.

You can access the Content view from Manage > Content.

You can use the view to start the Symantec Content Studio. You can click Content Studio to open the Symantec Content Studio.

See “About Symantec Content Studio” on page 789.

See “About custom content” on page 788.

See “Creating custom content” on page 792.

See “About mandates” on page 790.

See “About control statements” on page 791.

See “Performing policy analysis” on page 804.
About custom content

The Symantec Content Studio lets you customize content to fit the needs of your enterprise. The custom control statements and the custom mandates help you create the policies that suit the regulatory environment that your enterprise must inhabit. You use the Content Studio to map Symantec-created control statements and custom control statements to the custom mandates that you create and to your policies. You also map any of the control statement to checks, questions, or extended controls. You can also use the Content Studio to analyze your policies to help understand the scope of your policy coverage.

The Content Studio includes a large number of Symantec-created control statements. In addition, the Content Studio lets you create your own control statements. Any control statements can be mapped to the regulations or frameworks that you create. You can also map control statements to any Control Compliance Suite (CCS) policy in the Draft state. The Content Studio also lets you map control statements to checks, to questions from the Response Assessment module or to extended controls.

When you use Content Studio, you can start from the high-level regulations or frameworks that you require. Alternatively, you can begin from the individual control statements, then build from control statements into regulations or frameworks. Normally, you start by carefully analyzing the regulation or framework to determine the control statements that are required. This analysis lets you reuse control statements in multiple sections of the regulation or framework.

After these pieces are in place, you map checks, questions, and extended controls to control statements. Next, you map the control statements to the regulations or frameworks that you created. Then you map the control statements to your draft policies and perform policy analysis.

You can do the following using the custom content feature:

- Create custom control statements.
- Create custom regulatory content.
- Map custom control statements and Symantec provided control statements to custom regulatory content.
- Map control statements to checks, questions, and extended controls.
- Map policies to control statements.

See “Creating custom content” on page 792.
About Symantec Content Studio

The Symantec Content Studio lets you manage Symantec-created content in the Control Compliance Suite (CCS). It also lets you create your own custom content that can be used in the same way that you use Symantec-created content. Content consists of the regulations, frameworks, and control statements that underlie the policies that you create and publish. Custom content lets you fit CCS to your unique regulatory or framework needs. You use the Content Studio to map mandates and policies to control statements and control statements to checks, questions, and extended controls. Mappings link the regulations and frameworks that affect your enterprise, the policies you create to meet those mandates, and the underlying control statements, checks, questions, and extended controls.

You use the Content Studio in the Manage > Content view to map mandates, policies, and control statements, and to create custom content.

You can create the following custom content types:

- Regulations
- Frameworks
- Control statements

You can map any Symantec-created control statements that are included with CCS to the regulations or frameworks that you create. You can also map control statements you create to the regulations or frameworks that you create or to the CCS policies. You can also map control statements to checks, to questions from the Response Assessment module or to extended controls.

After you have created your custom content, you can use this content in CCS.

When you use the Content Studio, you can start from the high-level regulations or frameworks that you require. Alternatively, you can begin from the individual control statements, then build from control statements into regulations or frameworks. You start by carefully analyzing the regulation or framework to determine the control statements that are required. This analysis lets you reuse control statements in multiple sections of the regulation or framework, or in multiple policies. You can also use Symantec-created control statements in your custom regulations, frameworks, or policies.

After these pieces are in place, you map the regulations or frameworks you created to the control statements. You then map the control statements to the checks, questions, and extended controls. Finally, you create the new policies that match the mandates you use and map the control statements to those policies.

See “About custom content” on page 788.

See “Creating custom content” on page 792.
About mandates

A mandate is made up of one or more sections, each of which can optionally have one or more subsections.

A mandate has the following attributes:

- **Heading**
  
  Use the heading to assign a name to the mandate.

- **Prefix**
  
  Use to store any section number the mandate has. When the mandate is displayed in the Mandates area, the Content Studio displays the prefix, then the heading.

- **Levels**
  
  If the mandate has multiple levels, you can create and assign levels to the mandate or to the sections. A mandate and its subsections all use the same group of levels. If you edit levels in any part of a mandate, the levels change in every section.

- **Author**
  
  The name of the user who created the mandate.

  The author for all Symantec-created content is “Symantec.”

  The author for all custom content is the name of the name that was logged on when the mandate was created.

- **Path**
  
  The path in the mandate list to the mandate or to the section.

- **Body**
  
  The text of the mandate or the section.

- **Statement mappings**
  
  A list of the statements that you have mapped to the mandate or the section.

See “About custom content” on page 788.

See “Creating custom content” on page 792.

See “Modifying the details of a custom mandate or section” on page 794.

See “Mapping mandates to control statements” on page 795.

About regulations

Regulations are published government mandates such as HIPAA, Sarbanes-Oxley, or GLBA. These regulations describe the business functions and security functions that must be performed, usually with limited information on the implementation details.

The following are some of the regulations for which predefined policies exist:

- **HIPAA**
  
  Health Insurance Portability and Accountability Act
About frameworks

Frameworks are published best practices such as COBIT, COSO, and the ISO series. These frameworks describe implementation details. An example of such details is that the password policy should contain entries for length, complexity, and rotation.

The following are some of the frameworks for which predefined policies exist:

- COBIT: Control Objectives for Information and related Technology
- NIST: National Institute of Standards and Technology
- ISO: International Standards Organization
- COSO: Committee of Sponsoring Organizations of the Treadway Commission

About control statements

A control statement is a concise statement of a discrete portion of a regulation or framework. Since regulations and frameworks have large areas of overlap, the control statements reduce repetition by stating each portion a single time. For example, where differences exist between regulation or framework statement requirements, a single control statement exists that each of the entries is mapped to. The organizational mapping of policies to the control statement satisfies both the regulation and the framework requirements.

A control statement is mapped when it is linked to a mandate, policy, check, question, or extended control. Policies and mandates are mapped to control
statements. In turn, control statements are mapped to checks, questions, and extended controls.

A custom control statement is a control statement that you create to suit your enterprise needs. It may have none or minimal overlap with the control statements that Symantec provides with the Control Compliance Suite (CCS) content. The primary attribute of the custom control statement is that it meets your needs.

See “About custom content” on page 788.
See “Creating custom content” on page 792.
See “Mapping mandates to control statements” on page 795.
See “Mapping policies to control statements” on page 797.
See “Mapping checks to control statements” on page 799.
See “Mapping questions to control statements” on page 801.
See “Mapping extended controls to control statements” on page 803.
See “Viewing the control statements mapped to a regulation, framework, or policy” on page 806.

Creating custom content

The Symantec Content Studio lets you create your own custom content. Custom content consists of the regulations, the frameworks, or the control statements that you create to match your unique Policy needs.

Generally, you do the following when you create custom content:

■ Create custom regulations or frameworks.
■ Review the Symantec-provided control statements to find any that are applicable.
■ Create any needed custom control statements.
■ Map the subsections of your custom regulations or frameworks to your custom control statements or to the Symantec-created control statements.
■ Map control statements to questions, standards, extended controls, or any combination.
■ Create new policies in the Control Compliance Suite (CCS), then while the policies are in the Draft state map the policies to control statements.

You use the Symantec Content Studio to create and modify custom content. You can also use it to map user-created checks, extended controls, and questions to
the included control statements. You click **Manage > Content > Content Studio** to open the Content Studio.

See “**About Symantec Content Studio**” on page 789.

See “**About custom content**” on page 788.

### Creating a custom mandate or section

A mandate is a regulation or framework that you must comply with. The Symantec Content Studio lets you create the custom mandates that fit your specific needs. You can also map custom mandates to control statements in the Content Studio. Any regulation or framework is a mandate.

**To create a custom mandate**

1. In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Mandates**.

2. Do one of the following:
   - Click **New**, then click **Regulation** or **Framework**.
   - In the Mandates area, right-click, then click **New Regulation** or **New Framework**.
   - Click the mandate to add a section to, then click **New**, then click **Section**, then click **Under, Before, or After**.
   - In the Mandates area, right-click the mandate to add a section to, then click **New Section**.

3. In the Heading field of the details pane, you can type a name for the new regulation or framework.

4. In the Prefix field of the details pane, you can type a section number for the new regulation or framework.

5. To add levels to the mandate, click **Edit**.

6. In the **Edit Levels** dialog box, click the add icon with the yellow plus (+) symbol to add a level. Then type a name and description of the level. Click **OK** to close the dialog box and save the new levels.

7. In the details pane, type the text of the mandate in the body field.

8. Click **Save**.

See “**About custom content**” on page 788.

See “**About mandates**” on page 790.

See “**Modifying the details of a custom mandate or section**” on page 794.
Modifying the details of a custom mandate or section

After you have created a mandate or section, you can make changes to it in the Symantec Content Studio. You can change any of the mandate attributes or section attributes. You can also add new sections to the mandate or section.

You also use the mandates workspace to map statements to the custom mandates.

**To modify a mandate or section**

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click **Mandates**.
2. Click the mandate or section to which you want to make changes.
3. Make any needed changes to the mandate or section.
4. Click **Save**.

Creating custom control statements

Custom control statements let you define how you meet the requirements of the custom mandates you create.

You can create control statements from start or you can create by copying from an existing custom or predefined statements. When you copy control statements the mappings to checks, questions, and extended controls of the control statement are copied too. The mappings to policies and mandates are not copied.

**To create a custom control statement from start**

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click **Statements**.
2. Do one of the following:
   - Click **New**, then click **Statement**.
   - In the Statements area, right-click, then click **New Statement**.
3 In the **Heading** box of the **Details** pane, you can type a name for the new statement.

4 In the **Body** box of the **Details** pane, you can type the control statement content.

5 Select a status for the control statement from the Status options.

6 Click **Save**.

**To create a custom control statement from an existing statement**

1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.

2 In the Statements area, right-click a control statement, then click **Copy**.

3 Click **Paste** to create a copy of the selected control statement.

4 In the **Heading** box of the **Details** pane, modify the name of the statement.

5 In the **Body** box of the **Details** pane, modify the control statement content.

6 Select a status for the control statement from the Status options.

7 Click **Save**.

See “**What is a control statement?**” on page 687.

See “**Mapping mandates to control statements**” on page 795.

See “**Mapping policies to control statements**” on page 797.

See “**Mapping checks to control statements**” on page 799.

See “**Mapping questions to control statements**” on page 801.

See “**Mapping extended controls to control statements**” on page 803.

See “**Viewing the control statements mapped to a regulation, framework, or policy**” on page 806.

**Mapping mandates to control statements**

The Symantec Content Studio lets you map multiple control statements to a single mandate. When you do so, you tie the mandate to every control statement that is relevant to the mandate. You can also map a single control statement to one or more mandates.

---

**Note:** You must always map the control statements to a section in the mandate and not to root of the mandate.
You can use the **Mandates** view to map one or more control statements to a single mandate. You can also use the **Statements** view to map a single control statement to one or more mandates.

**To map one or more control statements to a single mandate**

1. In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Mandates**.
2. Click the mandate section that you want to map control statements to.
3. Click **Statement Mappings**.
4. Locate the statement that you want to map to the section in the Available Statements table and do one of the following:
   - Click the statement, then click the up arrow icon to map it to the section.
   - Click the statement and drag it to the Mapped Statements table.
5. Click **Save**.

**To remove a mapped control statement from a mandate**

1. In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Mandates**.
2. Click the mandate section that you want to remove the mapped control statements from.
3. Click **Statement Mappings**.
4. Locate the statement that you want to remove from the mandate section in the Mapped Statements table and do one of the following:
   - Click the statement, then click the down arrow icon to remove the mapping to the mandate section.
   - Click the statement and drag the statement to the Available Statements table.
5. Click **Save**.

**To map a single control statement to one or more mandates**

1. In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
2. Click the control statement that you want to map to one or more mandates.
3. Click **Mandate Mappings**.
4 Click All Mandates to display the list of mandates in the Content Studio.
5 Select a mandate section the control statement should be mapped to, and click the add icon with the yellow plus (+) symbol.

The added mandate sections are shown grouped by mandate in the Mapped Sections area.

To remove one or more mandates from a single control statement
1 In the navigation bar in the lower left corner of the Symantec Content Studio window, click Statements.
2 Click the control statement that you want to remove one or more mandates from.
3 Click Mandate Mappings.
4 Click All Mandates to display the list of mandates in the Content Studio.
5 Select a mandate to remove, and do one of the following:
   ■ Click the remove icon with the red X symbol.
   ■ Drag the mandate from the Mapped Sections area to the All Mandates area.

See “About custom content” on page 788.
See “About mandates” on page 790.
See “About control statements” on page 791.
See “Creating custom content” on page 792.
See “Viewing the control statements mapped to a regulation, framework, or policy ” on page 806.

Mapping policies to control statements

By mapping policies to control statements, you connect the mandates that you must comply with to the policies that validate compliance.

You can use the Policies view to map one or more control statements to a single policy. You can also use the Statements view to map a single control statement to one or more policies.

To map one or more control statements to a policy
1 In the navigation bar in the lower left corner of the Symantec Content Studio window, click Policies.
2 Click the policy that you want to map control statements to.
3 Locate the statement that you want to map to the mandate in the Available Statements table and do one of the following:
- Click the statement, then click the up arrow icon to map it to the mandate.
- Click the statement and drag it to the Mapped Statements table.

4 Click Save.

To remove a mapped control statement from a policy

1 In the navigation bar in the lower left corner of the Symantec Content Studio window, click Policies.

2 Click the policies that you want to remove the mapped control statements from.

3 Locate the statement that you want to remove from the mandate in the Mapped Statements table and do one of the following:
- Click the statement, then click the down arrow icon to remove the mapping to the mandate.
- Click the statement and drag the statement to the Available Statements table.

4 Click Save.

To map one or more policies to a single control statement

1 In the navigation bar in the lower left corner of the Symantec Content Studio window, click Statements.

2 Click the control statement that you want to map one or more extended controls to.

3 Click Policy Mappings.

4 Click All Policies to display the list of policies.

5 Select a policy that should be mapped to the control statement, and do one of the following:
- Click the add icon with the yellow plus (+) symbol.
- Drag the policy to the Mapped Policies area.

To remove one or more policies from a single control statement

1 In the navigation bar in the lower left corner of the Symantec Content Studio window, click Statements.

2 Click the control statement that you want to remove one or more policies from.
3 Click **Policy Mappings**.

4 In the **Mapped** area, select a policy to remove, and do one of the following:
   - Click the remove icon with the red X symbol.
   - Drag the check from the **Mapped** area to the **All Policies** area.

See “About Symantec Content Studio” on page 789.

See “Creating custom content” on page 792.

See “Creating custom control statements” on page 794.

See “Mapping mandates to control statements” on page 795.

See “Mapping checks to control statements” on page 799.

See “Mapping questions to control statements” on page 801.

### Mapping checks to control statements

By mapping checks to control statements, you connect the mandates that you must comply with to the checks that validate compliance.

You can use the **Standards** view to map one or more control statements to a single check. You can also use the **Statements** view to map a single control statement to one or more checks.

If a standard contains one or more copied checks, you can clone the control statements that are mapped to the checks.

**To map a single control statement to one or more checks**

1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.

2 Click the control statement that you want to map one or more checks to.

3 Click **Check Mappings**.

4 Click **All Checks** to display the list of checks in groups by standard in the Content Studio.

5 Select a check that should be mapped to the control statement, and do one of the following:
   - Click the add icon with the yellow plus (+) symbol.
   - Drag the check to the Mapped Checks area.

The added checks are shown grouped by standard in the Mapped Checks area.
To remove one or more checks from a single control statement

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Statements.
2. Click the control statement that you want to remove one or more checks from.
3. Click Check Mappings.
4. Click All Checks to display the list of checks that in groups by standard in the Content Studio.
5. Select a check to remove, and do one of the following:
   - Click the remove icon with the red X symbol.
   - Drag the check from the Mapped Checks area to the All Checks area.

To map a single check to one or more control statements

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Standards.
2. Click the check that you want to map one or more control statements to.
3. Select a statement that should be mapped to the check, and do one of the following:
   - Click the statement, then click the up arrow icon to map it to the check.
   - Drag the statement to the Mapped Statements area.

To unmap one or more control statements from a single check

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Standards.
2. Click the check that you want to remove one or more control statements from.
3. Select a statement to remove, and do one of the following:
   - Click the statement, then click the down arrow icon to unmap it from the check.
   - Drag the statement from the Mapped Statements area to the Available Statements area.

To clone the control statements that are mapped to a copied check

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Standards.
2. Right-click the group, standard, or check that includes copied checks.
3. Click Clone Mappings.
4. In the dialog box, click Ok.
Mapping questions to control statements

By mapping a Response Assessment question to a control statement, you take advantage of the built-in Response Assessment ability to track policy acceptance. You can use the Questions view to map one or more control statements to a single question. You can also use the Statements view to map a single control statement to one or more questions.

Before you map questions to control statements, you must connect the Content Studio to the Response Assessment module Server.

To connect the Content Studio to the Response Assessment module Server

1  In the navigation bar in the lower left corner of the Symantec Content Studio window, click Questions.
2  Right-click the Questions area on the left of the Content Studio dialog, then click Connect.
3  In the Select a Response Assessment module Server dialog, enter the name or IP address of the Response Assessment module server in the Server field. You can also select the server name from the drop-down list.
4  Enter the port to connect to the server in the Port. The default port is 1977.
5  Click OK to connect to the server.

To map one or more questions to a single control statement

1  In the navigation bar in the lower left corner of the Symantec Content Studio window, click Statements.
2  Click the control statement that you want to map one or more questions to.
3  Click Question Mappings.
4  Click All Questions to display the list of Questions in the Content Studio.
5  Select a question that should be mapped to the control statement, and do one of the following:
   ■  Click the add icon with the yellow plus (+) symbol.
   ■  Drag the check to the Mapped Questions area.
To remove one or more questions from single control statement

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click **Statements**.
2. Click the control statement that you want to remove one or more questions from.
3. Click **Question Mappings**.
4. Click **All Questions** to display the list of questions in the Content Studio.
5. Select a question to remove, and do one of the following:
   - Click the remove icon with the red X symbol.
   - Drag the question from the Mapped Questions area to the All Questions area.

To map a single question to one or more control statements

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click **Questions**.
2. Click the question that you want to map one or more control statements to.
3. Select a control statement that should be mapped to the question, and do one of the following:
   - Click the statement, then click the up arrow icon to map it to the question.
   - Drag the statement to the Mapped Statements area.

To unmap one or more control statements from a single question

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click **Questions**.
2. Click the question that you want to remove one or more control statements from.
3. Select a statement to remove, and do one of the following:
   - Click the statement, then click the down arrow icon to unmap it from the question.
   - Drag the statement from the Mapped Statements area to the Available Statements area.

See “About Symantec Content Studio” on page 789.

See “Creating custom content” on page 792.
Mapping extended controls to control statements

You can use the Symantec Content Studio to map control statements to evidence from extended evidence source. These sources include the following:

- Symantec Data Loss Prevention Connector
- Data the Control Compliance Suite (CCS) collects from CSV and ODBC data sources.

You can use the Extended Controls view to map one or more control statements to a single control. You can also use the Statements view to map a single control statement to one or more extended controls.

To map one or more control statements to a single extended control

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Extended Controls.
2. In the Extended Controls area, select the extended control that you want to map one or more control statements to.
3. In the Available Statements area, select a statement that should be mapped to the extended control, and do one of the following:
   - Click the statement, then click the up arrow icon to map it to the check.
   - Drag the statement to the Mapped Statements area.

To unmap one or more control statements from a single extended control

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Extended Controls.
2. In the Extended Controls area, select the extended control that you want to remove one or more control statements from.
3. In the Available Statements area, select a statement to remove, and do one of the following:
   - Click the statement, then click the down arrow icon to unmap it from the check.
   - Drag the statement from the Mapped Statements area to the Available Statements area.

To map one or more extended controls to a single control statement

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Statements.
2. Click the control statement that you want to map one or more extended controls to.
Performing policy analysis

You use the Symantec Content Studio to map the mandates with which you must comply to control statements. You also map the policies you create to the control statements. Policy analysis lets you view these mappings graphically to ensure that your policies completely cover the mandates.

Both policies and mandates are mapped to control statements. Policy analysis helps you view the control statements that are mapped to the mandates you must follow. You can then analyze those control statements and locate the control statements that are not mapped to a policy. This analysis helps you to ensure that your policies correctly implement the mandates with which you must comply.

When you find gaps in coverage, you can create additional policies and map them to the control statements.

When you perform policy analysis, you do the following:

- Click Extended Control Mappings.
- Click All Controls to display the list of extended controls.
- Select an extended control that should be mapped to the control statement, and do one of the following:
  - Click the add icon with the yellow plus (+) symbol.
  - Drag the extended control to the Mapped area.

To remove one or more extended controls from a single control statement

1. In the navigation bar in the lower left corner of the Symantec Content Studio window, click Statements.
2. Click the control statement that you want to remove one or more extended controls from.
3. Click Extended Control Mappings.
4. In the Mapped area, select an extended control to remove, and click the remove icon with the red X symbol.

See “About custom content” on page 788.

See “Creating custom content” on page 792.

See “About importing assets from Altiris” on page 411.

See “About importing incident data from Symantec Data Loss Prevention” on page 421.

See “Working with evidence sources” on page 821.
Map control statements to the mandates with which you must comply.

Map control statements to your policies.

Use the analysis view to view the links between the mandates and the control statements.

Simultaneously view the links between the policies and the control statements.

Locate any control statements that you mapped to mandates that are not also mapped to policies.

Repeat as necessary until all of the control statements are mapped to both mandates and policies.

See “About custom content” on page 788.

See “Creating custom content” on page 792.

See “About the Analysis view” on page 805.

See “Viewing the control statements mapped to a regulation, framework, or policy” on page 806.

See “Performing a gap analysis” on page 807.

About the Analysis view

The Analysis view lets you map policies and policy templates to regulations and best-practice frameworks. The Analysis view also lets you see the existing gaps in compliance between currently defined policies and the security regulations.

After you have analyzed the existing relationships, you can use the other views in the Symantec Content Studio to map control statements to required regulations and frameworks.

You can drag any regulation, framework, or policy from the tree view into the Analysis pane. You can drag multiple items into the view to examine their shared control statements.

In the Analysis view, the following icons and links are used to represent the different objects and their relationships on the map area:

- Depicts a control statement
- Depicts a regulation
- Depicts a policy or a policy template
- Depicts a framework
Viewing the control statements mapped to a regulation, framework, or policy

You can use the Analysis view to review the control statements that are mapped to one or more regulations, best-practice frameworks, or policies. You can use this view to determine the gaps between the regulations and frameworks with which you must comply and the policies you use to enforce those requirements.

You can view regulations, frameworks, and policies one at a time or in groups. You should use the content studio to map your frameworks and regulations to the control statements and map the control statements in turn to your policies. When mapping is complete, every framework or regulation should map to one or more control statements. Every control statement should in turn map to one or more policies. Through their mutual maps to shared control statements, every framework or regulation will be linked to one or more policies.

To view the control statements that are mapped to a regulation, framework, or policy

1. In the Symantec Content Studio window, on the navigation bar, click Analysis.

2. In the tree view, drag and drop any regulation, framework, or policy to the map area.
In the Analysis View, do one of the following:

- Right-click a control statement, and then click **Expand > Regulation** to display the regulations mapped to the control statement.
- Right-click a control statement, and then click **Expand > Frameworks** to display the frameworks mapped to the control statement.
- Right-click a control statement, and then click **Expand > Policies** to display the policies mapped to the control statement.
- Right-click a control statement, and then click **Expand > All** to display all regulations, frameworks, and policies linked to the control statement.
- Right-click any object and click **Remove** to remove it from the **Analysis** view.

If desired, return to 2 and add an additional regulation, framework, or policy.

See “**About custom content**” on page 788.

See “**Creating custom content**” on page 792.

See “**Performing policy analysis**” on page 804.

See “**About the Analysis view**” on page 805.

See “**Performing a gap analysis**” on page 807.

### Performing a gap analysis

Gap analysis helps you to review your enterprise mandates and policies. The analysis view lets you see how the mandates relate to one another and to the policies that you have mapped to those mandates. Gap analysis can help you to locate areas where you need to create additional policies to close any existing gaps in your policy coverage.

**To perform a gap analysis**

1. In the **Symantec Content Studio** window, click **Analysis**.
2. In the tree view, expand the Policies node.
3. Locate the required policy and drag it to the map area.
4. In the tree view, expand the Regulation or Framework node.
5. Locate the section relevant to the policy and drag it to the map area.
6. Click **Auto Layout**. The Auto Layout feature redraws the map with a balanced spacing between all the objects and zooms out so that the whole map is visible.
7. You can see the control statements that are not mapped to the policy. Use the Content Studio to map these Statements to the policy.
See “About custom content” on page 788.
See “Creating custom content” on page 792.
See “Performing policy analysis” on page 804.
See “About the Analysis view” on page 805.
See “Viewing the control statements mapped to a regulation, framework, or policy” on page 806.
Managing extended evidence sources

This chapter includes the following topics:
■ About the extended evidence sources system
■ End-to-end sequence of evidence import
■ Working with evidence sources
■ Working with extended controls
■ Working with evidence

About the extended evidence sources system

The Control Compliance Suite (CCS) assesses and reports on the risk and compliance posture of an organization. Sometimes, the organizations use external tools or applications other than CCS to get a complete compliance and risk compatibility status. These external applications generate important evidence that is used for reporting on the compliance compatibility of the organization.

CCS provides a mechanism to extend the evidence collection capabilities through the extended evidence sources system. This system lets you collect evidence from the applications which are external to CCS and contribute towards the risk and compliance assessment and reporting process. The extended evidence sources system lets you add an evidence source in CCS. Configure the evidence source to read the evidence data, which must be arranged in the format that is defined in CCS. After you convert the evidence data of the external application into the defined format, configure the evidence source to collect this data periodically. The extended evidence sources system leverages the evidence source to contribute to the risk and compliance scores of the CCS assets.
The extended evidence source system also provides a mechanism for extending the controls which are used to assess the CCS assets. You can register the extended controls of an external application with this system and also map them with the control statements. The evidence source configuration, the evidence that you import, and the extended controls are stored in the evidence database, CSM_EvidenceDB.

See “About the Extended Evidence Sources view” on page 810.
See “Working with evidence sources ” on page 821.
See “Working with extended controls” on page 825.
See “Working with evidence ” on page 832.
See “Mapping extended controls to control statements” on page 803.
See “About control statements” on page 791.

About the Extended Evidence Sources view

The Extended Evidence Sources view provides a rolled-up display of the configured evidence sources that you add to the extended evidence source system. You can access the Extended Evidence Sources view by navigating through the Manage > Extended Evidence Sources menu of the console.

The Extended Evidence Sources view contains the following columns and fields:

Table 20-1 Provides the columns and their descriptions

<table>
<thead>
<tr>
<th>Field or Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Name</td>
<td>Displays the names of the evidence source that you add.</td>
</tr>
<tr>
<td></td>
<td>An evidence source must be added to the system before you import evidence or extended controls from any external applications. The evidence collection job that is created in the Jobs view is of the same name as that of the evidence source.</td>
</tr>
<tr>
<td>Control Type</td>
<td>Displays the control type that you set for the evidence source when adding it.</td>
</tr>
<tr>
<td></td>
<td>The control types can either be Technical or Procedural.</td>
</tr>
<tr>
<td></td>
<td>See “About extended controls and control types” on page 813.</td>
</tr>
</tbody>
</table>
Table 20-1  Provides the columns and their descriptions *(continued)*

<table>
<thead>
<tr>
<th>Field or Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>Displays the schedule that is set for the evidence collection job. The evidence collection schedule is specific to every evidence source that you create.</td>
</tr>
<tr>
<td>Compute Compliance Score</td>
<td>Displays the option of whether the compliance score is calculated by the Control Compliance Suite or not. You set this option when you add the evidence source. If you have set the option for the evidence source, then the value displayed is True else the value displayed is False.</td>
</tr>
<tr>
<td>Compute Risk Score</td>
<td>Displays the option of whether the risk score is calculated by the Control Compliance Suite or not. You set this option when you add the evidence source. If you have set the option for the evidence source, then the value displayed is True else the value displayed is False.</td>
</tr>
<tr>
<td>Compliance Score Weight</td>
<td>Displays the weight that you specified for calculating the compliance score for the evidence source. You set the weight when you add the evidence source. The weight for calculating the compliance score must be between 0 and 1.</td>
</tr>
<tr>
<td>Risk Score Weight</td>
<td>Displays the weight that you specified for calculating the risk score for the evidence source. You set the weight when you add the evidence source. The weight for calculating the risk score must be between 0 and 1.</td>
</tr>
<tr>
<td>Search</td>
<td>Use this option to search for an evidence source that is listed for the view.</td>
</tr>
<tr>
<td>Clear</td>
<td>Use this option to clear the searched items that are displayed for the view.</td>
</tr>
</tbody>
</table>
Table 20-1 Provides the columns and their descriptions (continued)

<table>
<thead>
<tr>
<th>Field or Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column Chooser</td>
<td>Use this option to select the number of columns that you want to display for the view.</td>
</tr>
</tbody>
</table>

The tasks that you can perform through this view are as follows:

- Adding an evidence source
  See “Adding an evidence source” on page 822.
- Editing an evidence source
  See “Editing an evidence source” on page 824.
- Deleting an evidence source
  See “Deleting an evidence source” on page 824.
- Managing the extended controls
  See “Working with extended controls” on page 825.
- Viewing the imported evidence
  See “Viewing the imported evidence” on page 853.

See “About the extended evidence sources system” on page 809.
See “Working with evidence sources” on page 821.

About an evidence source

An evidence source refers to the external application, which can contribute to the risk and compliance assessment and reporting process of the Control Compliance Suite. You can add an evidence source for any external application into the extended evidence sources system through the Create or Edit Evidence Source wizard.

See “Adding an evidence source” on page 822.

You can configure an evidence source for any or all the following purposes:

- Collecting evidence data from the external applications
- Adding the extended controls used the external application
- Contributing to the risk score or the compliance score of the assets
- Calculating the risk and compliance score from the collected evidence

By default, the evidence sources of the applications such as Symantec Data Loss Prevention Connector and Response Assessment Module (RAM) are created in...
the **Extended Evidence Sources** workspace. These default evidence sources are created in the workspace automatically after you configure the applications in the Control Compliance Suite.

See “Working with evidence sources” on page 821.

**About extended controls and control types**

Extended controls refer to checks, policies, standards, or regulations that are used to assess or evaluate the assets. In the IT enterprises, assets are assessed against the extended controls for evaluating the compliance and risk compatibility. The Control Compliance Suite provides the infrastructure to extend the existing controls by importing or adding the extended controls of an external application. The extended controls are imported or added through the extended evidence source system. For example, you can import the extended controls of the application, Symantec Data Loss Prevention Connector into the Control Compliance Suite.

Extended controls are categorized into two types based on their function.

The control types are as follows:

- **Technical**
  The technical control type refers to the extended controls, which usually belong to the technical standards. Such technical standards are defined for various operating systems, which when evaluated against assets generate results such as pass or fail. For example, in Control Compliance Suite, the checks of the predefined standard for the Oracle platform, CIS Oracle 9i and 10g Database Security Benchmark v2.0 is a technical control type.

- **Procedural**
  The procedural control type refers to the extended controls, which are descriptive in definition and are used to make business decisions. Such controls are used for generic assessment of any business, which can also be non-technical. For example, the questionnaires of the Response Assessment Module of the Control Compliance Suite.

Before you add or import the extended controls you must add an evidence source to the extended evidence source system.

See “Adding an evidence source” on page 822.

The added or imported extended controls are stored in the evidence database, CSM_EvidenceDB. The extended controls are added or imported through the **Manage Extended Controls** dialog box. You can import the extended controls using various methods such as CSV file import or through APIs.

See “About methods to import the extended controls” on page 815.
The main advantage of importing the controls is to map the imported controls to the control statements through the Content Studio.

See “Mapping extended controls to control statements” on page 803.

See “Importing extended controls from a CSV file” on page 830.

See “Adding an extended control ” on page 826.

About evidence

In the Control Compliance Suite, the assessment results of evaluated assets are known as evidence. The assessment of assets is performed against well-defined regulations, standards, or policies of the IT enterprise. An evidence can either be positive or negative based on whether the assessment result of the evaluated asset is a pass or fail. Positive evidence refers to the additional information that is provided when an asset passes the assessment. Negative evidence refers to the information that is provided when the asset fails the assessment.

For example, you assess 20 Windows Server 2003 computers against the policy, SOX DSS Policy. A total number of 15 computers pass the evaluation while 5 computers fail. The evidence data that is collected from the assessment contain 15 passes and 5 fails. This evidence data is imported into the Control Compliance Suite and stored in the evidence database. You can generate reports and dashboards based on the collected evidence data to understand the overall compliance compatibility of the Windows Server 2003 computers.

You can import evidence of any application that is external to the Control Compliance Suite through a configured evidence source. The imported evidence is stored in the evidence database, CSM_EvidenceDB.

See “Adding an evidence source” on page 822.

You can import evidence using methods such as CSV file import, ODBC compliant database import, or through APIs.

See “About methods to import the evidence” on page 815.

You must add an evidence source through the Extended Evidence Sources view of the console before you import the evidence.

See “About an evidence source” on page 812.

See “About extended controls and control types” on page 813.

See “Importing evidence from CSV files or ODBC compliant databases” on page 849.
About methods to import the extended controls

Before you want to work with the extended controls of any external application, you must import them into the extended evidence system. It is important that you create an evidence source before you import the extended controls.

See “Adding an evidence source” on page 822.

The methods that are used to import the extended controls are as follows:

- CSV file import
- APIs

To learn about the APIs, refer to the Control Compliance Suite API Reference Guide that is located in the <product_install_directory>/Symantec/CCS/Reporting and Analytics/Documentation/API_Help.

Ensure that you arrange the extended controls information as per the defined format before you import them from the CSV files.

See “About CSV file format for extended controls” on page 826.

See “Importing extended controls from a CSV file” on page 830.

About methods to import the evidence

The Control Compliance Suite imports evidence using various methods such as CSV file import, ODBC compliant database import, and through APIs. To import evidence using the CSV file import or ODBC compliant database import methods, you must create data locations in the Control Compliance Suite. You can either create a data location through the Settings > General > Data Locations view of the console or when creating the evidence source.

You can associate one evidence source with one only data import methodology. For example, you create an evidence source, MyProvider that imports the evidence of an application, DLP. The import operation is performed through the CSV file import method. You cannot use the evidence source, MyProvider to import the evidence of the same application that is stored in an ODBC compliant database.

See “Configuring the data locations” on page 165.

The methods that are used to import evidence are as follows:

- CSV file import
- ODBC database connectivity
- APIs

To learn about the APIs, refer to the Control Compliance Suite API Reference Guide that is located in the
About compliance score contribution from an evidence source

An evidence source can contribute to the compliance score of assets present in the CCS asset system. The percentage of contribution is decided by the weights that are assigned to the evidence source for the compliance score calculations. The asset system calculates an average compliance score depending on the weights that are obtained from the CCS sources and the external evidence sources. The compliance score calculation is displayed in the details pane of the Asset system. The details pane also displays the break-up contribution of every source and the associated weight. This weighted average compliance score is also displayed in the reports which display the asset compliance score.

For every compliance score a corresponding weight must be set to quantify the severity of the compliance score of the assets. The compliance score is calculated based on the weight that is set for an evidence source. The value set as the weight of a compliance score must be within 0 and 1. For example, if the compliance score of an evidence source, P1 is 7 and weight is 0.5, then the total compliance score is 7*0.5, which equals 3.5. Similarly, if the compliance score of an evidence source, P2 is 9 and weight is 1, then the total compliance score is 9*1, which equals 9.

An evidence source can contribute to the compliance score of an asset through any of the following methods:

- Compliance score calculation of assets by CCS based on the collected evidence
  In this method, the aggregate compliance score of the assets is calculated for every evidence record and provided to the asset system.

- Compliance score calculation using the CCS Web service API
  In this method, the aggregate compliance score of the asset is calculated using the API, UpdateComplianceScore.
  To learn about the APIs, refer to the Control Compliance Suite API Reference Guide that is located in the <product_install_directory>/Symantec/CCS/Reporting and Analytics/Documentation/API_Help.
The aggregate compliance score of every asset is displayed in the **General** tab column of the **Asset system** view.

See “About risk score contribution from an evidence source” on page 817.

See “About compliance score calculation from evidence” on page 818.

### About risk score contribution from an evidence source

An evidence source can contribute to the risk score of the assets that are present in the Control Compliance Suite asset system. The percentage of contribution is decided by the weights that are assigned to the evidence source for the risk score calculations. The asset system calculates an average risk score for the assets based on the weights derived from the CCS sources and the external evidence sources. The risk score calculation is displayed in the details pane of the **Asset system**. The details pane also displays the break-up contribution of every source and the associated weight. This weighted average risk score is also displayed in the reports which display the asset risk score.

For every risk score a corresponding weight must be set as per the severity of the risk for the associated assets. The value set as the weight of a risk score must be within 0 and 1. For example, if the risk score of an evidence source, P1 is 5 and weight is 0.5, then the total risk score is 5 * 0.5, which equals 2.5. Similarly, if the risk score of an evidence source, P2 is 7 and weight is 1, then the total risk score is 7*1, which equals 7.

An evidence source contributes to the risk score of an asset through any of the following methods:

- **Risk score calculation of assets by CCS based on the collected evidence**
  
  In this method, the risk score of an asset is calculated for every evidence record that is imported into the extended evidence sources system.

  See “About risk score calculation from evidence” on page 818.

- **Risk score calculation using the CCS Web service API**
  
  In this method, the aggregate risk score of the asset is calculated using the API, UpdateRiskScore. The aggregate risk score is calculated by taking the weighted average of the evidence that is collected for an asset.

  To learn about the APIs, refer to the [Control Compliance Suite API Reference Guide](<product_install_directory>/Symantec/CCS/Reporting and Analytics/Documentation/API_Help).

  The aggregate risk score of an asset is displayed in the **General** tab column of the **Asset system** view.

  See “About risk score calculation from evidence” on page 818.
About compliance score calculation from evidence

In the Control Compliance Suite, the compliance score determines the compliance adherence level of the assets that are assessed against the extended controls. In the extended evidence sources system, the compliance score calculation is performed on the assessment results of the assets and the extended controls. The assessment results of the assets contain the evidence, which along with the extended controls are imported into the extended evidence sources system.

The compliance score is calculated for an asset based on the number of extended controls that pass or fail in an asset assessment.

The Control Compliance Suite uses the following formula to calculate the compliance score:

\[
\text{No. of checks passed}/(\text{total number of checks} - \text{not applicable checks})
\]

Irrespective of whether you import the extended controls for the evidence source or not, you can still configure the evidence source for the compliance score calculation. The compliance score option can be set through the Create or Edit Evidence Source wizard for every evidence source. You must also specify a weight through the same wizard for the compliance score calculation.

See “About risk score calculation from evidence” on page 818.

See “About compliance score contribution from an evidence source” on page 816.

About risk score calculation from evidence

Risk score is calculated for an asset only when an asset fails in the assessment that is performed against an extended control. In the Control Compliance Suite, risk score is used to quantify the vulnerability of the asset of an IT organization.

In the extended evidence sources system, the risk score calculation is performed on the assessment results of the assets and the extended controls. The assessment results of the assets contain the evidence, which along with the extended controls are imported into the extended evidence sources system. Hence, the risk score is specific to every evidence source that is associated with the imported evidence or extended controls.

Risk score is calculated from the CIA values of the asset and the Common Vulnerability Scoring System v2 (CVSS) values of the extended controls. You must import the extended controls and set the appropriate values for the CVSS attributes to derive the correct risk score values. If the CVSS attribute values of the extended controls are not set, then the risk score does not get calculated. Since, the CIA values of the assets are not gathered during evidence import, the Control Compliance Suite uses the default CIA values to calculate the risk score of the assets.
See “About risk score calculation” on page 657.

The risk score calculation is set through the Create or Edit Evidence Source wizard for every evidence source. You must also specify a weight through the same wizard for the risk score calculation.

See “About compliance score calculation from evidence” on page 818.

End-to-end sequence of evidence import

The Control Compliance Suite lets you import extended controls and evidence into the extended evidence sources system.

Table 20-2  Sequence of tasks to import evidence and their descriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an evidence source</td>
<td>You must add an evidence source to the extended evidence sources system and</td>
</tr>
<tr>
<td></td>
<td>configure it to import the extended controls and evidence.</td>
</tr>
<tr>
<td></td>
<td>See “Adding an evidence source” on page 822.</td>
</tr>
</tbody>
</table>
### Table 20-2  Sequence of tasks to import evidence and their descriptions

(continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Decide the method to import the evidence       | You must decide the method to import the evidence into the extended evidence sources system. See “About methods to import the extended controls” on page 815. Ensure to do the following based on the method you select to import the evidence:  
  - Arrange the evidence information in the CSV file as per the defined format. See “About CSV file format for evidence” on page 833.  
  - Arrange the evidence information for the ODBC compliant database columns as per the defined format. See “About ODBC mappings for evidence” on page 844.  
  You can also import the extended controls that resulted in the evidence generation when used to assess the assets. In the CSV file, ensure that you arrange the extended controls in the defined format for successful import operation. See “About CSV file format for extended controls” on page 826. |
| Add the extended controls                      | This step is optional for evidence import operation. You can add the extended controls to the extended evidence sources system through the Manage Extended Controls dialog box.                                                                                                           |
| Import the evidence into the extended evidence sources system | You can import the evidence through the Create or Edit Evidence Source wizard, which is used to add the evidence source. See “Importing evidence from CSV files or ODBC compliant databases” on page 849.                                                                                   |
Working with evidence sources

In the Control Compliance Suite, the extended evidence sources system imports extended controls or evidence through an evidence source. The imported extended controls and evidence belong to applications that are external to the Control Compliance Suite. You add an evidence source into the Control Compliance Suite infrastructure through the Manage > Extended Evidence Sources view of the console.

See “About the extended evidence sources system” on page 809.
See “About an evidence source” on page 812.

The evidence source imports the extended controls and evidence using methods that are interpreted by the extended evidence sources system.

See “About methods to import the extended controls” on page 815.

In the Extended Evidence Sources management, after you add the evidence source, you require to configure it for evidence collection. You can also edit an evidence source and delete it from the Manage > Extended Evidence Sources view of the console.

Before you start working with an evidence source, ensure that you perform the following:

- Configure the data location for the evidence source of the extended evidence sources system.
  See “Configuring the data locations” on page 165.

- Define the method to import the extended controls or evidence into the system. For example, if the method is CSV file import, then ensure that the file format contains the required headers. You must also ensure to enter the correct data corresponding to every header.
  See “About CSV file format for evidence” on page 833.
  See “About CSV file format for extended controls” on page 826.

- Add an evidence source to the extended evidence sources system.
  See “Adding an evidence source” on page 822.

See “Working with extended controls” on page 825.

See “Working with evidence” on page 832.

See “Editing an evidence source” on page 824.

See “Deleting an evidence source” on page 824.

Adding an evidence source

You add an evidence source to the extended evidence sources system through the Extended Evidence Sources view. Add the evidence source before you import an extended control or an evidence.

See “About the extended evidence sources system” on page 809.

You can add an evidence source to the system and configure it as an evidence collection job. View the evidence collection job details through the Jobs view of the console.
To add an evidence source and create an evidence collection job

1. Go to Manage > Extended Evidence Sources view of the console.
2. In the Extended Evidence Sources view, click Add Evidence Source.
   You can also right-click on the workspace of the Extended Evidence Sources view and select, Add Evidence Source.
3. In the Specify evidence source details panel of the Create or Edit Evidence Source wizard, enter the details for the evidence source and click Next.
   Check Create evidence collection job to create an evidence collection job for the evidence source that you configure.

   **Note:** The Create evidence collection job option cannot be edited after you create an evidence source.

4. In the Specify site and data locations panel of the wizard, associate an existing data location with the evidence source and click Next.
   You can also create a new data location through this panel and associate it with the evidence source.
5. In the Add reconciliation rules panel of the wizard, add the assets for which you want to import the evidence or extended controls and then click Next.
6. In the Schedule panel of the wizard, set the schedule for the evidence collection job and then click Next.
7. In the Specify scores details panel of the wizard, select the risk score and compliance score options and click Next.
8. In the Summary panel of the wizard, review the configuration details of the evidence source that you add to the extended evidence sources system.

You can also choose not to configure the evidence source as an evidence collection job.

To add an evidence source but not create an evidence collection job

1. Go to Manage > Extended Evidence Sources view of the console.
2. In the Extended Evidence Sources view, click Add Evidence Source.
   You can also right-click on the workspace of the Extended Evidence Sources view and select, Add Evidence Source.
3 In the **Specify evidence source details** panel of the **Create or Edit Evidence Source** wizard, enter the details for the evidence source and click **Next**.

4 In the **Specify scores details** panel of the wizard, select the risk score and compliance score options and click **Next**.

5 In the **Summary** panel of the wizard, review the configuration details of the evidence source that you add to the extended evidence sources system.

See “**Editing an evidence source**” on page 824.

### Editing an evidence source

You can edit an evidence source, which you have added to extended evidence sources system. The evidence source was through the **Extended Evidence Sources** view of the console.

**To edit an evidence source**

1. Go to Manage > **Extended Evidence Sources** view of the console.
2. Select an evidence source that is listed in the **Extended Evidence Sources** workspace and right-click on it to select **Edit Evidence Source**.
3. In the **Edit Evidence Source** wizard, edit the details of the evidence source by navigating through the wizard.

See “**Adding an evidence source**” on page 822.

See “**Deleting an evidence source**” on page 824.

### Deleting an evidence source

You can delete an evidence source from the extended evidence sources system through the **Extended Evidence Sources** view of the console.

---

**Note:** If you delete the evidence source, then the associated evidence collection job is also deleted.

**To delete an evidence source**

1. Go to Manage > **Extended Evidence Sources** view of the console.
2. In the **Extended Evidence Sources** workspace, select an evidence source, right-click on it and select **Delete Evidence Source**.
3. Read the message that prompts and click **Yes** to delete the evidence source.
Working with extended controls

In the Control Compliance Suite, the extended evidence sources system provides the infrastructure to import the extended controls of any application. Before you import the extended controls into the extended evidence sources system, you must know about the extended controls and the control types.

See “About extended controls and control types” on page 813.

You can add, edit, delete, and import the extended controls through the Manage Extended Controls dialog box of the Extended Evidence Sources view of the console.

The extended controls are imported into the system using various methods such as CSV file import or APIs.

See “About methods to import the extended controls” on page 815.

One of the main advantages to import the extended controls into the system is to map them to the control statements through the Content Studio of the Control Compliance Suite.

See “Mapping extended controls to control statements” on page 803.

Before you start working with the extended controls, ensure that you perform the following:

- Add an evidence source to the extended evidence sources system
  In the extended evidence sources system, you require to add an evidence source before you import the extended controls.
  See “Adding an evidence source” on page 822.

- Configure the CSV file from which you want to import the extended controls.
  For example, the CSV file that contains the extended controls information must be formatted with specific headers. The extended controls information must be arranged accordingly for each of the headers of the file.
  See “About CSV file format for extended controls” on page 826.

- Add or import the controls into the extended evidence sources system.
  See “Adding an extended control” on page 826.
  To import the controls, you must browse to the folder where the CSV file that contains the extended controls is located.
  See “Importing extended controls from a CSV file” on page 830.
Adding an extended control

You can add one or more extended controls to an evidence source of the extended evidence sources system. Before you add an extended control to the system, you must add an evidence source.

See “Adding an evidence source” on page 822.

To add an extended control to an evidence source

1. Go to Manage > Extended Evidence Sources view of the console.
2. In the Extended Evidence Sources view, click Manage Extended Controls.
3. In the Manage Extended Controls dialog box, select the evidence source from the down-down list, Select Evidence Source.
4. Click the Add Control icon.
5. In the Add Control dialog box, enter the details of the extended control that you want to add.

See “Editing an extended control” on page 831.

See “Deleting an extended control” on page 831.

See “Mapping extended controls to control statements” on page 803.

About CSV file format for extended controls

You can import the extended controls into the extended evidence sources system using the CSV file import method. To register the extended controls with the system, you must define the extended controls information in a specific CSV file format.

Do the following to create the CSV file with the extended controls information:

- Understand the definition of the CSV file headers from the table and gather the related information for the extended controls.
- Define specific headers in the CSV file as per the format.
- Arrange the extended controls information correctly for the defined headers in the CSV file.

The CSV file headers and their descriptions that you must specify in a CSV file are as follows:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlID</td>
<td>Specify the unique identifier (ID) of the extended control that you add. The external application defines the IDs.</td>
</tr>
<tr>
<td>ControlName</td>
<td>Specify the name of the extended control that you add. You can specify the same name of the extended control as available in the external application or specify a new name.</td>
</tr>
<tr>
<td>Category</td>
<td>Specify a category for the extended control that you add. Categories are used to group the controls and map them with the extended control statements through the <strong>Content Studio</strong>. For example, in Symantec Data Loss Prevention Connector, a policy when violated results in incidents. The categories of incidents are, network, discover, and endpoint.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description for the extended control that you add.</td>
</tr>
</tbody>
</table>
| Confidentiality | Select a value from the drop-down list for this risk attribute that measures the impact to confidentiality if a check fails. Confidentiality is the act of limiting the access and disclosure of information to only authorized users. The impact of unauthorized disclosure of confidential information can lead to security risk, loss of public confidence, or legal action against the organization. Select any of the following value for the attribute:  
  - No Impact  
  - Partial  
  - Complete  
  See “Check risk attributes” on page 584. |
Integrity

Select a value from the drop-down list for this attribute, which measures the impact of the integrity if a specific check fails.

Integrity refers to the genuineness of the information. Integrity dictates that information must be protected from improper modification. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. Continuous use of corrupted data can result in inaccuracy, fraud, or erroneous decisions.

Select any of the following value for the attribute:

- No Impact
- Partial
- Complete

See “Check risk attributes” on page 584.

Availability

Select a value from the drop-down list of this attribute that measures the impact to availability if a specified check fails.

Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space affect the availability of a system. If a mission-critical asset is unavailable to its end users, the mission of the organization may be affected.

Select any of the following value for the attribute:

- No Impact
- Partial
- Complete

See “Check risk attributes” on page 584.
Access Vector

Select a value from the drop-down list of this attribute that reflects how vulnerability is exploited in a system.

According to the type of access that is required for the attacker to exploit the vulnerability, this attribute can be assigned the following values:

- Local accessible
- Adjacent Network Accessible
- Network Accessible

See “Check risk attributes” on page 584.

Access Complexity

Select a value from the drop-down list of this attribute that measures the complexity of the attack that is required to exploit the vulnerability in a system.

The possible values for this attribute are as follows:

- Low
- Medium
- High

See “Check risk attributes” on page 584.

Authentication

Select a value from the drop-down list of this attribute that measures the number of times an attacker must authenticate to a target for exploiting the vulnerability.

This attribute does not measure the strength or complexity of the authentication process. Authentication gauges only the fact whether an attacker is required to provide credentials before the exploration of the vulnerability.

The possible values for this attribute are as follows:

- Multiple Instances
- Single Instance
- No Authentication

See “Check risk attributes” on page 584.

For example, you want to import an extended control or policy of Symantec Data Loss Prevention Connector. A predefined policy, Payment Card Industry Data
Security Standard when violated, results in an incident of category, Network. You must arrange the policy information in the CSV file as per the defined format.

The CSV file format for the Symantec Data Loss Prevention Connector policy is as follows:

<table>
<thead>
<tr>
<th>ControlID</th>
<th>ControlName</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Payment Card Industry Data Security Standard</td>
<td>Network</td>
<td>The Payment Card Industry (PCI) Data Security Standard (DSS) is jointly determined by the major payment card companies such as Visa and MasterCard. This comprehensive standard is intended to help organizations proactively protect customer account data. This policy detects the credit card data, which if exposed can represent a violation of this standard.</td>
</tr>
</tbody>
</table>

See “Importing extended controls from a CSV file” on page 830.

See “About methods to import the extended controls” on page 815.

Importing extended controls from a CSV file

You can import the extended controls from a CSV file into the extended evidence sources system through the Manage Extended Controls dialog box. Before you import the extended controls, ensure that the controls information are arranged in the CSV file as per the defined format.

See “About CSV file format for extended controls” on page 826.

To import the extended controls from a CSV file

1. Go to Manage > Extended Evidence Sources view of the console.
2. In the Extended Evidence Sources view, click Manage Extended Controls.
3. In the Manage Extended Controls dialog box, select the evidence source from the down-down list, Select Evidence Source.
   
   You must add an evidence source before you import the extended controls into the system.

   See “Adding an evidence source” on page 822.

4. In the Manage Extended Controls dialog box, click the Import Controls icon.
5. In the Select Extended Controls file dialog box, browse to the .csv file that contains the extended controls and import.
See “Working with extended controls” on page 825.

Editing an extended control

You can edit an extended control that is already added into the extended evidence sources system through the Manage Extended Controls dialog box.

To edit an extended control
1. Go to Manage > Extended Evidence Sources view of the console.
2. In the Extended Evidence Sources view, click Manage Extended Controls.
3. In the Manage Extended Controls dialog box, select the evidence source from the down-down list, Select Evidence Source whose controls you want to edit.
4. Select the extended controls from the list that you want to edit and click the Edit Control icon.
5. In the Edit Control dialog box, edit the details of the extended control.

See “Adding an extended control” on page 826.
See “Deleting an extended control” on page 831.

Deleting an extended control

You can delete either a single extended control or multiple extended controls in the extended evidence sources system. Earlier, the extended controls were either added or imported to the system through the Manage Extended Controls dialog box.

Note: After you delete the extended controls, the mappings with the control statements of the Content Studio are also deleted.

To delete an extended control
1. Go to Manage > Extended Evidence Sources view of the console.
2. In the Extended Evidence Sources view, click Manage Extended Controls.
3. In the Manage Extended Controls dialog box, select the evidence source from the down-down list, Select Evidence Source.
4. Select the extended controls from the list and click the Delete Control icon.
   Read the message that prompts before you delete the extended controls.

See “Editing an extended control” on page 831.
See “Adding an extended control” on page 826.
Working with evidence

In the Control Compliance Suite, the extended evidence sources system provides the infrastructure to import evidence of any application. Before you import the evidence into the extended evidence sources system, you must know about evidence.

See “About evidence” on page 814.

Evidence is imported into the system using various methods such as CSV file import, import from ODBC compliant database, or APIs.

See “About methods to import the extended controls” on page 815.

Before you start working with evidence of any external application, ensure that you perform the following:

- Configure the data location to specify a CSV file network location or establish an ODBC compliant database connection. The evidence is collected using these methods.
  See “Configuring the data locations” on page 165.

- Add an evidence source to the extended evidence sources system.
  In the extended evidence sources system, you require to add an evidence source before you import the evidence. At a time, you must associate an evidence source with only one import method. For example, if you associate an evidence source with the CSV file import method, then you cannot associate the same evidence source with the ODBC import method.
  The evidence source can also be configured as an evidence collection job, which can be scheduled accordingly for evidence collection. The evidence collection job collects evidence from the CSV files or the ODBC compliant databases as per the configuration.
  See “Adding an evidence source” on page 822.

- Configure the CSV file or the ODBC compliant database that contains the evidence.
  For example, if you use the CSV file import method to import the evidence, then ensure that the file contains the appropriate CSV headers.
  See “About CSV file format for evidence” on page 833.

See “Working with evidence sources” on page 821.

See “Working with extended controls” on page 825.

See “Importing evidence from CSV files or ODBC compliant databases” on page 849.
Setting tasks to roles for evidence collection

You must have the requisite permission to execute specific tasks that are related to the extended evidence sources system. These tasks are assigned to the roles that you can define for the extended evidence sources system.

In the Control Compliance Suite, you create a custom role for the system through the Settings > Role view of the console.

See “Creating a custom role” on page 110.

The following tasks must be associated with the custom role that you create for the extended evidence sources system:

- Manage Configuration Settings
- View Assets
- View All Jobs
- Manage Evidence definitions
- View Asset Reconciliation Rules
- Manage Jobs
- Import Assets
- View Configuration Settings

See “About roles” on page 96.

See “Configuring roles and permissions” on page 95.

About CSV file format for evidence

You can import the evidence of any application into the extended evidence sources system using the CSV file import method. To successfully import the evidence into the system, you must arrange the evidence information in the defined CSV file format. The evidence that is collected from the CSV file is stored in the evidence database, CSM_EvidenceDB.

Do the following to import the evidence from the CSV file:

- Understand the definition of the CSV file headers and gather the related information for the evidence.
  The CSV file headers represent the asset-related and evidence-related information of the assets. The evidence-related information is derived from the assessment of the assets.

- Define specific headers in the CSV file as per the format.
- Arrange the asset-related and evidence-related information correctly for the defined headers in the CSV file.

The CSV file header format that is defined by the system and their descriptions are as follows:

**Table 20-4** Contains the CSV file headers, their description, and their requirement types

<table>
<thead>
<tr>
<th>CSV header</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence.Record.AssetClass</td>
<td>This field represents the class to which the assets belong. The class of the assets is required by the Control Compliance Suite Asset System to create the assets. For example, assets can be of Windows Machine or Windows Directory AssetClass.</td>
<td>Optional</td>
</tr>
<tr>
<td>Evidence.Record.Asset1, Evidence.Record.Asset2, Evidence.Record.Asset3, Evidence.Record.Asset4, Evidence.Record.Asset5, Evidence.Record.Asset6, Evidence.Record.Asset7, and Evidence.Record.Asset8</td>
<td>These eight asset fields represent the primary fields and mandatory fields of an asset that are required to import the evidence. The asset-related information such as the primary fields and mandatory fields are mapped to the headers, Asset1 to Asset8 in the file. You must arrange the asset data in the ascending order of the names. These fields are required if the Asset ID is null.</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Table 20-4  Contains the CSV file headers, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>CSV header</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence.Record.ClassType</td>
<td>This field determines the type of information that are stored for the Asset1 to Asset8 fields.</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>The types of classes are as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Asset</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ IPAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Unknown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For example, if you specify, IPAddress for this field, then the infrastructure searches for assets of the specific IPAddress in the Asset System. If the asset exists, then an AssetID is created for the asset and the evidence data is imported. If two assets of different asset types are found, then the IPAddress of the parent asset alone is resolved.</td>
<td></td>
</tr>
<tr>
<td>Evidence.Record.AssetID</td>
<td>This field identifies the asset that is available in the Control Compliance Suite Asset System.</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>If an asset is not already available in the Asset System, then an Asset ID is created for the asset.</td>
<td></td>
</tr>
<tr>
<td>Evidence.Record.EvaluationIncidentID</td>
<td>This field represents the identifier (ID) of the evidence.</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>For example, for the Symantec Data Loss Prevention Connector, the ID of an incident must be specified for this field.</td>
<td></td>
</tr>
<tr>
<td>Evidence.Record.ControlID</td>
<td>This field identifies the controls such as an incident, check, or a questionnaire uniquely.</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
Table 20-4  Contains the CSV file headers, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>CSV header</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence.Record.AssessmentSource</td>
<td>This field represents the source name such as machine name on which the assessment or evaluation was first performed.</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>For example, name of the host computer on which the Symantec Data Loss Prevention Connector is installed.</td>
<td></td>
</tr>
<tr>
<td>Evidence.Record.Category</td>
<td>This field represents the category of the assessment that is supported by the external application.</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>For example, in Symantec Data Loss Prevention Connector, the incident categories that are supported are, network, discover, and endpoint. A policy can be violated for any specific incident.</td>
<td></td>
</tr>
<tr>
<td>Evidence.Record.AssessmentMessage</td>
<td>The field contains the assessment description or evaluation description of the asset. This description is useful in case of failures.</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>This information is derived from the external application.</td>
<td></td>
</tr>
<tr>
<td>Evidence.Record.AssessmentEvidence</td>
<td>This field contains the evaluated or assessed data of the asset.</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>The field value must be a string of alphanumeric type.</td>
<td></td>
</tr>
</tbody>
</table>
Table 20-4 Contains the CSV file headers, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>CSV header</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence.Record.RawAssessmentState</td>
<td>This field identifies the state of the assessed or evaluated data. For example, in the Symantec Data Loss Prevention Connector, the assessment data or evaluation data is either detected or blocked. The field value can be any string of alphanumeric type.</td>
<td>Optional</td>
</tr>
</tbody>
</table>
| Evidence.Record.Status                          | This field indicates the state of the external application. The value of this field must be an integer whose value is from 0 to 3. The values of this field are as follows:  
  ■ 0 This means pass and the application maps to positive assessment.  
  ■ 1 This means fail and the application maps to negative assessment.  
  ■ 2 This means neutral and the application maps to an evaluation.  
  ■ 3 This means unknown as the application’s assessment result is not known and has no value. For example, if the asset is non-functional during data evaluation, the result is unknown. | Mandatory        |
Table 20-4  Contains the CSV file headers, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>CSV header</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence.Record.Severity</td>
<td>This field defines the metrics of the assessment that is calculated based on either the CIA ratings or by some custom formula. The value of this field must be an integer whose value is from 0 to 10.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Evidence.Record.CustomAttributes XML</td>
<td>This field lets you provide custom attributes along with the assessment data or evaluation data. The attributes can be a name-value pair. These attributes can be used for filtering when retrieving the assessment data. &lt;CustomAttributes&gt; &lt;Ca name=&quot;Protocol&quot; value=&quot;SMTP&quot;/&gt; &lt;Ca name=&quot;Type&quot; value=&quot;Network Incident&quot;/&gt; &lt;/CustomAttributes&gt;</td>
<td>Optional</td>
</tr>
<tr>
<td>Evidence.Record.GeneratedDate</td>
<td>This field indicates the timestamp (UTC) when the assessment data or evaluated data was collected from the asset.</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

See “About ODBC mappings for evidence” on page 844.

See “About methods to import the extended controls” on page 815.

See “About evidence field format for predefined asset types” on page 839.

See “Importing evidence from CSV files or ODBC compliant databases” on page 849.
About evidence field format for predefined asset types

The Control Compliance Suite lets you import evidence of assets that belong to the predefined asset types into the extended evidence sources system. To successfully import evidence, you must appropriately arrange the primary and mandatory fields of the predefined asset types for the asset-related CSV file headers. In the CSV file, you must arrange the fields of the predefined asset types as per the format that is defined by the infrastructure.

To import evidence of assets that belong to the predefined asset types, you must do the following:

- Gather and arrange the primary and mandatory fields of the predefined asset type in the CSV file as per the defined format.
  In the CSV file, map the primary and mandatory fields with the asset-related headers in the ascending order. The asset-related headers range from Asset1 to Asset8 in the CSV file for evidence import. The remaining headers represent the evidence-related information of the assets.

- Gather and arrange the evidence information of the assets with the evidence-related headers of the CSV file.
  See “About CSV file format for evidence” on page 833.

The mapping between the primary and mandatory fields and the CSV file headers is as follows:

<table>
<thead>
<tr>
<th>Predefined asset type</th>
<th>Primary and mandatory fields</th>
<th>Header format</th>
</tr>
</thead>
</table>
| SQL Database          | The following fields that are listed in the ascending order are to be mapped to the headers:  
  ■ Database Name  
  ■ Domain/Workgroup Name  
  ■ Host Name (Node)  
  ■ Server Name (Instance) | The headers to which the fields are to be mapped are as follows:  
  ■ Evidence.Record.Asset1  
  ■ Evidence.Record.Asset2  
  ■ Evidence.Record.Asset3  
  ■ Evidence.Record.Asset4 |
Table 20-5  Defines the header format for asset fields of the predefined asset types (continued)

<table>
<thead>
<tr>
<th>Predefined asset type</th>
<th>Primary and mandatory fields</th>
<th>Header format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>The following fields that are listed in the ascending order are to be mapped to the headers:</td>
<td>The headers to which the fields are to be mapped are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Domain/Workgroup Name</td>
<td>■ Evidence.Record.Asset1</td>
</tr>
<tr>
<td></td>
<td>■ Host Name (Node)</td>
<td>■ Evidence.Record.Asset2</td>
</tr>
<tr>
<td></td>
<td>■ Major Version</td>
<td>■ Evidence.Record.Asset3</td>
</tr>
<tr>
<td></td>
<td>■ Server Name (Instance)</td>
<td>■ Evidence.Record.Asset4</td>
</tr>
<tr>
<td>ESM Agent</td>
<td>The following fields that are listed in the ascending order are to be mapped to the headers:</td>
<td>The headers to which the fields are to be mapped are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ ESM Manager</td>
<td>■ Evidence.Record.Asset1</td>
</tr>
<tr>
<td></td>
<td>■ OS Details</td>
<td>■ Evidence.Record.Asset2</td>
</tr>
<tr>
<td></td>
<td>■ OS Version</td>
<td>■ Evidence.Record.Asset3</td>
</tr>
<tr>
<td></td>
<td>■ Platform</td>
<td>■ Evidence.Record.Asset4</td>
</tr>
<tr>
<td></td>
<td>■ Registered Name</td>
<td>■ Evidence.Record.Asset5</td>
</tr>
<tr>
<td>Oracle Configured Databases</td>
<td>The following fields that are listed in the ascending order are to be mapped to the headers:</td>
<td>The headers to which the fields are to be mapped are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Database Name</td>
<td>■ Evidence.Record.Asset1</td>
</tr>
<tr>
<td></td>
<td>■ Domain/Workgroup Name</td>
<td>■ Evidence.Record.Asset2</td>
</tr>
<tr>
<td></td>
<td>■ Host Name (Node)</td>
<td>■ Evidence.Record.Asset3</td>
</tr>
<tr>
<td></td>
<td>■ OS Type</td>
<td>■ Evidence.Record.Asset4</td>
</tr>
<tr>
<td></td>
<td>■ Server Name</td>
<td>■ Evidence.Record.Asset5</td>
</tr>
<tr>
<td></td>
<td>■ Server Name (Instance)</td>
<td>■ Evidence.Record.Asset6</td>
</tr>
<tr>
<td></td>
<td>■ Server NetBIOS Name</td>
<td>■ Evidence.Record.Asset7</td>
</tr>
<tr>
<td></td>
<td>■ Windows Domain Name or UNIX IP address</td>
<td>■ Evidence.Record.Asset8</td>
</tr>
</tbody>
</table>
### Table 20-5

Defines the header format for asset fields of the predefined asset types *(continued)*

<table>
<thead>
<tr>
<th>Predefined asset type</th>
<th>Primary and mandatory fields</th>
<th>Header format</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Oracle Configured Servers</strong></td>
<td>The following fields that are listed in the ascending order are to be mapped to the headers:</td>
<td>The headers to which the fields are to be mapped are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ OS Type</td>
<td>■ Evidence.Record.Asset1</td>
</tr>
<tr>
<td></td>
<td>■ Server Name</td>
<td>■ Evidence.Record.Asset2</td>
</tr>
<tr>
<td></td>
<td>■ Server NetBIOS Name</td>
<td>■ Evidence.Record.Asset3</td>
</tr>
<tr>
<td></td>
<td>■ Windows Domain Name or UNIX IP address</td>
<td>■ Evidence.Record.Asset4</td>
</tr>
<tr>
<td><strong>UNIX File</strong></td>
<td>The following fields that are listed in the ascending order are to be mapped to the headers:</td>
<td>The headers to which the fields are to be mapped are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ File Name (with path)</td>
<td>■ Evidence.Record.Asset1</td>
</tr>
<tr>
<td></td>
<td>■ Host IP Address</td>
<td>■ Evidence.Record.Asset2</td>
</tr>
<tr>
<td></td>
<td>■ Machine Name</td>
<td>■ Evidence.Record.Asset3</td>
</tr>
<tr>
<td><strong>UNIX Group</strong></td>
<td>The following fields that are listed in the ascending order are to be mapped to the headers:</td>
<td>The headers to which the fields are to be mapped are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Group Database</td>
<td>■ Evidence.Record.Asset1</td>
</tr>
<tr>
<td></td>
<td>■ Group Name</td>
<td>■ Evidence.Record.Asset2</td>
</tr>
<tr>
<td></td>
<td>■ IP Address</td>
<td>■ Evidence.Record.Asset3</td>
</tr>
<tr>
<td></td>
<td>■ Machine Name</td>
<td>■ Evidence.Record.Asset4</td>
</tr>
<tr>
<td><strong>UNIX Machine</strong></td>
<td>The following fields that are listed in the ascending order are to be mapped to the headers:</td>
<td>The headers to which the fields are to be mapped are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ IP Address</td>
<td>■ Evidence.Record.Asset1</td>
</tr>
<tr>
<td></td>
<td>■ Machine Name</td>
<td>■ Evidence.Record.Asset2</td>
</tr>
<tr>
<td></td>
<td>■ Operating Distribution Field</td>
<td>■ Evidence.Record.Asset3</td>
</tr>
<tr>
<td></td>
<td>■ Operating System</td>
<td>■ Evidence.Record.Asset4</td>
</tr>
<tr>
<td></td>
<td>■ Operating System Version</td>
<td>■ Evidence.Record.Asset5</td>
</tr>
</tbody>
</table>
Table 20-5 Defines the header format for asset fields of the predefined asset types (continued)

<table>
<thead>
<tr>
<th>Predefined asset type</th>
<th>Primary and mandatory fields</th>
<th>Header format</th>
</tr>
</thead>
</table>
| Windows Directory     | The following fields that are listed in the ascending order are to be mapped to the headers:  
■ Domain/Workgroup Name  
■ Directory Name  
■ Machine Name  
| The headers to which the fields are to be mapped are as follows:  
■ Evidence.Record.Asset1  
■ Evidence.Record.Asset2  
■ Evidence.Record.Asset3  
| |
| Windows Domain        | The following field is mapped to the header:  
■ Domain Name  
| Evidence.Record.AssetField1  
| |
| Windows File          | The following fields that are listed in the ascending order are to be mapped to the headers:  
■ Domain/Workgroup Name  
■ File Name (with path)  
■ Machine Name  
| The headers to which the fields are to be mapped are as follows:  
■ Evidence.Record.Asset1  
■ Evidence.Record.Asset2  
■ Evidence.Record.Asset3  
| |
| Windows Group         | The following fields that are listed in the ascending order are to be mapped to the headers:  
■ Domain/Workgroup Name  
■ Group Name  
■ Group Name (Pre-Windows 2000)  
■ Machine Name  
| The headers to which the fields are to be mapped are as follows:  
■ Evidence.Record.Asset1  
■ Evidence.Record.Asset2  
■ Evidence.Record.Asset3  
■ Evidence.Record.Asset4  
<p>|</p>
<table>
<thead>
<tr>
<th>Predefined asset type</th>
<th>Primary and mandatory fields</th>
<th>Header format</th>
</tr>
</thead>
</table>
| **Windows Machine**   | The following fields that are listed in the ascending order are to be mapped to the headers:  
  ■ Domain/Workgroup Name  
  ■ Machine Name  
  ■ Machine is BDC  
  ■ Machine is PDC  
  ■ Machine is server  
  ■ OS Major Version  
  ■ OS Minor Version  
  ■ OS Type | The headers to which the fields are to be mapped are as follows:  
  ■ Evidence.Record.Asset1  
  ■ Evidence.Record.Asset2  
  ■ Evidence.Record.Asset3  
  ■ Evidence.Record.Asset4  
  ■ Evidence.Record.Asset5  
  ■ Evidence.Record.Asset6  
  ■ Evidence.Record.Asset7  
  ■ Evidence.Record.Asset8 |
| **Organization MS-Exchange** | The following field is to be mapped to the header:  
  ■ Organization DN | The header to which the field is to be mapped is as follows:  
  ■ Evidence.Record.Asset1 |
| **Administrative Groups MS-Exchange** | The following field is to be mapped to the header:  
  ■ Administrative Group DN | The header to which the field is to be mapped is as follows:  
  ■ Evidence.Record.Asset1 |
| **Exchange Server** | The following field is to be mapped to the header:  
  ■ Server DN | The header to which the field is to be mapped is as follows:  
  ■ Evidence.Record.Asset1 |
| **NDS Tree** | The following field is to be mapped to the header:  
  ■ Tree Name | The header to which the field is to be mapped is as follows:  
  ■ Evidence.Record.Asset1 |
| **NetWare File Server** | The following fields are to be mapped to the header:  
  ■ Object name (DN)  
  ■ Tree name | The headers to which the fields are to be mapped are as follows:  
  ■ Evidence.Record.Asset1  
  ■ Evidence.Record.AssetField2 |

See “About CSV file format for evidence” on page 833.
About ODBC mappings for evidence

You can import the evidence of any application into the extended evidence sources system using the ODBC compliant database import method. To successfully import the evidence into the system, you must arrange the evidence information in the defined ODBC database column format. The evidence that is collected from the ODBC compliant database is stored in the evidence database, CSM_EvidenceDB.

To facilitate the ODBC data collector to collect data successfully from the ODBC compliant databases you must create the database tables as per the defined format.

See “Format to create ODBC compliant database tables” on page 363.

If the database table is not created as per the defined format, then you can map the table or view names and field names through the Entity Table Mapping dialog box. You can access this dialog box when selecting a data location through the Create or Edit Evidence Source wizard.

Do the following to import the evidence from the ODBC compliant database:

- Understand the definition of the ODBC database column names and gather the related information for the evidence.
  The ODBC database column names represent the asset-related and evidence-related information of the assets. The evidence-related information is derived from the assessment of the assets.

- Define the database column names as defined in the table.

- Arrange the asset-related and evidence-related information correctly for the database columns.

Note: You must ensure that you create all the database columns for the database even if there is no evidence information available for a specific column.
Table 20-6 Contains the ODBC database column names, their description, and their requirement types

<table>
<thead>
<tr>
<th>ODBC database column names</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset1, Asset2, Asset3, Asset4, Asset5, Asset6, Asset7, and Asset8</td>
<td>These eight asset fields represent the primary fields and mandatory fields of an asset that are required to import the evidence. The asset-related information such as the primary fields and mandatory fields are mapped to the headers, Asset1 to Asset8 in the file. You must arrange the asset data in the ascending order of the names. These fields are required if the Asset ID is null.</td>
<td>Optional</td>
</tr>
<tr>
<td>ClassType</td>
<td>This field determines the type of information that are stored for the Asset1 to Asset8 fields. The types of classes are as follows: ■ Asset ■ IPAddress ■ Unknown For example, if you specify, IPAddress for this field, then the infrastructure searches for assets of the specific IPAddress in the Asset System. If the asset exists, then an AssetID is created for the asset and the evidence data is imported. If two assets of different asset types are found, then the IPAddress of the parent asset alone is resolved.</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
Table 20-6  Contains the ODBC database column names, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>ODBC database column names</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssetID</td>
<td>This field identifies the asset that is available in the Control Compliance Suite Asset System. If an asset is not already available in the Asset System, then an Asset ID is created for the asset.</td>
<td>Optional</td>
</tr>
<tr>
<td>EvaluationIncidentID</td>
<td>This field represents the identifier (ID) of the evidence. For example, for the Symantec Data Loss Prevention Connector, the ID of an incident must be specified for this field.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>ControlID</td>
<td>This field identifies the controls such as an incident, check, or a questionnaire uniquely.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>AssessmentSource</td>
<td>This field represents the source name such as machine name on which the assessment or evaluation was first performed. For example, name of the host computer on which the Symantec Data Loss Prevention Connector is installed.</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Table 20-6 Contains the ODBC database column names, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>ODBC database column names</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>This field represents the category of the assessment that is supported by the external application. For example, in Symantec Data Loss Prevention Connector, the incident categories that are supported are, network, discover, and endpoint. A policy can be violated for any specific incident.</td>
<td>Optional</td>
</tr>
<tr>
<td>AssessmentMessage</td>
<td>The field contains the assessment description or evaluation description of the asset. This description is useful in case of failures. This information is derived from the external application.</td>
<td>Optional</td>
</tr>
<tr>
<td>AssessmentEvidence</td>
<td>This field contains the evaluated or assessed data of the asset. The field value must be a string of alphanumeric type.</td>
<td>Optional</td>
</tr>
<tr>
<td>RawAssessmentState</td>
<td>This field identifies the state of the assessed or evaluated data. For example, in the Symantec Data Loss Prevention Connector, the assessment data or evaluation data is either detected or blocked. The field value can be any string of alphanumeric type.</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Table 20-6 Contains the ODBC database column names, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>ODBC database column names</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
</table>
| Status                     | This field indicates the state of the external application. The value of this field must be an integer whose value is from 0 to 2. The values of this field are as follows:  
■ Positive  
   This means that the application maps to positive assessment.  
■ Negative  
   This means that the application maps to negative assessment.  
■ Neutral  
   This means that the application maps to an evaluation. | Mandatory         |
| Severity                   | This field defines the metrics of the assessment that is calculated based on either the CIA ratings or by some custom formula. The value of this field must be an integer whose value is from 0 to 10. | Mandatory         |
Table 20-6  Contains the ODBC database column names, their description, and their requirement types (continued)

<table>
<thead>
<tr>
<th>ODBC database column names</th>
<th>Description</th>
<th>Requirement type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomAttributes XML</td>
<td>This field lets you provide custom attributes along with the assessment data or evaluation data. The attributes can be a name-value pair. These attributes can be used for filtering when retrieving the assessment data. For example, &lt;CustomAttributes&gt; &lt;ca name=&quot;Protocol&quot; Value=&quot;SMTP&quot;/&gt; &lt;ca name=&quot;Type&quot; value=&quot;Network Incident&quot;/&gt; &lt;/CustomAttributes&gt;</td>
<td>Optional</td>
</tr>
<tr>
<td>GeneratedDate</td>
<td>This field indicates the timestamp (UTC) when the assessment data or evaluated data was collected from the asset.</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

See “About CSV file format for evidence” on page 833.

Importing evidence from CSV files or ODBC compliant databases

You can import the evidence from the CSV files or from the ODBC compliant database into the extended evidence sources system.

The prerequisites to import evidence are as follows:

- Gather the primary fields and mandatory fields of the asset type for which the evidence is to be collected. If the assets belong to the predefined asset types, then the primary fields and mandatory fields can be gathered from the Control Compliance Suite. See “Predefined asset types” on page 236.
Create a CSV file with appropriate headers or configure the ODBC compliant database columns as per the defined format.
See “About CSV file format for evidence” on page 833.
See “About ODBC mappings for evidence” on page 844.

Ensure that the asset information which you provide in the CSV file or the ODBC tables is of correct format.
If the evidence collection job fails to add the assets in the system due to incorrect or inadequate asset information, the evidence for the assets are not added to the database.

To import evidence from a CSV file or an ODBC compliant database
1 Go to Settings > General > Data Locations.
   Share the network path where the new CSV file is located.
2 Go to Manage > Extended Evidence Sources view of the console.
3 In the Extended Evidence Sources view, click Add Evidence Source.
4 In the Create or Edit Evidence Source wizard, create a new evidence source.
   See “Adding an evidence source” on page 822.

You can associate an evidence source with any of the methods to import evidence such as CSV file import or ODBC compliant database import. You must configure a data location to access the CSV files or the ODBC compliant databases for evidence import.

See “End-to-end sequence of evidence import” on page 819.
See “Importing evidence from Response Assessment Module” on page 850.

Importing evidence from Response Assessment Module

The extended evidence sources system lets you import evidence from the Response Assessment module (RAM). You can create questionnaires to answer your business challenges in RAM. In RAM, a questionnaire is interpreted as the evidence.

The tasks that you require to perform for importing evidence from RAM are as follows:
### Table 20-7  Tasks to configure the evidence source for RAM

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an evidence source for RAM</td>
<td>By default, RAM creates an evidence source, Symantec Response Assessment module provider in the <strong>Extended Evidence Sources</strong> view of the console.</td>
</tr>
<tr>
<td>Create a data location</td>
<td>You must create a data location for connecting to the RAM database. The RAM database can be connected using the ODBC connection details. You can edit the already added RAM evidence source to configure its data location. See “Editing an evidence source” on page 824.</td>
</tr>
<tr>
<td>Configure the evidence collection job RAM</td>
<td>Configure the existing evidence source for RAM as the evidence collection job. You can configure the evidence source as a job through the Create or Edit Evidence Source wizard. The default view name of the RAM database is RAM.Evidence3rdPt, which you must specify in the Entity Table mapping. The entity table mapping is interpreted by the ODBC data collector for data collection. See “About the entity table mapping” on page 160.</td>
</tr>
</tbody>
</table>

See “Configuring Response Assessment Module in Control Compliance Suite” on page 196.

See “Mapping custom questionnaires to evidence” on page 851.

### Mapping custom questionnaires to evidence

After you configure the Response Assessment Module (RAM) evidence source, you can perform other tasks such as mapping the RAM questions and generating reports.

You can do the following tasks with a custom Response Assessment Module (RAM) questionnaire:
Table 20-8  Mapping questionnaire and generating reports for RAM

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map the RAM questions to control statements</td>
<td>You can map the RAM questions to the control statements through the <strong>Content Studio</strong>. See “Mapping questions to control statements” on page 801.</td>
</tr>
<tr>
<td>Map the control statements to a policy</td>
<td>After the policy is created, map the control statements to the policy. The control statements are mapped to the frameworks and regulations that your enterprise must adhere to. The policy reports do not work if the policy and questions in the questionnaire are not linked to the same control statements. See “Mapping policies to control statements” on page 797.</td>
</tr>
<tr>
<td>Publish the policy</td>
<td>After the policy is mapped to the control statements, publish the policy for user acceptance. See “Publishing a policy” on page 704.</td>
</tr>
<tr>
<td>Run the evidence collection job</td>
<td>You can configure the existing evidence source for RAM as the evidence collection job. You can configure the evidence source as a job through the <strong>Create or Edit Evidence Source</strong> wizard. See “Running a job now” on page 719.</td>
</tr>
<tr>
<td>Synchronize the reporting database</td>
<td>After the policy is published, synchronize the reporting database to run reports. <strong>Note:</strong> Evidence from RAM is only imported if it exists in the Evidence table of the RAM database. See “Synchronizing the reporting database” on page 167.</td>
</tr>
</tbody>
</table>
Table 20-8  Mapping questionnaire and generating reports for RAM (continued)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
</table>
| Generate reports            | Generate reports on the control statements that are mapped to the RAM questions. The reports are scheduled from the Reporting > Report Templates view of the console. After the reporting database is synchronized, run the following reports to view the RAM data:  
  ■ Policy Compliance by Asset  
  ■ Policy Control Statement Mappings  
  ■ Policy Summary  
See “Predefined report descriptions” on page 741.  
See “Scheduling a report ” on page 746. |

Viewing the imported evidence

You can view the evidence that is imported from the external applications into the Control Compliance Suite. The evidence details are displayed in the evidence viewer, which is accessible through the Extended Evidence Sources view of the console. The evidence viewer displays the evidence details for every evidence source, which is configured for the extended evidence sources system.

To view the imported evidence

1. Go to Manage > Extended Evidence Sources view of the console.
2. In the Extended Evidence Sources view, select an evidence source and then click View Imported Evidence.  
You can also select an evidence source, right-click on it, and then select View Imported Evidence.
3. In the Imported Evidence for [evidence source name] dialog box, set the filter criteria to view the evidence details that are collected for the selected evidence source.

See “Working with evidence sources ” on page 821.
Understanding the integration services APIs

This chapter includes the following topics:

■ **About the integration interfaces**

■ **Control Compliance Suite APIs**

**About the integration interfaces**

The Control Compliance Suite (CCS) aims to provide a flexibility to the third-party clients to integrate the core functionality of CCS within their own business processes. To serve the purpose, all the application modules in the CCS expose their core functionality to the third-party clients through a set of APIs.

The integration interfaces aim at achieving the following objectives:

■ Make it easier for the third-party users of CCS to automate certain large-scale tasks.

■ Enable the third-party users to customize the core CCS features to suit their business objective that is related to assets management, compliance, and reporting.

■ Equip the .NET as well as non-.NET users to effectively integrate with CCS through the exposed functionality.

**Control Compliance Suite APIs**

To help you choose the appropriate APIs for your application, refer the following table that lists the exposed APIs for each module in the Control Compliance Suite:
Note: For a detailed description of each API, go to <InstallDir>\Symantec\CCS\Reporting and Analytics\Documentation\API_Help and launch the CCS_API_Reference_Guide.htm.

Table 21-1  Control Compliance Suite APIs

<table>
<thead>
<tr>
<th>Module name</th>
<th>APIs</th>
</tr>
</thead>
</table>
| Assets management APIs    | ■ IAssetService  
  ■ CreateAssetImportJob  
  ■ Delete  
  ■ GetDetails  
  ■ GetScores  
  ■ Search  
  ■ UpdateRiskScore  
  ■ UpdateComplianceScore  
  ■ Update  
  ■ IAssetGroupService  
  ■ AddAssetsToAssetGroup  
  ■ GetDetails  
  ■ Search  
  ■ IAssetMetaDataService  
  ■ GetAllAssetTypes  
  ■ GetAllAttributes  
  ■ GetAttributesOnFilter  
  ■ ISiteService  
  ■ GetAllSites  
  ■ GetSite |
<table>
<thead>
<tr>
<th>Module name</th>
<th>APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards management APIs</td>
<td>■ IStandardService</td>
</tr>
<tr>
<td></td>
<td>■ GetSectionsFromStandard</td>
</tr>
<tr>
<td></td>
<td>■ Search</td>
</tr>
<tr>
<td></td>
<td>■ ISectionService</td>
</tr>
<tr>
<td></td>
<td>■ GetChecksFromSection</td>
</tr>
<tr>
<td></td>
<td>■ GetSectionsFromSection</td>
</tr>
<tr>
<td></td>
<td>■ Search</td>
</tr>
<tr>
<td></td>
<td>■ ICheckService</td>
</tr>
<tr>
<td></td>
<td>■ Search</td>
</tr>
<tr>
<td></td>
<td>■ ISMJobService</td>
</tr>
<tr>
<td></td>
<td>■ CreateCollectionJob</td>
</tr>
<tr>
<td></td>
<td>■ CreateCollectionEvaluationJob</td>
</tr>
<tr>
<td></td>
<td>■ CreateEvaluationJob</td>
</tr>
<tr>
<td></td>
<td>■ GetCollectionJob</td>
</tr>
<tr>
<td></td>
<td>■ GetCollectionEvaluationJob</td>
</tr>
<tr>
<td></td>
<td>■ GetEvaluationJob</td>
</tr>
<tr>
<td></td>
<td>■ GetCheckEvaluationResults</td>
</tr>
<tr>
<td></td>
<td>■ UpdateCollectionJob</td>
</tr>
<tr>
<td></td>
<td>■ UpdateCollectionEvaluationJob</td>
</tr>
<tr>
<td></td>
<td>■ UpdateEvaluationJob</td>
</tr>
<tr>
<td>Jobs management APIs</td>
<td>■ IJobManagerService</td>
</tr>
<tr>
<td></td>
<td>■ CancelJobExecution</td>
</tr>
<tr>
<td></td>
<td>■ deleteJob</td>
</tr>
<tr>
<td></td>
<td>■ deleteJobRun</td>
</tr>
<tr>
<td></td>
<td>■ deleteSchedule</td>
</tr>
<tr>
<td></td>
<td>■ EnnumRunningJobs</td>
</tr>
<tr>
<td></td>
<td>■ ExecuteJob</td>
</tr>
<tr>
<td></td>
<td>■ GetJobInfoByName</td>
</tr>
<tr>
<td></td>
<td>■ getJobRuns</td>
</tr>
<tr>
<td></td>
<td>■ getLatestNJobRuns</td>
</tr>
<tr>
<td></td>
<td>■ GetJobStatusInfo</td>
</tr>
<tr>
<td></td>
<td>■ GetJobStatusList</td>
</tr>
<tr>
<td></td>
<td>■ getSchedule</td>
</tr>
<tr>
<td></td>
<td>■ getAllSchedules</td>
</tr>
<tr>
<td></td>
<td>■ IsJobNameUnique</td>
</tr>
<tr>
<td></td>
<td>■ IsJobNameUpdateUnique</td>
</tr>
<tr>
<td></td>
<td>■ ScheduleJob</td>
</tr>
<tr>
<td>Module name</td>
<td>APIs</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Extended evidence sources APIs</td>
<td>■ IExtendedEvidenceSourcesISSService</td>
</tr>
<tr>
<td></td>
<td>■ InsertIncidentRecords</td>
</tr>
<tr>
<td></td>
<td>■ InsertOrdinalValues</td>
</tr>
<tr>
<td></td>
<td>■ RegisterControls</td>
</tr>
<tr>
<td></td>
<td>■ RegisterEvidenceProvider</td>
</tr>
<tr>
<td>Exceptions management APIs</td>
<td>■ IExceptionManagerService</td>
</tr>
<tr>
<td></td>
<td>■ DoesExceptionExist</td>
</tr>
<tr>
<td></td>
<td>■ GetAllExceptions</td>
</tr>
<tr>
<td></td>
<td>■ GetExceptionByID</td>
</tr>
<tr>
<td></td>
<td>■ GetExceptionByTitle</td>
</tr>
<tr>
<td></td>
<td>■ RequestException</td>
</tr>
<tr>
<td></td>
<td>■ SetExceptionState</td>
</tr>
<tr>
<td></td>
<td>■ TerminateException</td>
</tr>
<tr>
<td></td>
<td>■ UpdateException</td>
</tr>
<tr>
<td>Entitlements management APIs</td>
<td>■ IEntitlementsManagerService</td>
</tr>
<tr>
<td></td>
<td>■ MarkAssetAsControlPoint</td>
</tr>
<tr>
<td></td>
<td>■ GetAssetsMarkedAsControlPoints</td>
</tr>
<tr>
<td></td>
<td>■ CreateEntitlementsImportJob</td>
</tr>
<tr>
<td>Third-party events subscriptions APIs</td>
<td>■ IEventNotificationService</td>
</tr>
<tr>
<td></td>
<td>■ EnumerateSubscriptions</td>
</tr>
<tr>
<td></td>
<td>■ RenewSubscriptions</td>
</tr>
<tr>
<td></td>
<td>■ Subscribe</td>
</tr>
<tr>
<td></td>
<td>■ Unsubscribe</td>
</tr>
<tr>
<td></td>
<td>■ UnsubscribeAll</td>
</tr>
<tr>
<td></td>
<td>■ UnsubscribeWithEventId</td>
</tr>
<tr>
<td>Tags management APIs</td>
<td>■ ITagManagerService</td>
</tr>
<tr>
<td></td>
<td>■ AddTag</td>
</tr>
<tr>
<td></td>
<td>■ CreateTag</td>
</tr>
<tr>
<td></td>
<td>■ CreateTagCategory</td>
</tr>
<tr>
<td></td>
<td>■ DeleteTag</td>
</tr>
<tr>
<td></td>
<td>■ DoesTagExist</td>
</tr>
<tr>
<td></td>
<td>■ GetObjects</td>
</tr>
<tr>
<td></td>
<td>■ RemoveTag</td>
</tr>
<tr>
<td></td>
<td>■ SetTag</td>
</tr>
</tbody>
</table>
Migration utilities

This chapter includes the following topics:

- About the Standard Migration Utility
- About the Symantec ESM Policy to CCS Standard Migration Utility
- About the CCS Data Migration utility

About the Standard Migration Utility

The Standard Migration Utility (SMU) lets you migrate the following to Control Compliance Suite (CCS) 9.0.1 or later format:

- Custom standards of the existing Technical Standard Packs (TSP)
- Custom standards that you have created

You can use the migrated standards in CCS 9.0.1 or later after you migrate the standards to the CCS 9.0.1 or later format.

You can migrate the complex checks of the custom standards of the following TSPs:

- Security Essentials for Red Hat Enterprise Linux 5.0
- CIS Security Benchmark for HP-UX v1.3.1
- CIS AIX Benchmark v1.0.1
- CIS Solaris 10 Benchmark v4.0
- CIS Oracle 9i and 10g Database Security Benchmark v2.0
- Security Essentials for Microsoft SQL Server 2005
- CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0
You can migrate all the generic checks of all the TSPs available to the CCS 9.0.1 or later format. After migration to the 9.0.1 or later format, you can import standards, perform data collection, and evaluate the migrated checks in CCS 9.0.1 or later. You cannot migrate the complex checks of the standards that are present in CCS 8.60 but are not present in CCS 9.0.1 or later. You can find the messages for the checks in the log file.

The utility can migrate only one standard at a time.

About the Standard Migration Utility system requirements

You must ensure that the workstation meets the following hardware requirements:

- 3.0 GHz CPU
- 1 GB RAM
- 1 GB free disk space
- Monitor resolution set to 1024x768 pixels or greater

You must ensure that the workstation meets the following software requirements:

- Microsoft Windows Server 2003 SP1 or later
- Microsoft Windows XP SP2 or later
- Microsoft .NET 3.0
- Microsoft Jet OLE DB 4.0

Note: You can download the Microsoft Jet OLE DB 4.0 utility from the Internet.
About the Standard Migration Utility packaging and deployment

The utility is present in the Symantec_Control_Compliance_Suite_Migration_Utility_10.0_Win.exe Web package.

You can extract the content of the Web package to any location. The installation of the Control Compliance Suite (CCS) 9.0.1 or later is not mandatory on the computer where you want to migrate the standard. The extraction of the package creates the following folders:

■ bin
■ Documentation
■ MetaData
■ Output
■ Schema

The bin folder contains the binaries that you must have for migration. The Documentation folder contains the Symantec Standard Migration Utility Guide. The MetaData folder contains password-protected .mdb files for the four platforms. These .mdb files are required to migrate complex checks and for replacing target types. The utility generates the migrated files in the CCS 9.0.1 or later format in the output folder. The output file is an .xml file that is time stamped. The Schema folder contains PolicyTree.xsd, which is the XSD for CCS 8.6. The Schema folder also contains standard.xsd, which is the XSD for CCS 9.0.1 or later. These files are required for validation.

Note: The .mdb files in the MetaData folder are password-protected.

Standard Migration Utility

The following notes describe the known issues in the Standard Migration Utility:

■ Checks that have the following fields are not migrated:

ACCOUNTTYPE          GROUP data source
RELATIVEADSIPATH     IISVIRTUALDIRECTORIES data source
BROWSINGENABLED      IISVIRTUALDIRECTORIES data source

The checks that are created by using these fields are also not migrated.
The utility does not look into the values that are sent to various operators in the input standard expressions, for example, Match operator. The utility does not perform any corrective action on the operators. It does not correct improper regular expressions too. The utility migrates the expressions and may display an error during evaluation.

If the 8.60 input standard has the predicates that have any one of the following, then you must correct the standard as per 9.0.1 format before migration:

- Unequal number of open and closed brackets
- Individual expressions that are not in brackets
  
  

Otherwise, the checks are not migrated.

The Standard Migration Utility does not migrate a standard that contains checks to scan multiple platforms such as UNIX, Windows, SQL, and Oracle. Ensure that the checks in a standard pertain to single platform.

The check Are Deleted Database pages Zeroed out? of the standard Security Essentials for Exchange 2007 is properly migrated using the utility. However, the migrated check will not function as expected.

In CCS 8.60 when server related checks were evaluated against a administrative group or organization target the checks used to be evaluated against all servers under the administrative group/organization. This behavior is no longer supported in CCS 9.0.1. The user will not be able to evaluate a server related check on any target other than a server. Similarly, checks applicable to organizations and administrative groups can only be evaluated against an organization and an administrative group assets respectively.

Some of the fields required in the Exchange 2000 standard are not available in the product and migration utility. Any check using any of the following fields will not be migrated by the Standard Migration Utility:

- MAILADMIN.EXCHANGE2KDIRECTORY.CHANNEL_EVERYONEACCESS
- MAILADMIN.EXCHANGE2KDIRECTORY.CLASS_MSEXCHCHATMAXCONNECTIONS
- MAILADMIN.EXCHANGE2KDIRECTORY.ADSI_MSEXCHAUTHENTICATIONFLAGS_NONRMS
- MAILADMIN.EXCHANGE2KDIRECTORY.FILTER_ENABLED
- MAILADMIN.EXCHANGE2KDIRECTORY.COMMUNITY_EVERYONEACCESS
- MAILADMIN.EXCHANGE2KDIRECTORY.ADSI_MSEXCHSMTPRELAYRESTRICTION
How to use the Standard Migration Utility

The Standard Migration Utility is a command-line tool. This tool accepts command-line options and produces a standard that is consistent with CCS 9.0.1 or later standard schema. The tool provides a logging facility because CCS 8.60 or older standard can have a large number of procedures, checks, and sections to migrate. The details about each item that the tool migrates is successfully logged. The utility also logs any item that does not migrate and includes reasons for not migrating the item.

A user who has the permissions to import a standard can import the migrated standard into CCS 9.0.1 or later.

About the command-line options

You must provide the following command-line options to the utility:

- -standard
- -platform

You must type the following in the command prompt and press enter to start the migration:

StandardMigrator.exe -standard <fully qualified name of the standard file> -platform <Unix/Oracle/Windows/SQL/Exchange>

Note: You must run the command from the StandardMigrationTool\bin folder.

For example,

StandardMigrator.exe -standard “D:\build_drops\5th Dec\StandardMigrationtool\SampleOldStandards\Old_CISAIXV101.std” -platform UNIX

The possible values for the platform are UNIX, Oracle, Windows, SQL, and Exchange. The option is case insensitive.

About validation

The Standard Migration Utility validates the following:

- Input Standard
  After you provide the details to the utility, the utility checks whether the input file exists and if the platform is valid. The input standard file is then validated against the PolicyTree.xsd. The process of migration continues if the input file is valid. If the input standard file is invalid then the message “Input standard is invalid” appears. The utility then prompts whether you want to
continue with the migration. The log file is updated with the details of the validation error in the input standard. If you choose to continue, then the migration continues with an invalid input standard.

- Migrated Standard
The utility logs all successful migration of standards to the log file. The errors are also logged in the log file. The final standard in the CCS 9.0.1 or later format that is migrated is validated against the CCS 9.0.1 or later standard that is shipped with the tool. If invalid, a message appears that states that the standard has been migrated but it is invalid. Otherwise, a valid standard is generated. A migration without an error indicates the generation of a valid CCS 9.0.1 or later standard.
You can still receive a valid standard that may contain invalid checks. For example, if during migration the utility fails to migrate a particular check, then the log file contains the migration errors of that check. But because the tool skips that check and continues the migration of other checks, the final migrated standard is valid. However, the standard does not contain the invalid check.

About the log file configuration settings
The details of logging is configurable through the StandardMigrator.exe.config file that is located in the bin folder. Open the configuration file in a standard text editor to make the changes.

The configuration file has the following settings:

- add key="CheckTypeToMigrate" value=
You can use this option to specify whether all checks or only the generic checks are to be migrated.
For example, <add key="CheckTypeToMigrate" value="generic" />
The setting has the following possible values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Migrates all the checks in the standard.</td>
</tr>
<tr>
<td>Generic</td>
<td>Migrates only the generic checks in the standard.</td>
</tr>
</tbody>
</table>

The default value is All.

- Log.Disable
You can use this option to disable the entire logging subsystem. When you enable this option, all of the log messages written by the application and its support assemblies are ignored.
**Note:** Enabling this option can provide a performance gain. However, no diagnostic output exists, regardless of severity.

The setting has the following possible values:

- True
- False

The default value is false.

**Log.FileLogger.Severity**

Each diagnostic message written to the logging subsystem has a severity associated with it. Severity is defined as one of the following values:

- **Error**
  These messages indicate that some type of critical error has occurred. Messages with a severity of Error usually indicate that a component is no longer capable of functioning. The component also operates under reduced functionality or may have lost data.

- **Warning**
  Messages with a severity of Warning usually indicate that a potential problem has occurred that may cause more serious consequences later if not corrected.

- **Information**
  Informational messages are used to indicate normal flow of execution. These messages are usually employed to mark milestone events during normal execution.

- **Verbose**
  Verbose messages provide more in-depth details about normal or abnormal execution and are intended to aid in diagnosing problems in the field.

The Log.FileLogger.Severity option provides a way to filter the messages that get output based upon a severity threshold. The following four possible values exist for Log.FileLogger.Severity:

- **Error**
  Messages with a severity of Error is the output.

- **Warning**
  Messages with severity of Warning or Error is the output.

- **Information**
  Messages with severity of Information, Warning, or Error is the output.

- **Verbose**
  Messages with severity of Verbose, Information, Warning, and Error is the output.

The default value is Error.

**Log.FileLogger.BaseFilename**
This parameter defines the base file name that is used for log files of this application. Log file names take the following form:
base_filename.timestamp.pid.sequence_number.extension
This option defines the base_filename portion of the log file name.
The default value is name of the executing assembly without the extension.

- **Log.FileLogger.LogDirectory**
  This parameter specifies the location to which log files for this application are written. You may specify either a relative path or an absolute (rooted) path for this option. The behavior differs depending upon the path that you specify. If you specify an absolute (rooted) path, log files are written to that directory. Do not use this method except in situations where the base logging directory is undesirable.
  If you specify a relative path, that path is added to the base logging directory and log files are written into that directory. Use this method because it allows all log files to be written under a common directory structure.
  By default, the base logging directory is:
  <common_app_data>\Symantec.CSM\Logs
  The <common_app_data> directory is a special directory defined by Windows. Its location varies depending upon the operating system. <common_app_data> resolves in the following location on different versions of Windows:

  - Windows 2000/XP/2003: <systemdrive>\Documents and Settings\All Users\ApplicationData
  - Windows Vista/2008: <systemdrive>\ProgramData

  If <common_app_data> is undesirable as a location for the base logging directory, you can change the base logging directory.
  The default value is Empty (logs are written to <common_app_data>\Symantec.CSM\Logs).

- **add key="MetadataLocation" value=**
  You can use this option to specify metadata location and name in the configuration file.
  For example, <add key="MetadataLocation" value="C:\patch_chk_metadata.mdb" />
  The setting has the following possible values:

  - Metadata location with name.
  - If value of this key is empty then the Standard Migration Utility uses the default metadata depending upon the platform specified.
About migration summary report

The migration summary report is generated after migration of the standards. This summary report is generated in the Output folder. The summary report name is same as the name of the migrated standard with “MigrationSummary” prefixed before the file name.

For example,
MigrationSummary_Symantec_2_6_2009 11_37_17 AM.csv

The output file is a .csv file that has the following columns:

<table>
<thead>
<tr>
<th>Check</th>
<th>Section</th>
<th>Status</th>
</tr>
</thead>
</table>

Limitations in the Standard Migration Utility

The utility has the following limitations:

- Constant upgrade or changes are needed to the Standard Migration Utility as upgrade or changes occur in CCS 9.0.1 or later content.

- The utility migrates only “procedures” and “policy” tags under the “tree” tag of the custom standards that are migrated. The utility does not migrate “refmachine” and “scopes” tags under the “tree” tag. If “refmachine” and “scopes” tags are present then the utility discards the tags as they are not required for migration in CCS 9.0.1 or later.

- In CCS 8.60 through scopes you can specify the following:
  - Where to get files from
  - Whether to get content
  - Sub folders to be included

9.0.1 does not have scopes. The Standard Migration Utility performs the function of scopes for most of the cases. Otherwise, you need to specify these parameters in the check itself (in the selectors and filters of the checks).

If the input check does not have the following fields, then post migration such a check fetches files from default location (\ root and one level below root):

- UNIX.File.Parent Directory
- UNIX.File.Fully Qualified Name
- UNIX.File.Base Name

To correct this problem modify the migrated check as shown:
An input check (Search for world writable directories with sticky bit set in whole box) with expression
<expression name="n0" ...
<text>"UNIX.FILE.ISWOTH" = True</text>
<selectors>
<text>"UNIX.FILE.TYPE" = "directory"</text>
<text>"UNIX.FILE.ISWOTH" = True</text>
</selectors>
</expression>

Is migrated to check with expression
<datacollectionqueries>
<datacollectionquery mosentityname="Unix.File">
<mosfields>
...
</mosfields>
<filters>
<filter filteroperator="And">
<filtertext>Unix.File.Type = 'directory'</filtertext>
<filtertext>Unix.File.IsWOTH = 'True'</filtertext>
</filter>
</filters>
</datacollectionquery>
</datacollectionqueries>
</procedure>
<expressions>
<expressions>
<expression name="n0" ...
<text>Unix.File.IsWOTH = 'True'</text>
<selectors>
<text>Unix.File.Type = 'directory'</text>
<text>Unix.File.IsWOTH = 'True'</text>
</selectors>
</expression>
</expressions>
</expressions>

It should be changed to
<datacollectionqueries>
<datacollectionquery mosentityname="Unix.File">
<mosfields>
...

Change LIKE to "match" in the input check if the input check has the LIKE operator with a value that has patterns other than the patterns recognized by SQL equivalent LIKE operator, for example %, _, [a-z], [%]. Otherwise, you might receive a run time error during evaluation.

For example, you should change Field1 LIKE 'ab.*c' to Field1 match 'ab.*c'

### Troubleshooting evaluation mismatches

Some evaluation mismatches may occur while the product evaluates the migrated standard. The following resolutions exist for the problem:
Consider a check with two or more expressions, where some, but not all, have the same selectors and the MOS field. This check can give an incorrect evaluation result.

For example, if we have a check such as:

```
<precondition>
<description>Description</description>
<expressions>
<expression name="A1" default="Unknown" rollup="Or"
selectorOperator="AND">
<text>Wnt.Service.Name %~ '/alerter/I'</text>
</expression>
</expressions>
<predicate>[A1]</predicate>
</precondition>
```

```
<description>Description</description>
<expressions>
<expression name="A2" default="False" rollup="And"
selectorOperator="OR">
<text>Wnt.Service.StartupType = 'Automatic'</text>
<selectors>
<text>Wnt.Service.Name = 'Error Reporting Service'</text>
</selectors>
</expression>
</expressions>
```
Where the expression A1 does not have a selector and A2 has selector and both deal with same field (Wnt.Service.Name). The reason is that the selector in A2 creates a filter and the utility will filter data as per the filter tag. So in the example given the data for "alerner" Service (expression A1) is never retrieved.
To resolve this problem, you should include a selector in A1 as shown:

```xml
<procedure>
  <precondition>
    <procedure>
      <description>Description</description>
      <expressions>
        <expression name="A1" default="Unknown" rollup="Or" selectorOperator="AND">
          <text>Wnt.Service.Name %~ '/alerter/I'</text>
          <selectors>
            <text>Wnt.Service.Name = 'Alerter'</text>
          </selectors>
        </expression>
      </expressions>
      <predicate>[A1]</predicate>
    </precondition>
  </procedure>
</procedure>
```

```xml
<procedure>
  <precondition>
    <procedure>
      <description>Description</description>
      <expressions>
        <expression name="A2" default="False" rollup="And" selectorOperator="OR">
          <text>Wnt.Service.StartupType = 'Automatic'</text>
          <selectors>
            <text>Wnt.Service.Name = 'Error Reporting Service'</text>
          </selectors>
        </expression>
      </expressions>
      <predicate>[A2]</predicate>
    </precondition>
  </procedure>
</procedure>
```
Problem

If a check calls a procedure 1 and that procedure 1 calls another procedure 2 that accepts argument. But the procedure 1 calls procedure 2 without the arguments, then the check can give an incorrect evaluation result.

For example, if we have a procedure such as:

```xml
<procedure name="P2">
<expressions>
  <expression name="A1" default="True" rollup="OR" selectorOperator="AND">
    <text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" = !ProductName</text>
  </expression>
</expressions>
<predicate>[A1]</predicate>
</procedure>

<procedure name="P1">
<precondition>
  <procedurename custom="False">P2</procedurename>
</precondition>
<expressions>
  <expression name="A1" default="Unknown" rollup="AND" selectorOperator="AND">
    <text>"WNT.PATCHASSESSMENT.BPM_PATCH_STATUS" != Missing Service Pack</text>
    <selectors>
      <text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" = !ProductName</text>
    </selectors>
  </expression>
</expressions>
</procedure>
```
Where the procedure P2 accepts an argument and it is called from procedure “P1” without providing any argument. Procedure “P1” is called from check, so in this case the check results in “Not Applicable”. As procedure “P2” is called from the “Predicate” tag of the procedure “P1” without providing argument and “P2” does not receive the value of the argument that the procedure expects.
To resolve this problem you must call procedure “P2” by providing argument as shown:

```xml
<procedure name="P2">
<expressions>
<expression name="A1" default="True" rollup="OR" selectorOperator="AND">
<text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" = !ProductName</text>
</expression>
</expressions>
<predicate>[A1]</predicate>
</procedure>

<procedure name="P1">
<precondition>
<procedure>
<predicate>[proc:P2 (ProductName = !ProductName)]</predicate>
</procedure>
</precondition>
<expressions>
<expression name="A1" default="Unknown" rollup="AND" selectorOperator="AND">
<text>"WNT.PATCHASSESSMENT.BPM_PATCH_STATUS" != Missing Service Pack</text>
<selectors>
<text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" = !ProductName</text>
</selectors>
</expression>
</expressions>
<predicate>[A1]</predicate>
</procedure>
```
About the Symantec ESM Policy to CCS Standard Migration Utility

The Symantec ESM Policy to CCS Standard Migration Utility lets you map the existing ESM policies to CCS standards. You can also migrate ESM policies to the CCS standards by using the CCS Check Builder. However, the CCS Check Builder is time consuming and the level of complexity is high.

To make the ESM policy migration procedure seamless, Symantec has designed the migration utility that automates the process of CCS standard creation from an ESM policy.

The Symantec ESM Policy to CCS Standard Migration Utility is a command-line utility that takes the ESM Policy XML as an input. The utility then generates a CCS Standard XML as an output. At a time, the utility can take only one ESM Policy XML as an input.

<table>
<thead>
<tr>
<th>ESM</th>
<th>CCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM policy name</td>
<td>CCS standard name</td>
</tr>
<tr>
<td>ESM module name</td>
<td>CCS section</td>
</tr>
<tr>
<td>ESM OS platform</td>
<td>CCS section</td>
</tr>
<tr>
<td>ESM check title</td>
<td>CCS check name</td>
</tr>
<tr>
<td>ESM check description</td>
<td>CCS check description</td>
</tr>
<tr>
<td>ESM message, message string ID, or message numeric ID</td>
<td>CCS check expression</td>
</tr>
<tr>
<td>ESM check CIA value</td>
<td>CCS check CIA value</td>
</tr>
</tbody>
</table>

**Note:** Only the compliance-related checks include the CIA value. If an ESM check does not pertain to compliance, then the CIA value for the corresponding CCS check displays as “Undefined”.

About packaging and deployment

A Web package by the name `Symantec_Control_Compliance_Suite_ESM_SU_39_Migration_Utility_10.0_Win.exe` contains the migration utility. You can run the Web package on your local...
computer to extract the content. The utility creates a folder by the name "ESMPolicyToCCSStandard," which contains the following binaries:

<table>
<thead>
<tr>
<th>File</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESMPolicyToCCSStandard.exe</td>
<td>Migration Utility</td>
</tr>
<tr>
<td>ESMPolicyToCCSStandard.exe.config</td>
<td>Migration Utility Configuration file</td>
</tr>
<tr>
<td>Security-content.xml</td>
<td>Security Content XML</td>
</tr>
<tr>
<td>Symantec.CSM.Resources.SUResources.dll</td>
<td>SU Resources Assembly</td>
</tr>
<tr>
<td>ESMTargetTypeMapping.xml</td>
<td>ESM Target Type Mapping XML</td>
</tr>
<tr>
<td>Symantec™ ESM Policy to CCS Standard Migration Utility User's Guide</td>
<td>Documentation</td>
</tr>
</tbody>
</table>

**Additional information about the files**

The additional information of the files is as follows:

- **security-content.xml**
  The security-content.xml file contains the metadata information about the ESM checks and the ESM security messages. In addition, it contains the mapping of all the ESM security messages that an ESM check generates.

- **Symantec.CSM.Resources.SUResources.dll**
  The Security Content XML is located in the update package that is created for Reporting Database Link (RDL). The Security Content XML is updated and is shipped with every ESM Security Update release.

**System requirements for the ESM Policy to CCS Standard Migration Utility**

The computer on which you want to install the migration utility must meet the following hardware requirements:

- 3.0 GHz CPU
- 1 GB RAM
- 1 GB free disk space
The computer on which you want install the migration utility must meet the following software requirements:

- Microsoft Windows Server 2003 SP1 or later
- Microsoft Windows Server 2003 x64 SP1 or later
- Microsoft Windows XP Professional SP2 or later
- Microsoft Windows XP Professional x64 SP2 or later
- Microsoft Windows Vista
- Microsoft Windows Vista x64
- Windows Server 2008
- Microsoft Windows Server 2008 x64

About installing the migration utility

Run the Web package to extract the content. You may copy all the files from the ESMPolicyToCCSStandard folder to a new folder under any of the following folders:

- CCS console installation folder from
  %APPDATA%\Symantec\CCS-<hostname>\<New folder for the migration utility>

- DPS installation directory, that is, from <CCS Installation Directory>\DPS\<New folder for the migration utility>

- Any other folder. In this case, you have to configure the 'ReferencedAssemblyLocation' attribute in configuration file viz.
  ESMPolicyToCCSStandard.exe.config. Read the comments in configuration file to understand what value you should specify for this attribute.

Uninstalling the migration utility

To remove this utility, delete the folder ESMPolicyToCCSStandard that the utility Web package has created.

About the input file in the ESM Policy to CCS Standard Migration Utility

The migration utility requires the ESM Policy XML. You can generate the ESM Policy XML by using the Policy Tool, which is provided with ESM. The Policy Tool utility exports ESM policies as XML formatted files.
Executing the migration utility

To start using the migration utility, you have to copy all the files in an installation folder and then run the utility.

**Executing the migration utility**

- You must run the following format from the command prompt for the utility to start migrating data:

  ```
  ESMPolicyToCCSStandard.exe -e <esmpolicy.xml> -m {NUMERIC | STRING} [-c {message categories}] [-o {ccsstandard.xml}] [-xs]
  ```

  The following table describes the parameters and their corresponding descriptions:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-e</td>
<td>ESM Policy XML file path. You must specify the path of the ESM Policy XML using this option. The path must exist and be accessible.</td>
</tr>
<tr>
<td>-m</td>
<td>This option is mandatory. You can specify either NUMERIC or STRING. If NUMERIC is specified, the utility creates CCS check expression based on ESM security message's numeric ID. If you specify the string, the utility creates CCS check expression based on ESM security message's string ID. See “About the message IDs in ESM Policy to CCS Standard Migration Utility” on page 881.</td>
</tr>
<tr>
<td>-o</td>
<td>This parameter is optional. Output Standard XML file path. You can specify the path for this output standard XML file by using this option. The path must exist and be accessible. The path can be a directory, a filename, or an entire path of a file. By default, output standard XML is created in the current directory and the filename is Standard-&lt;ESM Policy&gt;.xml.</td>
</tr>
<tr>
<td>-xs</td>
<td>This parameter is optional. If you specify this option, then the migration utility does not migrate the ESM suppressions to CCS Standard. See “About ESM suppressions migration” on page 881.</td>
</tr>
</tbody>
</table>
This parameter is optional. You can customize the default list of the messages categories that are migrated to the standard.

For example, if you do not want to migrate the messages whose categories are system Information, then you can use the -c option with the list of comma separated message categories in addition to the other regular options whilst executing the migration tool.

ESMPolicyToCCSStandard.exe -e "policy.xml" -m STRING -c 1,2,3,8,500

In the above example,-c 1,2,3,8,500 refers to migration of all messages that belong to the following categories: Policy Compliance, Patch Assessment, Change Notification, ICE, Network Assessment respectively.

See “About the default category iDs for creating the formula” on page 880.

The following is the example of the format:

ESMPolicyToCCSStandard.exe -e "D:\ESM\ESMPolicies\CIS\Window2003\ciswin2k3DC.xml" -m STRING -o "D:ESM\CCS Standards\CIS\CIS Win2K3 Domain Controller.xml" -c 1,2,3,8,500.

### About the default category iDs for creating the formula

By default, the Migration utility uses the messages with the following category IDs for creating the formula:

Table 22-2 lists the default category iDs for creating the formula

<table>
<thead>
<tr>
<th>Category ID</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Policy Compliance</td>
</tr>
<tr>
<td>2</td>
<td>Patch Assessment</td>
</tr>
<tr>
<td>3</td>
<td>Change Notification</td>
</tr>
<tr>
<td>7</td>
<td>System Information</td>
</tr>
<tr>
<td>8</td>
<td>ICE</td>
</tr>
<tr>
<td>500</td>
<td>Network Assessment</td>
</tr>
</tbody>
</table>

See “Table 22-2” on page 880.
About the log file in the ESM Policy to CCS Standard Migration Utility

The migration utility creates a log file in the same location from where you execute the utility. The name of the log file is as follows:

```
ESMPolicyToCCSStandard.<ESMPolicyFilename>.<DateTime>.<Process ID>.<Sequence Number>.csv
```

About ESM suppressions migration

If you run the migration utility without specifying the `–xs` option, then the ESM suppressions gets migrated to CCS Standard. The utility creates the "Is any ESM message suppressed?" check for each module. The "Is any ESM message suppressed?" check fails if any ESM message is suppressed. The migration utility does not create multiple CCS checks per suppressed message in ESM. It creates one such check per ESM module for each ESM OS version. As evidence for the check failure, you can see the suppressed messages for the corresponding ESM module. You can mark the CCS check as exception and use the features that the CCS Exception Management application provides.

**Note:** For the "Is any ESM message suppressed?" check to work as explained, you must uncheck the 'Do not collect suppressed messages' check box in ESM data collector configuration before data collection. When you uncheck the 'Do not collect suppressed messages' check box, the ESM data collector collects the suppressed messages during data collection.

About the message IDs in ESM Policy to CCS Standard Migration Utility

Every security message that an ESM check generates has a distinct numeric ID. The string ID is the string representation for the numeric message ID and is platform independent.

For example, for the ESM security message “System allows blank passwords,” the numeric IDs for different OS Versions are as follows:

<table>
<thead>
<tr>
<th>OS Version</th>
<th>Message Numeric ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>105336</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>205336</td>
</tr>
<tr>
<td>Windows 2008</td>
<td>248336</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>228336</td>
</tr>
</tbody>
</table>
OS Version | Message Numeric ID
--- | ---
Windows XP | 200336

However, the message string ID across all OS versions is “ESM_PASSTNONE”. Only the Message IDs that belong to one of the following message categories are included for migration:

- Policy compliance
- Patch Assessment
- Change notification
- System information
- ICE
- Network assessment

**Advantages and disadvantages of policy migration based on the Message String ID**

Using the `-m STRING` option creates CCS check expression based on the Message String ID.

The advantage of policy migration based on the Message String ID is that the Message String ID is platform independent. Hence, you can copy the check and use it for the ESM assets that are running on different operating systems by changing the target type.

The disadvantage is that the raw reports of the policy runs contain only the Message Numeric ID of the security messages. The ESM data collector retrieves the Message String ID from the Message Schema XML which is deployed with the ESM data collector. For CCS 10.0 Update, this Message Schema XML is generated from the security-content.xml of SU 2010.03.01 (SU 39).

Sometimes, the ESM data collector may fail to retrieve the Message String ID of the security message. This happens when an ESM agent with a higher SU version reports a security message that is newly added in the specified SU. In such a scenario, the check may not evaluate as expected. As a resolution, you must obtain the ESM data collector upgrade package and upgrade the SU version of the Message Schema XML and the SU Resources assembly.
Advantages and disadvantages of migration based on Message Numeric ID

Using the ‘-m NUMERIC’ option creates CCS check expression based on Message Numeric ID.

The advantages of policy migration based on the Message Numeric is that if the ESM data collector cannot find the metadata for an ESM message in its Message Schema XML, it requests the ESM manager to format the messages. Hence, irrespective of the SU version of the ESM data collector, the CCS check is always evaluated as expected. The ESM data collector gathers the details from the ESM manager if an ESM agent with a higher SU reports a security message, which is new in the specified SU. In such a scenario, the CCS check is evaluated as expected even though metadata for that message is not available with the ESM data collector.

The disadvantages is that the Message Numeric ID is platform-dependent. Hence, the same check cannot be used across ESM agents that are installed on different operating systems.

Limitations of the migration utility

The migration utility has the following limitations:

- This utility does not support automatic synchronization of modified ESM policies and CCS standards. For example, if you translate ESM policy "ESM_A" CCS standard "CCS_A". Afterward, if you modify "ESM_A", you have to re-run the utility to create a new version of the standard.

- Only one CCS check is created for an ESM check that is based on a name-list or a template. Therefore, the ESM messages that are reported for an entry in a name-list or a template are reported as evidence.

- You cannot use the utility to migrate the ESM policies for the following ESM platforms:
  - NDS/NetWare
  - Tru64
  CCS 10.0 Update does not support the NDS/NetWare and Tru64 target types for ESM data collector.

- To migrate ESM suppressions to CCS, the utility creates the CCS check “Is any ESM message suppressed?” for each module. The “Is any ESM message suppressed?” check fails if any ESM message is suppressed. The utility does not create multiple CCS checks per suppressed message in ESM. Also, the utility does not convert the ESM suppressions to CCS exceptions. However, you can manually mark the check “Is any ESM message suppressed?” as CCS exception.
You cannot choose the message categories to be considered when you migrate the ESM checks. The utility uses all the categories that are mentioned in the About Message string ID.

See “About the message IDs in ESM Policy to CCS Standard Migration Utility” on page 881.

The utility migrates only the enabled ESM checks from the ESM policy.

Troubleshooting for ESM Policy to CCS Standard Migration Utility

You may encounter problems when you use the migration utility. This chapter includes information on the problems that may occur and their resolution.

Table 22-3  Migration utility problems and their resolution

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Could not find file &lt;path&gt;\Symantec.CCS.Apps.Standards.Exceptions.dll</td>
<td>If you have not yet visited Standards view from the CCS console, assemblies related to standards do not exist in the console installation folder. Launch the CCS 10.0 Update console and go to the Standards UI. Go to Manage &gt; Standards.</td>
</tr>
<tr>
<td>CCS Console pulls assemblies dynamically to the CCS installation folder (i.e. %APPDATA%\Symantec\CCS-&lt;hostname&gt;) as and when it needs them.</td>
<td></td>
</tr>
<tr>
<td>Could not retrieve module long name for '&lt;module short name&gt;', skipping all checks for this module. Use the updated Symantec.CSM.Resources.ESMSUResources.dll</td>
<td>The ESM Policy XML contains the module short name for the ESM modules that are included in the policy. The utility first retrieves the code for the module long name from the Security Content XML. The utility then retrieves the actual module long from the SU Resources assembly. If either of them is out-dated, it may not contain information for the modules that were recently added in ESM content. Without the module long name, the utility cannot create CCS 10.0 Update checks because the CCS 10.0 Update ESM Message entity schema only understands module long names. To resolve this issue, you need to use the utility with the latest Security Content XML and latest SU Resources assembly.</td>
</tr>
</tbody>
</table>
### Table 22-3 Migration utility problems and their resolution (continued)

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Cannot locate the latest Security Content XML | Security Content XML is present in the update package that is created for RDL and is shipped with every Security Update released by ESM Content. You can find the update package for RDL in the following location on the ESM manager: `<ESM Installation Folder>\update\ble\<Latest SU Version>\en\UpdatePackage.rdl`. Perform the following in the given order:  
  - Create a copy of the package. Do not tamper the original file because RDL may give errors if it fails to find the file UpdatePackage.rdl.  
  - Rename it from UpdatePackage.rdl to UpdatePackage.zip.  
  - Extract the content of this compressed file.  
  - Copy the security-content.xml file from the extracted folder. Save the XML in the CCS 10.0 Update console installation folder from where you intend to run the Symantec ESM Policy to CCS Standard Migration Utility.  
  **Note:** If a new module is added in the latest SU update, you need the corresponding ESM data collector upgrade package. |
| Cannot locate the latest SU Resources Assembly | Copy the latest Symantec.CSM.Resources.ESMSUResources.dll from the `<DPS installation Folder>\Data Collectors\ESM` to the CCS 10.0 Update console installation folder from where you intend to run the Symantec ESM Policy to CCS Standard Migration Utility.  
  If the Symantec.CSM.Resources.ESMSUResources.dll in the `<DPS Installation Folder>\Data Collectors\ESM` is also outdated, you need to update CCS content. |
### About the CCS Data Migration utility

During the upgrade process of the Control Compliance Suite 9.0.1 to the Control Compliance Suite 10.0 you can also migrate the databases of the individual CCS applications. Use the CCS Data Migration utility to migrate the data of the applications such as, Extended Evidence Sources, Reports, Dashboard, Assets, and Policies. The CCS Data Migration utility is an executable, MigrationUtility.exe and is located in the `<Install Directory>\Application Server` directory of the product.

You are prompted to run the CCS Data Migration utility after the upgrade process, or you can choose to run the utility at a later stage.

The CCS Data Migration utility extracts the SQL connection details from the Application Server and shuts down the Application Server Service. After the migration is complete, the Application Server Service is automatically restarted.

The CCS Data Migration utility lets you migrate data of the following applications:

- Evidence Management
- Reports and Dashboards data
- Asset data

### Table 22-3  Migration utility problems and their resolution *(continued)*

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Warning message: ESM OS Version '[ESM OS Version]' is not supported. Skipping migration of checks enabled for it. | This warning message is displayed in case of the following:  
- A different ESM OS version is encountered.  
- Migration of all checks that are enabled for that ESM OS version is skipped. |
| Warning message:  
The description information for the CCS Check may be blank as the utility could not retrieve the ESM Check Description. | The ESM check description is migrated as CCS check description. First the migration utility retrieves the check description code from the Security Content XML. Then the utility retrieves the actual text for the check description from the SU Resources assembly. This error may occur if either of them is out-dated.  
To resolve this problem, use the updated Security Content XML and updated SU Resources Assembly. |
Policies

See “Prerequisites for running the CCS Data Migration Utility” on page 887.

See “Running the CCS Data Migration Utility” on page 888.

Prerequisites for running the CCS Data Migration Utility

Following are the prerequisites for running the CCS Data Migration Utility:

■ You must be in the role of CCS Administrator to run the CCS Data Migration Utility.

■ You must run the CCS Data Migration Utility on the computer which has the CCS Application Server is installed.

■ Set the value of the **Index creation memory (in KB)** to 0 for the SQL server. The **Index creation memory** setting can be done through the **Memory** page of the **SQL Server Properties** dialog box.

■ You must ensure that no jobs are running when you run the CCS Data Migration Utility.

■ You must configure and activate the SQL Server Service Broker for successful migration of the Reporting database, CSM_Reports.

  See “Configuring the SQL Server Service Broker” on page 888.

Before running the CCS Data Migration Utility, it is recommended that you change the initial size of tempdb to 1 GB and set Auto Growth to 10% of the initial size on the production database (CSM_DB) server and the reporting database (CSM_Reports) server. You can avoid memory related errors while running the reporting synchronization job under peak load condition by changing these settings.

**To change the settings of tempdb**

1. Connect to the SQL database
2. Expand Databases > System Databases > tempdb.
3. Right click tempdb and select Properties.
4. Click Files. Set the Initial size of tempdb to 1024 MB. The default value for Auto Growth is 10% and it is the recommended value.

See “About the CCS Data Migration utility” on page 886.

See “Running the CCS Data Migration Utility” on page 888.
Configuring the SQL Server Service Broker

By default, the Control Compliance Suite configures the SQL Server Service Broker. If you have configured the SQL Server Service Broker for any specific scenario, then you must execute the stored procedure, spManageUDMSQLBroker.

The scenarios for which the configuration of the SQL Server Service Broker can change are as follows:

- The reporting database is installed or upgraded by a user who is not in the role of a dbo.
- The reporting database is recovered from the back-up.
- The user credentials that are configured to access or synchronize the reporting database have changed.

You must execute the stored procedure, spManageUDMSQLBroker to activate and configure the SQL Server Service Broker for the specific user context. You must execute the stored procedure in the user context that has the privileges to run the database synchronization process.

The command to execute the stored procedure spManageUDMSQLBroker is as follows:

```
exec dbo.spManageUDMSQLBroker 1, '<Reporting user name>', '<RDB Name>'
```

Running the CCS Data Migration Utility

After the upgrade process is complete, you are prompted to run the CCS Data Migration Utility. You can choose to run the utility at this stage or later. You can also select certain applications at a time for migration.

---

**Note:** You must take a backup of the reporting database, before beginning the database migration process.
To run the CCS Data Migration Utility

1  Navigate to the <Install Directory>\Application Server.
   (By default, the <Install Directory> is C:\Program Files\Symantec\CCS folder).

2  Double-click MigrationUtility.exe.
   In the Migrate Application Data dialog box, by default, all the applications are checked.

   Note: You must not uncheck the option, Reports and Dashboards data in the utility.

3  Click Migrate to start the database migration process.
   The Evidence Management, Reports and Dashboards data, Asset data, and Policies are migrated by the utility. You can view the progress of the migration in the Status pane.
   The status pane also shows the status of post migration operations. For the Reports and Dashboards data, the post migration operation includes triggering of the synchronization job for the reporting database. You can track the status of the synchronization job through the jobs workspace.

4  After migration is complete, click Finish.
   Click Cancel if you want to stop the data migration when in progress.

   Note: In case of an error, click View Errors to view the error details.

See “About the CCS Data Migration utility” on page 886.
See “Prerequisites for running the CCS Data Migration Utility” on page 887.

Skipping CCS Reports and Dashboards data migration

After you upgrade to Control Compliance Suite 10.0, if you do not want to migrate the existing reporting database of the previous CCS installation, then you need not use the CCS Data Migration utility.
To skip the Reports and Dashboards data migration

1. Navigate to the <install directory>\Application Server folder of the product. (By default, the folder is, C:\Program Files\Symantec\CCS\Reporting and Analytics\Application Server).
2. Run the CleanReportingData.exe.

**Note:** On running the CleanReportingData.exe, all data and database objects of the old reporting database are deleted.


See “Synchronizing the reporting database” on page 167.
About the Unified Data Model

The Control Compliance Suite Reporting database was redesigned for version 10.0. The new design is named the Unified Data Model (UDM). The UDM provides the following attributes to the database:

- **Extensibility** The database can accept data from the Control Compliance Suite modules and third-party applications with a minimal change. Additions to the data or updates to the data do not affect the existing data. The reports and the dashboards function in the same way.

- **Scalability** The model is planned and implemented to handle metrical and dimensional data for assets and users within a huge enterprise environment. The model generates reports in a timely manner.

- **Versatility** The model allows for customizations with a low degree of difficulty.

See “Mapping 9.0.1 tables to 10.0 views” on page 898.

About the asset-based views

The asset-based views are generated from the data in the reporting database. The following table lists the asset-based views and their descriptions:
### Table A-1  Asset-based views

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vAsset</td>
<td>The common asset information for all asset types.</td>
</tr>
<tr>
<td>vAssetAttributeLookup</td>
<td>All asset data in a lookup format including common assets and attributes.</td>
</tr>
<tr>
<td>vAssetResults</td>
<td>Asset-based results.</td>
</tr>
<tr>
<td></td>
<td>An example is aggregated compliance scores.</td>
</tr>
<tr>
<td>vAssetResultsLookup</td>
<td>The same data as the vAssetResults, but in a lookup format.</td>
</tr>
<tr>
<td>vAssetRollup</td>
<td>Asset-based rollup metrics.</td>
</tr>
<tr>
<td></td>
<td>An example is exception counts.</td>
</tr>
<tr>
<td>vAssetFolder</td>
<td>Asset folders.</td>
</tr>
<tr>
<td>vAssetFolderMembership</td>
<td>Asset folder membership.</td>
</tr>
<tr>
<td>vAssetGroup</td>
<td>Asset groups.</td>
</tr>
<tr>
<td>vAssetGroupMembership</td>
<td>Asset group membership.</td>
</tr>
<tr>
<td>vAssetSummary</td>
<td>Summarizes the current version combining results and rollup information.</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.

See “Mapping 9.0.1 tables to 10.0 views” on page 898.

### About the standards-based views

The standard-based views are generated from the reporting database. The following table lists the standards-based views and their descriptions:

### Table A-2  Standards-based views

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vStandard</td>
<td>Standards.</td>
</tr>
<tr>
<td>vStandardChecks</td>
<td>Checks on standards.</td>
</tr>
<tr>
<td>vStandardChecksRollup</td>
<td>Rollup metrics by check that are not associated to a specific asset.</td>
</tr>
</tbody>
</table>
Table A-2  Standards-based views (continued)

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vStandardCheckResults</td>
<td>Raw check results.</td>
</tr>
<tr>
<td>vStandardCheckResultsWithEvidence</td>
<td>Raw check results including text and XML evidence.</td>
</tr>
<tr>
<td>vStandardResults</td>
<td>Standard aggregate and count results.</td>
</tr>
<tr>
<td>vStandardRollup</td>
<td>Standard metrics.</td>
</tr>
<tr>
<td></td>
<td>An example is exception counts.</td>
</tr>
<tr>
<td>vStandardSections</td>
<td>Standard sections.</td>
</tr>
<tr>
<td>vStandardSummary</td>
<td>Current standard values that combine results and rollup information.</td>
</tr>
<tr>
<td>vStandardTags</td>
<td>Tags associated to standards.</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.

See “Mapping 9.0.1 tables to 10.0 views” on page 898.

About the asset-to-standard views

The following table lists the asset-to-standard results views and their descriptions:

Table A-3  Asset-to-standard views

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vComplianceAssetSummary</td>
<td>A compliance-based view that combines assets, standards, asset results, and standard results.</td>
</tr>
<tr>
<td>vComplianceAssetSummaryLookup</td>
<td>The same data as the vComplianceAssetSummary but in a lookup format.</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.

See “Mapping 9.0.1 tables to 10.0 views” on page 898.

About the entitlement-based views

The entitlements in Control Compliance Suite facilitate the ability to monitor access rights within the organization. The Entitlements view in the console lets you efficiently gather the permissions data from the various platforms.
The following table lists the entitlement-based views and their descriptions:

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vEntitlementControlPoint</td>
<td>Entitlement control point is a version of the asset under control.</td>
</tr>
<tr>
<td>vEntitlementReviewCycle</td>
<td>A specific review cycle and the state of the review.</td>
</tr>
<tr>
<td>vEntitlementReviewCyclePlan</td>
<td>The plan that is used for the review cycle.</td>
</tr>
<tr>
<td>vEntitlementFrequency</td>
<td>The frequency that is used for the review cycle. For example, the frequency can be a weekly review or a monthly review.</td>
</tr>
<tr>
<td>vEntitlementControlPointTrusteeMembership</td>
<td>Maps a control point to a specific trustee.</td>
</tr>
<tr>
<td>vEntitlementTrustee</td>
<td>Trustee.</td>
</tr>
<tr>
<td>vEntitlementTrusteeFlat</td>
<td>A flatten view of the trustee information. The view is used in reporting.</td>
</tr>
<tr>
<td>vEntitlementTrusteePermissionLookup</td>
<td>Tracks changed permissions for a trustee</td>
</tr>
<tr>
<td>vEntitlementTrusteeLookup</td>
<td>Trustee information. For example, the read permissions for a trustee.</td>
</tr>
<tr>
<td>vEntitlementWorkflowTrail</td>
<td>Participants can provide comments during the review cycle and stores the different states of a control point in a review cycle.</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.
See “Mapping 9.0.1 tables to 10.0 views” on page 898.

**About the policy-based views**

The policy features of Control Compliance Suite let you manage, publish, and track your policies across an organization. You can also collect evidence of due care of the policy compliance. Policies include the control statements that are mapped to regulations and frameworks. The ability to map lets you discover any gaps in the current policies and lets you comply with the regulation requirements for your organization.
The following table lists the policy views and their descriptions:

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vPolicy</td>
<td>Policy data</td>
</tr>
<tr>
<td>vPolicyRollup</td>
<td>Policy rollup metrics</td>
</tr>
<tr>
<td>vPolicyCategory</td>
<td>Policy categories</td>
</tr>
<tr>
<td>vPolicyClarification</td>
<td>Policy clarifications</td>
</tr>
<tr>
<td>vPolicyComment</td>
<td>Policy comments</td>
</tr>
<tr>
<td>vPolicyContentLevel</td>
<td>Content level for a policy</td>
</tr>
<tr>
<td>vPolicyContentNote</td>
<td>Content notes</td>
</tr>
<tr>
<td>vPolicyContentToStatement</td>
<td>Content to statement mapping</td>
</tr>
<tr>
<td>vPolicyControlStatement</td>
<td>Control statements</td>
</tr>
<tr>
<td>vPolicyStatementToCheck</td>
<td>Control statements to check mapping</td>
</tr>
<tr>
<td>vPolicyStatementToEvidence</td>
<td>Control statement to third-party evidence mapping</td>
</tr>
<tr>
<td>vPolicyStatementToQuestion</td>
<td>Control statement to questions mapping</td>
</tr>
<tr>
<td>vPolicyToStatement</td>
<td>Policy to control statement mapping</td>
</tr>
<tr>
<td>vPolicyToTarget</td>
<td>Policy to associated groups, folders, and assets</td>
</tr>
<tr>
<td>vPolicyUserRespones</td>
<td>Policy user responses</td>
</tr>
<tr>
<td>vPolicyTags</td>
<td>Tags that are associated with the policies</td>
</tr>
<tr>
<td>vPolicyContent</td>
<td>Content</td>
</tr>
<tr>
<td>vFrameworkName</td>
<td>Content framework name</td>
</tr>
<tr>
<td>vRegulationName</td>
<td>Regulation Name lookup</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.
See “Mapping 9.0.1 tables to 10.0 views” on page 898.
About the user views

The views contain user specific information. The following table lists the user views and their descriptions:

**Table A-6**  
**User views**

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vUser</td>
<td>Users that are configured from the user management.</td>
</tr>
<tr>
<td>vUserSubject</td>
<td>Native explicit read permissions for objects.</td>
</tr>
<tr>
<td></td>
<td>The objects can be asset folders.</td>
</tr>
<tr>
<td>vUserTest</td>
<td>Native explicit read permissions for objects.</td>
</tr>
<tr>
<td></td>
<td>The objects can be policy or standards.</td>
</tr>
<tr>
<td>vUserAsset</td>
<td>Resolved users to assets.</td>
</tr>
<tr>
<td></td>
<td>The dashboard systems use the view and the view is based on the last logon to the Web console.</td>
</tr>
<tr>
<td>vUserStandard</td>
<td>Resolved users to standards.</td>
</tr>
<tr>
<td></td>
<td>The dashboard systems use the view and the view is based on the last logon to the Web console.</td>
</tr>
<tr>
<td>vUserPolicy</td>
<td>Resolved users to policies.</td>
</tr>
<tr>
<td></td>
<td>The dashboard systems use the view and view is based on the last logon to the Web console.</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.

See “Mapping 9.0.1 tables to 10.0 views” on page 898.

About the exception views

The following table lists the exception views and their descriptions:

**Table A-7**  
**Exception views**

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vException</td>
<td>Exception information</td>
</tr>
<tr>
<td>vExceptionIdentity</td>
<td>Users that are mapped to an exception</td>
</tr>
<tr>
<td>vExceptionMembership</td>
<td>A map of the exceptions to the objects that they apply</td>
</tr>
</tbody>
</table>
Table A-7  Exception views (continued)

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vExceptionTags</td>
<td>Tags that are associated to exceptions</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.
See “Mapping 9.0.1 tables to 10.0 views” on page 898.

About the tag views

The following table lists the tag views and their descriptions:

Table A-8  Tag views

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vTag</td>
<td>Tag definitions</td>
</tr>
<tr>
<td>vReportTags</td>
<td>Labels for the reports the international tables</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.
See “Mapping 9.0.1 tables to 10.0 views” on page 898.

About the third-party views

The following table lists the third-party views and their descriptions:

Table A-9  Third-party views and descriptions

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vThirdPartyProviders</td>
<td>All of the third-party providers that are registered in the evidence system</td>
</tr>
<tr>
<td>vThirdPartyControls</td>
<td>All of the third-party controls that are registered in the evidence system and the controls that are mapped to content</td>
</tr>
<tr>
<td>vThirdPartyEvidence</td>
<td>Provider imported evidence</td>
</tr>
<tr>
<td>vThirdPartyEvidenceLookup</td>
<td>Provider imported flattened custom XML evidence that is flattened</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.
See “Mapping 9.0.1 tables to 10.0 views” on page 898.

Mapping 9.0.1 tables to 10.0 views

The version 10.0 database uses views to display customer information. A view is a virtual table that is an abstract data structure.

This data structure has the following advantages:

■ Views can display a subset of a table's data.
■ Views can join and simplify multiple tables into one virtual table.
■ Views can display aggregated data easily.
■ Views can hide the complexity of the underlying database.
■ Views can provide another level of security because you can add permissions to views.

Table A-10 displays the result of migrating 9.0.1 tables to 10.0 views. A column may have multiple listings for either the tables or the views because the data in the tables are equivalent.

<table>
<thead>
<tr>
<th>9.0.1 table</th>
<th>10.0 view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>vAsset</td>
</tr>
<tr>
<td>Asset_Detail</td>
<td>vAssetAttributesLookup</td>
</tr>
<tr>
<td>BO_AssetToTags</td>
<td>vAssetTags</td>
</tr>
<tr>
<td>Checks</td>
<td>vStandardChecks</td>
</tr>
<tr>
<td>EM_ReviewCycle_FACT</td>
<td>vEntitlementWorkflowTrail</td>
</tr>
<tr>
<td>EM_ControlPoint_Fact</td>
<td>vControlPoint</td>
</tr>
<tr>
<td>EM_ControlPoint_Fact</td>
<td>vControlPointSnapshot</td>
</tr>
<tr>
<td>EM_Entritement_FACT</td>
<td>vEntitelymentTrusteeLookup,</td>
</tr>
<tr>
<td></td>
<td>vEntitelymentTrusteeFlat</td>
</tr>
<tr>
<td>EM_EntritementChange_FACT</td>
<td>vEntitelymentTrusteePermissionLookup</td>
</tr>
<tr>
<td>EM_Entritement_FACT</td>
<td>vEntitelymentTrustee</td>
</tr>
<tr>
<td>EM_FrequencySettings</td>
<td>vEntitelymentReviewFrequency</td>
</tr>
</tbody>
</table>
### Table A-10  
**Mapping 9.0.1 tables to 10.0 views (continued)**

<table>
<thead>
<tr>
<th>9.0.1 table</th>
<th>10.0 view</th>
</tr>
</thead>
<tbody>
<tr>
<td>EM_ReviewCycle</td>
<td>vEntitlementReviewCycle</td>
</tr>
<tr>
<td>EM_ReviewCycleSettings</td>
<td>vEntitlementReviewCyclePlan</td>
</tr>
<tr>
<td>CM_WorkflowTrail_Entry (where Type is control point)</td>
<td>vEntitlementWorkflowTrail</td>
</tr>
<tr>
<td>TP_Fact_Table</td>
<td>vThirdPartyEvidence,</td>
</tr>
<tr>
<td></td>
<td>vThirdPartyEvidenceLookup</td>
</tr>
<tr>
<td>PM_StatementCustomEvidenceProvider</td>
<td>vThirdPartyControls,</td>
</tr>
<tr>
<td></td>
<td>vThirdPartyProviders</td>
</tr>
<tr>
<td>EX_AssociationFor</td>
<td>vExceptionStandardCheckMapping</td>
</tr>
<tr>
<td>EX_AssociationTo</td>
<td>vExceptionStandardCheckMapping</td>
</tr>
<tr>
<td>EX_Exceptions</td>
<td>vException</td>
</tr>
<tr>
<td>EX_ExceptionAssociationFor</td>
<td>vExceptionMembership</td>
</tr>
<tr>
<td>EX_ExceptionAssociationTo</td>
<td>vExceptionMembership</td>
</tr>
<tr>
<td>EX_Identity</td>
<td>vExceptionIdentity</td>
</tr>
<tr>
<td>PM_Clarification</td>
<td>vPolicyClarification</td>
</tr>
<tr>
<td>PM_Comment</td>
<td>vPolicyComment</td>
</tr>
<tr>
<td>PM_Content</td>
<td>vPolicyContent</td>
</tr>
<tr>
<td>PM_Content</td>
<td>vPolicyContent</td>
</tr>
<tr>
<td>PM_ContentStatement</td>
<td>vPolicyContentToStatement</td>
</tr>
<tr>
<td>PM_ContentStatementLevel</td>
<td>HierarchyRelationship</td>
</tr>
<tr>
<td>PM_Level</td>
<td>vPolicyContentLevel</td>
</tr>
<tr>
<td>PM_MergedStatement</td>
<td>N/A</td>
</tr>
<tr>
<td>PM_Note</td>
<td>vPolicyContentNote</td>
</tr>
<tr>
<td>PM_Policy</td>
<td>vPolicy</td>
</tr>
<tr>
<td>PM_PolicyStatement</td>
<td>vPolicyToStatement</td>
</tr>
<tr>
<td>9.0.1 table</td>
<td>10.0 view</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>PM_PolicyTargetAssetCollection</td>
<td>vPolicyToResolvedAsset</td>
</tr>
<tr>
<td>PM_Statement</td>
<td>vPolicyControlStatement</td>
</tr>
<tr>
<td>PM_StatementCheck</td>
<td>vPolicyStatementToCheck</td>
</tr>
<tr>
<td>PM_StatementEntitlement</td>
<td>N/A</td>
</tr>
<tr>
<td>PM_StatementQuestion</td>
<td>vPolicyStatementToQuestion</td>
</tr>
<tr>
<td>PM_UserResponse</td>
<td>vPolicyUserResponse</td>
</tr>
<tr>
<td>Asset_Std_Summ,</td>
<td>vComplianceAssetSummary,</td>
</tr>
<tr>
<td>Asset_Std_Summ_Archive</td>
<td>vComplianceAssetSummaryLookup</td>
</tr>
<tr>
<td>Asset_Summary,</td>
<td>vAssetResults,</td>
</tr>
<tr>
<td>Asset_Summary_Archive</td>
<td>vAssetResultsLookup</td>
</tr>
<tr>
<td>Fact_Table,</td>
<td>vStandardCheckResults,</td>
</tr>
<tr>
<td>Fact_Table_Archive</td>
<td>vStandardCheckResultsLookup</td>
</tr>
<tr>
<td>EvalChecksToEvidence,</td>
<td>vStandardCheckResultsWithEvidence</td>
</tr>
<tr>
<td>EvalChecksToEvidence_Archive</td>
<td></td>
</tr>
<tr>
<td>Standards_Summary,</td>
<td>vStandardSummary</td>
</tr>
<tr>
<td>Standards_Summary_Archive</td>
<td></td>
</tr>
<tr>
<td>Sections</td>
<td>vStandardSections</td>
</tr>
<tr>
<td>Evaluation_Jobs</td>
<td>N/A</td>
</tr>
<tr>
<td>Standards</td>
<td>vStandard</td>
</tr>
<tr>
<td>BO_Tags</td>
<td>vTag</td>
</tr>
<tr>
<td>CM_UserMgmt_SecurityPrincipals</td>
<td>vUser</td>
</tr>
</tbody>
</table>

See “About the Unified Data Model” on page 891.
See “Running the CCS Data Migration Utility” on page 888.
Troubleshooting

This appendix includes the following topics:

■ About troubleshooting
■ Deployment troubleshooting
■ Configuration troubleshooting
■ Asset import troubleshooting
■ Data collection troubleshooting
■ Console and Web Console troubleshooting
■ Policy Module troubleshooting
■ Symantec ESM troubleshooting
■ Reports troubleshooting
■ Evidence import troubleshooting

About troubleshooting

Your Control Compliance Suite deployment is a complex of interlocking pieces. From time to time, it is possible that some part of the system may fail. If a failure occurs, the troubleshooting guide can help you to correct it.

In addition to the troubleshooting guide, you should consult the technical support knowledge base. The knowledge base includes references to additional issues and includes additional symptoms and corrective actions.

The knowledge base is available at the following URL:
http://www.symantec.com/business/support/overview.jsp?pid=53741&view=kb
You may require troubleshooting assistance with the following types of issues:

- Control Compliance Suite deployment
  See “Deployment troubleshooting” on page 902.

- Control Compliance Suite configuration
  See “Configuration troubleshooting” on page 907.

- Asset import
  See “Asset import troubleshooting” on page 908.

- Data collection
  See “Data collection troubleshooting” on page 910.

- Control Compliance Suite Console and Web Console
  See “Console and Web Console troubleshooting” on page 913.

- Policy Module
  See “Policy Module troubleshooting” on page 922.

- Symantec ESM
  See “Symantec ESM troubleshooting” on page 923.

### Deployment troubleshooting

The following possible problems can occur when you deploy the Control Compliance Suite.

**Failed Directory Server Installation**

See “Troubleshooting a failed Directory Server Installation” on page 903.

**Certificate does not match specified computer during deployment**

See “Troubleshooting when the Certificate does not match a specified computer during deployment” on page 903.

**Application Server Installation Wizard rejects Directory Server credentials**

See “Troubleshooting when the Application Server installation wizard rejects the Directory Server credentials” on page 904.

**Application Server, Directory Server, or Data Processing Service fail to start**

See “Troubleshooting when the Application Server, Directory Server, or Data Processing Service fail to start” on page 904.

**When you install with Remote Desktop Connection, installation logs are deleted when the user logs off**

See “Troubleshooting when installation logs are deleted when the user logs off after using Remote Desktop Connection to install” on page 905.
During the installation, an error message indicates that the state of the secure channel cannot be verified. See “Troubleshooting when an error message that indicates that the state of the secure channel cannot be verified appears during installation” on page 906.

When you install the Control Compliance Suite Console, an error message appears indicating that the Web server cannot be located. See “Troubleshooting when you encounter problems installing the Control Compliance Suite Console” on page 906.

When you install the Control Compliance Suite components on a virtual machine, an error warns that your screen does not meet the minimum required size. See “Troubleshooting when a warning appears about the minimum required screen resolution” on page 906.

Troubleshooting a failed Directory Server Installation

When you deploy the Control Compliance Suite (CCS), the CCS directory may fail to correctly install. If this error occurs, one of the following may be the cause:

- The domain account credentials that are used for the component are not valid. Supply valid credentials.
- The c:\Windows directory does not allow software to be installed. Change the permissions on the c:\Windows directory to allow software installation.
- Active Directory is not available. Install and configure Active Directory before installing CCS.
- The C:\Program Files directory on the Directory server host is compressed. Uncompress the C:\Program Files directory on the Directory server host. Reinstall the ADAM instance.

Troubleshooting when the Certificate does not match a specified computer during deployment

When you deploy the Control Compliance Suite (CCS), the certificate may not match the specified computer. If this error occurs, one of the following may be the cause:

- The ping utility has different results for the target computer when run from the Directory Server and from the target computer itself. Correct network errors to ensure that the same information appears when you use the ping utility from all computers.
An incorrect certificate type was specified during certificate creation. Create a new certificate of the correct type.

Troubleshooting when the Application Server installation wizard rejects the Directory Server credentials

When you deploy the Control Compliance Suite (CCS), the Application Server installation wizard may not accept the Directory Server credentials you supply. If this error occurs, one of the following may be the cause:

- The domain account credentials that are used for the component are not valid. Supply valid credentials.
- The credentials that were used to log on when the Directory Server was installed should be used. The credentials that were supplied during the installation should not be used. Supply the user credentials that were used to log on when the Directory Server was installed.

Troubleshooting when the Application Server, Directory Server, or Data Processing Service fail to start

When you deploy the Control Compliance Suite (CCS), the Application Server, the CCS directory, or a Data Processing Service instance may fail to start correctly. If this error occurs, the following may be the cause:
Host computer does not have Internet connectivity or connection to the VeriSign Web server is blocked.

Try any of the following solutions:

- Provide access to the VeriSign Web server the first time the service starts.
- Disable certificate checking for all components on the host.
- Manually download the Certificate Revocation List from VeriSign and install it on the host.
- In .NET Framework 3.5 there is a configuration option that allows bypassing the Authenticode verification by adding the following entry in the app.config file:

```xml
<configuration> <runtime>
<generatePublisherEvidence enabled="false"/> </runtime> </configuration>
```

For example, in a distributed setup, the Directory Support Service (DSS) is installed but after installation, the DSS, and Encryption Management Services do not start. To start the services, you can edit the Symantec.CSM.DSS.Service.exe.config file and Symantec.CSM.EncryptionManagement.Service.exe.config file and add the following lines:

```xml
<configuration> <runtime>
<generatePublisherEvidence enabled="false"/> </runtime> </configuration>
```

See “About logs and configuration files” on page 204.

**Troubleshooting when installation logs are deleted when the user logs off after using Remote Desktop Connection to install**

If you use Windows Remote Desktop Connection to install the Control Compliance Suite (CCS) components, the installation logs are deleted when you log off the computer.

Installation logs are stored in the `%temp%\csmsetup`. The folder that is used for the `%temp%` folder varies depending on the type of user logon. Files in the
%temp% folder are deleted automatically when a Remote Desktop Connection user logs out.

To retain these logs, you must manually copy the log file to another folder after the installation is complete but before logging out.

Troubleshooting when an error message that indicates that the state of the secure channel cannot be verified appears during installation

When you deploy the Control Compliance Suite (CCS), an error message may appear that indicates that the state of the secure channel cannot be verified. If this error message appears, it indicates that the computer has lost its secure channel with the domain.

To correct the issue, you must rejoin the computer to the domain.

Troubleshooting when an error message indicates the SSPI context cannot be generated during installation

When you deploy the Control Compliance Suite (CCS), an error message may appear that indicates that the SSPI context cannot be generated. The error message indicates that the computer that hosts the Microsoft SQL Server has lost its secure channel with the domain.

To correct the issue, you must rejoin the computer to the domain. You can then install CCS.

Troubleshooting when you encounter problems installing the Control Compliance Suite Console

When you install the Control Compliance Suite (CCS) Console an error message may indicate that the installer is unable to contact the Web server. If this message appears, you should use the IP address of the Web server instead of the server name.

Troubleshooting when a warning appears about the minimum required screen resolution

When you install the Control Compliance Suite (CCS) components on a virtual machine, a warning may appear that the screen resolution is below the minimum required if the virtual machine is minimized. If this error appears, repeat the installation with the virtual machine unminimized.
Configuration troubleshooting

The following configuration errors can occur in the Control Compliance Suite.

The user is unable to start the Certificate Management Console

See “Troubleshooting when the user is unable to start the Certificate Management Console” on page 907.

Synchronization jobs fail to complete

See “Troubleshooting when the user is unable to start the Certificate Management Console” on page 907.

Troubleshooting when the user is unable to start the Certificate Management Console

When you deploy the Control Compliance Suite (CCS), the Application Server, the CCS directory, or a Data Processing Service instance may fail to start correctly. If this error occurs, the following may be the cause:

A password error appears when the Certificate Management Console is started.

Verify that the user supplies the same password that was supplied during installation of the Directory Server.

The Certificate Management Console fails to start.

Verify that the user is an administrator of the ADAM or AD LDS installation on the Directory Server.

Verify that the user is a CCS Administrator.

Troubleshooting when synchronization jobs fail to complete after migration

If you use the Control Compliance Suite (CCS) Migration Utility, then start the CCS Console and start a Global Synchronization job, the synchronization jobs may fail to complete.

This error occurs because the synchronization job requires additional SQL Server permissions.

You should use the SQL Manager to assign the EXECUTE permission on the sp_upgradestats object to the database owner (dbo) of the CSM_Reports reporting database.
Asset import troubleshooting

The following errors can occur when you import assets:

Asset imports fail to complete
See “Asset import troubleshooting” on page 908.

Asset import jobs from a single site run slowly
See “Troubleshooting when asset import jobs from a single site run slowly” on page 909.

Asset import jobs fail and report an exception
See “Troubleshooting when asset import jobs fail and report an exception” on page 909.

Deleted ODBC data locations appear in the Data Processing Service settings
See “Troubleshooting when deleted ODBC data locations appear in the Data Processing Service settings” on page 910.

Troubleshooting when asset imports fail to complete

When you perform an Asset import, the import job may fail to complete correctly. If this error occurs, one of the following may be the cause:

Asset imports fail to complete.
Verify that the asset system is properly configured.
See “About assets” on page 233.
Verify that the reconciliation rules are correctly configured.
See “Creating reconciliation rules without manual review” on page 306.

Not all expected assets are imported.
Verify that the scope of the Asset Import job is valid for the given asset type.
See “About scopes in asset import” on page 349.

Not all assets of a given type are collected.
Verify that the data collector for the given asset type is properly configured.
The error message “An Error occurred in Data Query activity: Unable to retrieve list of Assets from ADAM: No Assets were resolved from the directory, either due to insufficient permissions or an invalid job definition” appears during asset import job processing.

Verify that the Application Server service account is trusted for delegation.

Verify that the Service Principal Names are properly registered.

Troubleshooting when asset import jobs from a single site run slowly

When you perform an Asset import, the import jobs from a single site may run more slowly than jobs from other sites. If a slow import happens, the following may be the cause:

One of the Data Processing Service Collectors that retrieve data from the site has failed.

Correct the fault that prevents the DPS from operating properly.

Temporarily unregister the DPS, then register it again when repair is complete.

Temporarily move the DPS to a site with no assets.

Troubleshooting when asset import jobs fail and report an exception

When you perform an Asset import, the Asset import job may fail with the following exception:

An error occurred in the data query activity. Unable to retrieve the list of assets from ADAM. No assets were resolved from the directory, either due to insufficient permissions or invalid job definition.

This error indicates that the asset types that you selected in the “Limit Asset Import Scope” dialog box do not match. The selected types should match the asset types that are contained in the asset folder or asset group that is used for asset import.

To correct the error, you should limit the asset import scope. You should include only the asset types that are contained in the asset folder or the asset group that is used for asset import.

For example, consider the following case:

■ You import Windows machines.
■ You use the “All Windows Machines” asset group.
■ The scope does not contain any domains, only Windows machines.
The scope that you select in the **Limit Asset Import Scope** dialog box contains only domains.

In this case, the asset import fails to resolve the assets unless you select “Machines” in the “Limit Asset Import Scope” dialog box.

**Troubleshooting when deleted ODBC data locations appear in the Data Processing Service settings**

When a user creates an ODBC data location and imports assets from the ODBC data location, then deletes the ODBC data location, the location may still appear in the Data Processing Service (DPS) settings.

If another user uses the data location, Asset Import jobs will fail, since the location no longer exists.

The user who created the ODBC data location or a Control Compliance Suite (CCS) Administrator should use the DPS Settings dialog to manually delete the platform and data location.

**Data collection troubleshooting**

The following errors can occur when you run data collection jobs:

- **Jobs fail to run**
  
  See “**Troubleshooting when data collection jobs fail to run**” on page 911.

- **Data collection jobs from a single site run slowly**
  
  See “**Troubleshooting when data collection jobs from a single site run slowly**” on page 911.

- **Exception appears during data collection for Oracle assets**
  
  See “**Troubleshooting when an exception appears during data collection for Oracle assets**” on page 912.

- **Data collection jobs fail with the error **Login failed for user.****
  
  See “**Troubleshooting when data collection jobs fail with the error **Login failed for user.**” on page 912.

- **Data collection jobs fail with an exception**
  
  See “**Troubleshooting when data collection jobs fail with an exception**” on page 912.

- **Data collection fails for Windows machines that do not have Internet Information Services installed**
See “Troubleshooting when “Computer Unreachable” errors appear for Windows computers that do not have Internet Information Services installed” on page 913.

Troubleshooting when data collection jobs fail to run

When you run a data collection job, the data collection job may fail to run properly at the scheduled time. If this error occurs, one of the following may be the cause:

- **Scheduled data collection jobs fail to run at the scheduled time.**
  - Verify that the scheduling user password is properly updated in user management.

- **Data collection jobs fail to run.**
  - Verify that the Application Server credentials are correct.

- **Data collection jobs fail to run.**
  - Verify that the Application Server and Directory Server credentials are both Local Administrators.

- **All jobs fail to run.**
  - Verify that the Production database host works properly.

- **Jobs fail to run, and the error “Dispatcher.SimpleDispatch” appears.**
  - Verify that the Symantec.CSM.DSS SPN is associated with only one account.

- **Jobs fail to run.**
  - Verify that the SPNs have been created properly. Also verify that the Service Name portion of the SPN for the Directory Service matches what is specified in the AppServerService.exe.config file.

Troubleshooting when data collection jobs from a single site run slowly

When you run data collection jobs, you may find that all data collection jobs from a single site run slowly.

One possible cause of this error is that one of the Data Processing Service Collectors that retrieve data from the site has failed. If this error occurs, you must correct the fault that prevents the DPS from operating correctly.

While you repair the error, you should remove the DPS from the site. If the failed DPS is associated with the site, the DPS Load Balancers continue to assign jobs to the DPS Collector. Until the DPS Collector is unable to retrieve the data and times out, the DPS Load Balancer does not reassign the job to another DPS Collector.

To remove the DPS Collector, you can do one of the following:

- Temporarily unregister the DPS, then register it again when repair is complete.
Troubleshooting when an exception appears during data collection for Oracle assets

When you run a data collection job, a `System.OutOfMemory` exception may appear when you collect data from Oracle assets. This error appears because data that the Control Compliance Suite (CCS) collects from Oracle Assets uses chained data queries. These queries are very memory-intensive.

To avoid this error, you should limit Oracle queries to 1000 assets per job.

Troubleshooting when data collection jobs fail with the error `Login failed for user`

When a data collection job runs, it may fail, and the error message `Login failed for user` may appear. If this error occurs, one of the following may be the cause:

- The ping utility has different results for the target computer when run from the Directory Server and from the target computer itself.
- Correct network errors to ensure that the same information appears when you use the ping utility from all computers.
- The Account that is used for the Data Processing Service is not a domain account.
- Use a domain account for the Data Processing Service.

Troubleshooting when data collection jobs fail with an exception

When you run data collection jobs, a data collection job may fail, and the following error message may appear:

An error occurred in the evaluation activity.
Unable to retrieve the list of assets from ADAM.
No assets were resolved from the directory, either due to insufficient permissions or invalid job definition.

If this error appears, it means that the standard that is associate with the asset group does not contain a target type that matches the assets in the asset group or the asset folder.

To correct the error, you should use the asset groups that contains the assets of the target type that the standard contains.

Consider the following example:
You run a data collection job with the standard that contains only “IIS Web Sites” target types. You use “All Windows Machines” asset group as to run the data collection. In this case, the data collection job fails unless you select an asset group that contains IIS Web Sites.

Troubleshooting when “Computer Unreachable” errors appear for Windows computers that do not have Internet Information Services installed

A data collection job can include both computers with the Microsoft Internet Information Services (IIS) Manager installed and computers without IIS installed. If you run a standard against that data collection job that includes IIS checks, the error “Computer Unreachable” appears for computers in the scope that do not have IIS installed.

Since the computer does not include IIS, the Control Compliance Suite (CCS) is unable to determine if the computer is reachable and that it does not collect data for non-IIS checks.

You should restructure your data collection job to separate out assets with IIS installed from the ones without IIS installed and recollect the data for the respective standards and assets.

Console and Web Console troubleshooting

The following errors can occur when using the Control Compliance Suite (CCS) Console and Web Console:

When installing the Control Compliance Suite Console, an error message appears indicating that the Web Server cannot be located.

See “Troubleshooting when you encounter problems installing the Control Compliance Suite Console” on page 906.

The user cannot start the Control Compliance Suite Console

See “Troubleshooting when the user cannot start the Control Compliance Suite Console” on page 915.

The Web Console is unable to connect to the Response Assessment module

See “Troubleshooting when the Web Console is unable to connect to the Response Assessment module” on page 916.

The Web Console does not correctly display Response Assessment module pages

See “Troubleshooting when the Web Console does not correctly display Response Assessment module pages” on page 916.
Configuration changes do not appear
See “Troubleshooting when configuration changes do not appear” on page 916.

The correct time does not appear on reports
See “Troubleshooting when the correct time does not appear on reports” on page 916.

Reports may cause a system slowdown or reports may fail
See “Troubleshooting when reports cause a system slowdown or reports fail” on page 917.

HTTP Error 401.1 - Unauthorized: Access is denied when you open the Web Console
See “Troubleshooting when the error HTTP Error 401.1 - Unauthorized: Access is denied appears when you open the Web Console” on page 917.

Blank reports may appear
See “Troubleshooting when blank reports appear” on page 917.

Error viewing dashboard on Web Console
See “Troubleshooting when an error appears while viewing a dashboard on the Web Console” on page 918.

Custom asset type does not appear in the console
See “Troubleshooting when you cannot create a custom asset type” on page 918.

Message “The Server is not operational” appears in the console
See “Troubleshooting when the message “The server is not operational” appears in the console” on page 918.

Message “The Server is not operational” appears in the console
See “Troubleshooting when the message “Login failed for user <user name>” appears in the Web console” on page 919.

-1 value is displayed in a chart for an asset risk score
See “Troubleshooting when -1 value is displayed in a chart for an asset risk score” on page 919.

Message ”Error in reading policy data” appears
See “Troubleshooting when an error message appears while navigating to the Policies page in the Web console” on page 920.

Dashboard panel data is incorrect
See “Troubleshooting when the dashboard panel data is incorrect” on page 920.

Expected data is not displayed in the policy panels
See “Troubleshooting when expected data is not displayed in the policy panels” on page 920.

Launching the Control Compliance Suite Console is slow
See “Troubleshooting when expected data is not displayed in the policy panels” on page 920.

Message "Login failed for user <username>" appears
See “Troubleshooting when an error message appears on the Control Compliance Suite console or in the logs of DPS” on page 921.

Delay in permission changes in the Web Console
See “Troubleshooting when there is a delay in permission changes in the Web Console” on page 922.

Web Console does not start after upgrading to version 10.0
See “Troubleshooting when the Web console does not start after upgrading to version 10.0” on page 922.

### Troubleshooting when the user cannot start the Control Compliance Suite Console

If a user is unable to start the Control Compliance Suite (CCS) Console, one of the following may be the cause:

<table>
<thead>
<tr>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user cannot locate the CCS Console installer.</td>
<td>The installer is hosted on the Application Server in the <code>\Application Server Name\CCS</code> directory.</td>
</tr>
<tr>
<td>The console is unable to contact the Application Server computer by name.</td>
<td>Ensure that the Domain Name Service is properly configured, or use the IP address of the Application Server.</td>
</tr>
<tr>
<td>The console is unable to successfully start.</td>
<td>Verify that the Application Server service account is trusted for delegation.</td>
</tr>
<tr>
<td></td>
<td>Verify that the Service Principal Names are properly registered.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring service accounts with unconstrained delegation” on page 189.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the S4U and constrained delegation” on page 190.</td>
</tr>
</tbody>
</table>
Troubleshooting when the Web Console is unable to connect to the Response Assessment module

The Web Console may be able to connect to the Response Assessment module. If this occurs, one of the following may be the cause:

Web Console is not configured to connect to the Response Assessment module.

Configure the Web Console to connect to the Response Assessment module.

*Note:* You configure the Web Console to connect to the Response Assessment Module when you install the Web Console.

See “About configuring the Web Console to contact RAM” on page 203.

All jobs fail to run.

Verify that the Production database host works properly.

Troubleshooting when the Web Console does not correctly display Response Assessment module pages

The Web Console may not correctly display Response Assessment module pages.

One possible cause for this is that the Internet Explorer Enhanced Security Components are installed and cookies are blocked on the Web Console Internet Information Services (IIS) Manager.

For the Response Assessment module to function correctly, you must allow the Web Console IIS Manager to set cookies.

Troubleshooting when configuration changes do not appear

The Control Compliance Suite (CCS) supports multiple simultaneous users. In certain circumstances, a user can make changes that adversely affect another user. If multiple users simultaneously make changes to the same configuration settings, only the changes made by the first user take effect.

If this happens, the second user should navigate to a different view, then return to the settings page and repeat any required settings changes.

Troubleshooting when the correct time does not appear on reports

When you run a report job, the correct time may not appear on generated reports if the time or locale setting was changed on the Application Server host.

To correct this error, you should do the following:
Troubleshooting when reports cause a system slowdown or reports fail

When a user runs a report job, the reports may cause a system slowdown or reports may fail completely.

This error may be caused when the complexity of the report exceeds the limits of the report engine the Control Compliance Suite (CCS) uses.

If it occurs, the only solution is to reduce the complexity of the report.

Troubleshooting when the error HTTP Error 401.1 - Unauthorized: Access is denied appears when you open the Web Console

The error HTTP Error 401.1 - Unauthorized: Access is denied may appear when you connect to the Web Console.

If this error occurs, the Service Principal Names (SPNs) used by the Web Console may be misconfigured.

To correct the error, you should properly configure the Service Principal Names (SPNs).

See [http://support.microsoft.com/kb/871179](http://support.microsoft.com/kb/871179)

Troubleshooting when blank reports appear

When you run a report, the report contents may not appear. The report appears to be blank.

This error occurs because the Reporting Database Synchronization job must run before you can run a report.

You should run the Reporting Database Synchronization job before you schedule the report. The synchronization job populates the database with the data in the production database. The synchronization job is an existing job and is in the Monitor > Jobs view.
Troubleshooting when an error appears while viewing a dashboard on the Web Console


This error can occur because you have the Service Principal Names (SPNs) set incorrectly on the Control Compliance Suite (CCS) Application Server.

You should use the `<install directory>\Application server\CCSSPNUUtil.exe` utility to verify that the SPNs are set correctly for the Application Server, and that there are no duplicate SPNs set.

Troubleshooting when you cannot create a custom asset type

If you use the **Add new asset type** wizard to create a custom asset type, the custom entity schema may not appear in the wizard. The failure occurs because Control Compliance Suite (CCS) Console is unable to successfully transfer the custom entity schema XML files from the Application Server.

This error can occur if the Application Server has not completed loading the custom entity schema. This error only occurs immediately after the Application Server starts and the service has not completed loading. The error does not appear if you use the Console on the same computer that hosts the Application Server. It does appear if you use the Console on another computer.

You should close the CCS Console and wait until the Application Server completes its startup sequence. The startup sequence takes less than 5 minutes to complete. When the Application Server startup is complete, restart the CCS Console, and the custom entity schema information appears. You can use the **Add new asset type** wizard to create a custom asset type with the custom schema.

Troubleshooting when the message “The server is not operational” appears in the console

When the user performs an action in the Control Compliance Suite (CCS) Console, the error message “The server is not operational” can appear.

This message appears because the CCS components are unable to contact the CCS Directory Server or the CCS Directory Server is busy.

The CCS Administrator can correct the issue. The CCS Administrator should do the following:

- Check the socket connection state on the CCS Directory Server host.
- Change the timeouts for the CCS Directory Server.
- Change the maximum number of socket connections for the CCS Directory Server.

To check the socket connection state on the CCS Directory Server host, you use the `NETSTAT` command from the command line. If one of the sockets is in a waiting state, the command output should be similar to the following:

```
TCP <CCS_Directory_Server_Name>:<Port> TIME_WAIT
```

You should use the Registry Editor to change the value of `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters\TCPTimedWaitDelay` to 35 seconds. If the key is not present, please add it to the registry as REG_DWORD type keys.

You should also use the Registry Editor to change the value of `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters\MaxUserPort` to 65530. This change increases the number of available socket connections on the CCS Directory Server. If the key is not present, please add it to the registry as REG_DWORD type keys.

Once you have completed these changes, you should restart the CCS Directory Server and retry the action in the CCS Console.

**Troubleshooting when the message “Login failed for user <user name>” appears in the Web console**

When you log on to the Control Compliance Suite (CCS) Web Console, the error message “Login failed for user <user name>” may appear. This error appears if the SQL credentials used for the production database or the reporting database change.

If this error occurs, the CCS Administrator should use the Internet Information Services (IIS) Manager to recycle the `CCS_WebAppPool` service on the CCS Web Console server.

See “About logs and configuration files” on page 204.

**Troubleshooting when -1 value is displayed in a chart for an asset risk score**

If you select asset risk score as the **Measure** for a panel, you may see a -1 score in the chart for certain assets.

The -1 score is generated in the following conditions:

- An evaluated asset that does not have any data collected on the checks
An asset with 100% compliance
You can correct the score by adding the following Subject settings:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Asset risk score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>is not equal to</td>
</tr>
<tr>
<td>Values</td>
<td>-1</td>
</tr>
</tbody>
</table>

Troubleshooting when an error message appears while navigating to the Policies page in the Web console

When you navigate to the Policies page in the Web console, the error message "Error in reading policy data" may appear for any of the following reasons:

- SPNs are not configured correctly
- IIS 7 computer is not set for delegation
- HTTP SPN is set on IIS 7 computer that is already configured to be trusted for delegation.
  HTTP SPN is not required on IIS 7 computers as the IIS 7 computers are configured for Kerberos authentication.

Troubleshooting when the dashboard panel data is incorrect

You have created a standard, asset, or policy or you have imported a standard, asset, or policy. You have run the evaluation job. You create a dashboard panel, but the data is not displayed or the data is incorrect.

You must run the Reporting Database Synchronization job in the Control Compliance Suite CCS Console. The job is in the Monitor > Jobs view. The data may not display correctly if the job has not been run.

Troubleshooting when expected data is not displayed in the policy panels

You have created a policy, mapped users, and published the policy. You open a policy panel in Web Console > Dashboards > Panels and you do not see the expected data.

Verify that the following jobs have run:

- Policy and Mandates Metrics Computation
- Reporting Database Synchronization
Daily policies

These jobs are scheduled to run once a day. You can manually start the Policy and Mandates Metrics Computation job and the Reporting Database Synchronization job. The jobs are located in Monitor > Jobs view of the CCS Console.

The daily policies job updates the following information:

- "Not read' audience
- Expiring policies per date
- Maintaining the review or approve by dates
- Mappings in synch with check deletions
- Detecting expired policy asset exceptions

You can start the policies job by resetting the start time. You can set the time in Settings > General > Policies > Run the daily policies job at. If you change the time, the job starts at that time until it is changed.

See “Configuring the policy settings” on page 174.

Troubleshooting when launching the Control Compliance Suite Console is slow

Launching the CCS console can be slow on a Windows 2003 or 2008 server with no Internet connectivity.

Do the following steps to improve the performance:

- Open the Internet Explorer browser on the computer that experiences the performance issue.
- Go to Internet Option and select the Advanced tab.
- Uncheck the box "check for publisher's revocation list".

Once the changes are made, the CCS console opens quickly.

Troubleshooting when an error message appears on the Control Compliance Suite console or in the logs of DPS

When you connect to the reporting database in a user context that has insufficient rights on the reporting database, an error message “Login failed for user <username>” appears on the Control Compliance Suite console or in the logs of the DPS in a reporting role.

To correct this issue, you must do the following
Check if you can connect to the SQL Server from the Application Server and DPS using the same user context

Verify whether the user context used to connect to the reporting database (CSM_Reports) is having the role of db_owner. Else change the user context or add the user context to the role of db_owner in the reporting database.

Troubleshooting when there is a delay in permission changes in the Web Console

When a user's permissions change in an Active Directory group, the user must do the following:

- Wait the default time before the change is disseminated through the system.
- Log off and logon to retrieve the new permissions.

A user sees the permission change in the Web Console dashboards after a default 60-minute delay.

You can add this setting to the web.config file to change the default delay time:

```xml
<add key="DynamicDashboard:GroupMembershipUpdateTimeSpan" value="2"/>
```

The value is measured in minutes. You must use a whole number.

Troubleshooting when the Web console does not start after upgrading to version 10.0

If the Web console does not start after you upgrade to version 10.0 and if the error message `System.Runtime.InteropServices.COMException (0x8007203A): The server is not operational` appears in the Web console logs on the CCS Web server computer, then do the following:

The Control Compliance Suite (CCS) Administrator should use the Internet Information Services (IIS) Manager to recycle the CCS_WebAppPool service on the CCS Web Console server.

See “About logs and configuration files” on page 204.

Policy Module troubleshooting

The following errors can occur when you use the Policy Module:

Cannot assign a reviewer or approver for a policy.

See “Troubleshooting when you cannot assign a reviewer or approver for a policy” on page 923.
Troubleshooting when you cannot assign a reviewer or approver for a policy

When you create a new policy, if no user has been explicitly assigned the Policy Reviewer or Policy Approver role, you cannot assign a reviewer or approver to the policy.

By default no user has been assigned to the Policy Reviewer role or the Policy Approver role. Earlier versions of the Control Compliance Suite (CCS) automatically assigned any users that you assigned to the CCS Administrator role were also assigned to the Policy Reviewer and Policy Approver roles automatically. This automatic assignment no longer occurs.

You must manually assign one or more users to the Policy Reviewer and Policy Approver roles, then assign the users to the policies you create.

Symantec ESM troubleshooting

The following errors can occur in Symantec ESM with Control Compliance Suite:

Cannot classify ESM 6.0 agents as different UNIX computers

See “Troubleshooting when you cannot classify ESM 6.0 agents as different UNIX computers” on page 923.

Troubleshooting when you cannot classify ESM 6.0 agents as different UNIX computers

If your Control Compliance Suite (CCS) deployment uses Symantec Enterprise Security Manager 6.0 as a data source, CCS cannot classify ESM 6.0 agents as different UNIX computers.

You cannot classify due to the changes that are made to the OS details field between ESM 6.0 and ESM 9.0 and later.

To change the way ESM 6.0 uses the OS details field

1. Update the ESM agents with SU 34 or later, then execute the Agent Information module on each ESM 6.0 agent.

2. In CCS 9.0 or later, import all ESM 6.0 Assets.
3 In CCS, create an Update reconciliation rule.
   You should include the “If an asset being imported exists in the asset system” condition. You must also include the “Update the specifying fields of an existing asset with the fields of an asset being imported” action.
   Use the **Only Selected fields** option when you add the update type and select **OS details** in the **Available Fields** list.

4 Update the
   
   ESM.Agent.RegisteredName, ESM.Agent.ESMManager, ESM.Agent.OSVersion, ESM.Agent.Platform, and ESM.Agent.OSDetails fields in the file `<Install directory>\Symantec\CCS\Reporting and analytics\Applications\Data Collectors\ESM\ESMAgentAsset.csv`.

5 Configure the CSV data collector and import the `ESMAgentAsset.csv` file.

---

**Reports troubleshooting**

The following errors can occur during report generation:

**Failed report generation job for an Entitlements Management report**

See “**Troubleshooting a failed report generation job for an Entitlements Management report**” on page 924.

**Performance slowdown in execution of report generation jobs**

See “**Troubleshooting performance slowdown in execution of report generation jobs**” on page 925.

---

**Troubleshooting a failed report generation job for an Entitlements Management report**

When you launch a report generation job for an Entitlements Management report, where data owner is included in the filter, the reporting job fails with the error "An error occurred in ReportDashboardActivity: There are no DPS Load Balancers available for job execution".

**To resolve this issue, you must do the following:**

1 Launch the Edit wizard for the EM report generation job.
2 Save the job without making any changes.
3 Execute the job.
   The EM report generation job runs successfully without any error.
Troubleshooting performance slowdown in execution of report generation jobs

While you run the report generation jobs, it is possible that the performance degrades over a period of time. The performance degradation happens when the report generation jobs fail or are cancelled during previous runs. The temporary data that is generated in the report generation job staging tables is not cleaned up when the report generation jobs fail or are cancelled. This results in performance degradation due to accumulation of data in the temporary staging tables.

Use the CleanStagingTables utility to clean the data in the temporary staging tables. The CleanStagingTables utility is located in the <installdir>\CCS\Reporting and Analytics\Application Server.

Prerequisites to run the CleanStagingTables utility

The prerequisites to run the CleanStagingTables utility are as follows:

■ The Application Server service must be running.
■ No reporting jobs must be running.

Running the CleanStagingTables utility

To run the CleanStagingTables utility

1 Navigate to <installdir>\CCS\Reporting and Analytics\Application Server.
2 Double click the CleanStagingTables utility.
3 The following message is displayed on the console: Ensure no report jobs are running. All the staging tables will be cleaned up. Do you want to continue (Y/N?)
   If you enter N, the utility stops and exits.
   If you enter Y, the console displays the progress of the utility.
   The utility exits after the cleanup of staging tables is complete.

Troubleshooting an error "XML document could not be created because server memory is very low" appears in a reporting database synchronization job

When the error "XML document could not be created because server memory is very low" appears in a reporting database synchronization job, you must change
the settings of the tempdb on the production database (CSM_DB) and the reporting
database (CSM_Reports).

To change the settings of tempdb:

1. Connect to SQL database.
2. Expand Databases > System Databases > tempdb.
3. Right click tempdb and select Properties.
4. Click Files. Set the initial size of tempdb to 1024 MB. The default value for
   Autogrowth is 10% and it is the recommended value.

If the error still persists, then restart the SQL server on the production database
(CSM_DB) and the reporting database (CSM_Reports).

Evidence import troubleshooting

The following error can occur when you import evidence:

Evidence collection job fails to run

See “Troubleshooting when Evidence collection job fails to run” on page 926.

Score contribution from an evidence source is not displayed in the Asset Details
pane

See “Troubleshooting when score contribution from an evidence source is not
displayed in the Asset Details pane” on page 926.

Troubleshooting when Evidence collection job fails to run

When you run the evidence collection job, the job may fail with an error,
“Composite Activity cannot transition to 'closed' status when there are active
child context still exists for child activity.”

This error occurs if asset addition fails due to some reason during evidence import.
To avoid getting the error in subsequent job runs, you have to restart the
application server service after you get this error.

Troubleshooting when score contribution from an evidence source is
not displayed in the Asset Details pane

When you register an evidence source using the ISS API with the score contribution
and calculation enabled, the scores may not be displayed in the Asset Details
pane.
The scores may not be displayed because the asset cache does not get updated with this information. Do the following to update the Asset Details pane:

- Go to the Manage > Extended Evidence Source view.
- Select the evidence source.
- Right click and select Edit Evidence source from the menu.
- Run through the wizard without making any changes.
Evidence import troubleshooting
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Complexity</td>
<td>The attribute that measures the complexity of the attack that is required to exploit the vulnerability. The values are High, Medium, and Low.</td>
</tr>
<tr>
<td>Access Vector</td>
<td>The metric that reflects how the vulnerability is exploited. The values are Local, Adjacent Network, and Network.</td>
</tr>
<tr>
<td>Add Rule</td>
<td>A type of reconciliation rule that is applied on the current assets to add the current asset to a specified location.</td>
</tr>
<tr>
<td>approval period</td>
<td>The subset of the entitlements review period.</td>
</tr>
<tr>
<td>asset group</td>
<td>A collection of assets of one or more types for evaluation and reporting. A user-defined group can be static or dynamic.</td>
</tr>
<tr>
<td>asset reconciliation</td>
<td>The resolution of the existing assets with the newly imported assets in the asset store.</td>
</tr>
<tr>
<td>asset store</td>
<td>The location in the Directory Support Service where all the assets that are discovered and reconciled are stored.</td>
</tr>
<tr>
<td>asset system</td>
<td>The overall CCS system that includes all the assets and the features to manage the assets. The assets include groupings, filters, tags, folders, credentials, and asset authorization.</td>
</tr>
<tr>
<td>asset type</td>
<td>A form of categories that are specific to the supported platforms to gather more specific data for the purpose of monitoring the network.</td>
</tr>
<tr>
<td>asset</td>
<td>A managed object in the system that has value, has an owner, has controlled access, and can have authority. The authority occurs when the asset is a person or a query engine.</td>
</tr>
<tr>
<td>attestation</td>
<td>The reply, the answer, or the additional information that is returned to a questionnaire author.</td>
</tr>
<tr>
<td>attester</td>
<td>The creator and owner of the response.</td>
</tr>
<tr>
<td>audience</td>
<td>The users to whom a policy applies.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The attribute that measures the complexity of the attestation that is required to exploit the vulnerability. The values are Multiple, Single, and None.</td>
</tr>
<tr>
<td>automatic remediation</td>
<td>A process that involves identifying the assets that are not in compliance and selecting a remediation notification method as part of the evaluation job.</td>
</tr>
</tbody>
</table>
Availability Impact
The attribute that measures the effect to availability of a successfully exploited vulnerability. The values are None, Partial, and Complete.

certificate
A file that the cryptographic systems uses as proof of identity. The file contains a user’s name and a public key.

check expression
An expression that is used to compare a property of an asset to a specified data value.

check formula
A formula that is created by using check expressions. Operators connect multiple check expressions to create a single check expression.

check
A statement that tests a condition for an asset, such as a test if passwords have a certain length.

clarification
A user request for additional details about a policy before the user accepts a policy or requests an exception.

compliance score
The percentage value of 0 to 100 that represents the level of adherence to a standard. The score is derived from the technical checks.

Confidentiality Impact
The attribute that measures the effect on confidentiality of a successfully exploited vulnerability. The values are None, Partial, and Complete.

content pack
The prepackaged questionnaire that is based on common standards.

Control Compliance Suite Application Server
The server that is responsible for all job executions, workflow, and schedules.

Control Compliance Suite Console
A GUI component of CCS.

Control Compliance Suite Directory Server
The server that stores the asset data, user rights and preferences, and information about jobs.

Control Compliance Suite Directory
Active Directory Application Mode, a Lightweight Directory Access Protocol (LDAP) directory service. Lets the applications store information in a directory, rather than in a flat file or in a database. ADAM is separate from any Active Directory domains that are deployed on the network. In CCS, ADAM/ADLDS is the Directory Server.

Control Compliance Suite Web Console
A Web-based user interface for creating policy awareness and managing dynamic dashboards.

control point
The data location in the system where the access permissions are granted and approved.

control statement
A single-sentence description of an activity, concept, or requirement called out by a regulation or a best-practice framework. These descriptions are a means of mapping related tasks and requirements between various regulations and best practices.
custom threshold  The threshold type that you use to set threshold conditions specific to a type of evaluation node.
dashboard  The high-level view that provides a summary roll-up of your organization's compliance.
data collector  The CCS component that retrieves information about assets from the network.
data item filter  A file that the cryptographic systems use as proof of identity. The file contains a user's name and a public key.
data location  The location of the CSV file.

**Data Processing Service Collector**  A role of the Data Processing Service. The DPS collector transmits data collection jobs to the data collector and retrieves results when the job is complete.

**Data Processing Service Evaluator**  A role of the Data Processing Service. The DPS evaluator compares data that is collected from the network to specified conditions, then stores the evaluation result for reporting.

**Data Processing Service Load Balancer**  A role of the Data Processing Service. The DPS load balancer distributes data collection jobs to the DPS collectors and to the DPS evaluators on the network.

**Data Processing Service Reporter**  A role of the Data Processing Service. The DPS reporter processes the evaluated data from the DPS data evaluator into the reports and the dashboards that are suitable for users.

**Data Processing Service**  A single service that has multiple roles in CCS. The roles include the DPS Collector, the DPS Evaluator, the DPS Load Balancer, and the DPS Reporter.

**Directory Support Service**  The service that works with the CCS Directory to check user rights on the directory items.

**entitlement**  The permission to access the control point.

**ESM (Enterprise Security Manager)**  An agent-based data collector for CCS.

**evaluation**  The process that is used to test the compliance of an asset with a standard, a section, or a check in the organization.

**evidence database**  The database that stores the proof of compliance with the policies and the checks.

**evidence definition**  A description of the information that is collected from the network that serves as proof of compliance with a particular policy.

**evidence**  The information that is collected from the network that proves that an organization is compliant with the policies that the organization has defined.

**exception request**  A user request for permission to defer compliance with a control statement that is included in a policy. The exception request can include the rationale for the request.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>exception</td>
<td>The temporary permission that allows a user with a valid business reason to violate an organizational policy or a technical standard.</td>
</tr>
<tr>
<td>field expression</td>
<td>An expression that uses an operator to compare a field with a particular value that a user specifies.</td>
</tr>
<tr>
<td>framework</td>
<td>A collection of the policies that define best practices. An organization voluntarily uses the policy best practices.</td>
</tr>
<tr>
<td>gap analysis</td>
<td>The analysis that lets you review how the policies that are defined for an organization match up to a regulation or a framework.</td>
</tr>
<tr>
<td>global threshold</td>
<td>The threshold type that you use to set conditions and then apply those conditions to all the evaluation nodes of the same type.</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>The attribute that measures the effect to integrity of a successfully exploited vulnerability. The values are None, Partial, and Complete.</td>
</tr>
<tr>
<td>job run</td>
<td>A particular instance of a job.</td>
</tr>
<tr>
<td>key field</td>
<td>The field in an evidence definition that lets you filter evidence results.</td>
</tr>
<tr>
<td>live data collection</td>
<td>The ESM configuration option for the site that tells the ESM collector to execute an ESM policy run.</td>
</tr>
<tr>
<td>location</td>
<td>An attribute of an asset. CCS users can create locations to represent geographical locations. Assets are associated with the appropriate location as well as with the services that work with those assets.</td>
</tr>
<tr>
<td>manual remediation</td>
<td>A process that involves identifying the assets that are not in compliance and selecting a remediation notification method from existing evaluation results.</td>
</tr>
<tr>
<td>MOS (Managed Object System)</td>
<td>An abstract representation of the network resources that are managed. A managed object can be a physical entity or a network service.</td>
</tr>
<tr>
<td>MOS schema</td>
<td>The object model that is used to represent network data.</td>
</tr>
<tr>
<td>no threshold (Information only node)</td>
<td>The threshold type that you use to retrieve summary data of evaluation nodes for which no threshold conditions are set.</td>
</tr>
<tr>
<td>object</td>
<td>A type of entity that is contained within the Directory Support Service. These entities include policy, asset, or standard. Objects are always the final level of the tree.</td>
</tr>
<tr>
<td>overall compliance score</td>
<td>The percentage value of 0 to 100 that represents the level of adherence to regulations. The compliance score is derived from the technical checks and the procedural controls.</td>
</tr>
<tr>
<td>policy mapping</td>
<td>The process of matching the policies that an organization defines to the frameworks or the regulations that the organization must comply with.</td>
</tr>
<tr>
<td>policy state</td>
<td>The status of a policy. The different states of a policy are planning, review, use, or retired.</td>
</tr>
</tbody>
</table>
Policy Template
A sample policy that is created by Symantec that can be used to create the custom policies that suit an organization’s needs.

Policy
A set of guidelines that are issued by a company to its employees to keep the company compliant with certain government regulations. The guidelines help to maintain the company’s standards and reputation.

Post Rule
A type of reconciliation rule that is applied on the current assets after the asset becomes a part of the asset store.

Pre Rule
A type of reconciliation rule that is applied on the current assets before the asset becomes a part of the asset store.

Predefined rules
Reconciliation rules that are built in the asset system. The asset system has Add, Pre, and Update types of rules.

Production Database
The database that stores collected data from the data collectors. The DPS evaluator uses the stored data.

Question Type
The question categorization that is based on the method that is used to provide a solution.

Questionnaire Author
The creator and owner of the questionnaire.

Questionnaire
The set of questions that ask for responses from the attester that are created by the questionnaire author. The questionnaire hierarchy contains the questionnaire, the groups, the questions, and the answers.

Reconciliation Rule
A rule that defines a condition and a course of action that is to be taken when an asset is imported into the system. A set of actions is executed when the imported asset satisfies the specified set of conditions.

Regulation
A collection of the policies that define an organization’s compliance with a governmental rule or regulation. Compliance is mandatory, which an outside body imposes.

Remediation
A process that involves identifying the assets that are not in compliance and sending notifications to the appropriate personnel to resolve the issues.

Report Template
A report definition that is used by CCS for generating a report. The user can make a copy of a predefined template to create a new customized template.

Reporting Database
The database that stores the evaluation data. The DPS reporter uses the stored evaluation data.

Retention Age
The time period for retaining the evidence data in the evidence database.

Review Cycle
The time frame during which the data owner must complete the entitlement approval process.

Risk Impact
A check’s risk level that is calculated by computing the total Confidentiality, Integrity, Availability, and Vulnerability settings.
risk rating
An asset’s risk level that is calculated by computing the total Confidentiality, Integrity, Availability, and Vulnerability settings.

risk score
The percentage value of 0 to 100 for an asset that is calculated by computing the total Confidentiality, Integrity, and Availability settings. Risk scores are used to compute the severity of a failure of a particular check for a given asset.

RMS
A data collector that retrieves data from a bv-Control installation.

role
A designation that is based on a collection of predefined tasks that defines what a user is able to do in CCS.

section
A collection of subsections and checks. Sections are used to organize the checks and the subsections into logical groups.

site
A set of assets assigned to one or more Data Processing Services (DPS). Assigning sites to a DPS facilitates load balancing, data collection, data evaluation, and reporting from the assets that are assigned to a site.

standard
A collection of sections that contain checks and subsections. Assets are evaluated against a standard to provide a compliance score.

tag
An attribute that can be attached to an item such as an asset, policy, group, standard, evaluation result, query, or query result. The user can then search by such items as “My SOX assets.” The tag is sometimes referred to as a label.

task
A specific action such as Create a policy or Run an evaluation that the user performs. A collection of predefined tasks defines a role.

threshold check field
Threshold parameters for which the threshold values are set for a node.

tiered dashboard
The hierarchical representation of roll-up data.

trend analysis
An analysis that shows an organization’s frameworks, regulations, and policies information and helps organizations to determine the extent of their policy compliance.

trend
A graphical representation of data that is collected for a dashboard. A trend displays the security assessment posture of the organization over a given period of time.

TSP (Technical Standard Pack)
A collection of checks that can be run by a user to verify compliance with industry security and configuration best practices for various operating systems and applications.

Update Rule
A type of reconciliation rule that is applied on the imported assets to update their properties with the values of the current assets that are newly imported.
access control 95
add rule 310
  conditions and actions 280
alternative approvers 498
Altiris
  asset types 412
  CCS Asset Export Task settings 416
  creating import job 415, 417
  CSV file 419
  importing assets 411
  installing 413
  tasks 414
Analysis view 805
annotations
  adding 128
  deleting 129
application server 32–33
  authentication type 161
  credentials 189
  requirements 46
application server database
  settings 186
approve entitlements 514
architecture 30
asset groups 296
  copying and pasting 377
  creating 369
  dynamic 297
  editing 376
  predefined 297
  static 297
asset import 288
  Altiris 411
  default and supported scope 351
  default data collector 322
  first time 316
  scenarios 321
  scope 349
  specific and common fields for custom asset 338
asset import (continued)
  specific and common fields from CSV data collector 335
  specific and common fields from default collector 332
  specific fields from default data collector 329
  using a CSV file 353
  using csv data collector 324
  using ODBC data collector 325
asset system tasks 375
  asset group tasks 376
  asset tasks 391
global tasks 377
asset type fields
  ESM 238
asset types 235
  common fields 345
  create 446
  custom 274
  extend 451
  predefined 236
  probable 273
assets 233
  active 306
  Altiris 412
  applying tags 392
  asset groups 296
  basic concepts 232
  batch size 121
  count settings 178
  custom asset types 274
  editing 391
  field filters 292
  folder hierarchy 234
  getting started 225
  importing 288
  importing for the first time 319
  importing from Symantec Data Loss Prevention 421
  importing specific and common fields for custom asset 338
assets  (continued)
  importing specific and common fields from CSV
data collector  335
  importing specific and common fields from
default data collector  332
  importing specific fields from default data
collector  329
  manual review  295
  moving  392
  predefined asset types  236
  predefined platforms  235
  primary and secondary  275
  probable asset types  273
  reconciliation  295
  reconciliation rules  276
  removing tags  392
  reviewing manually  367
  risk score from evidence source  817
  site scope  234
  tagging  296
  types  235
  updating  344
audience
  about  688
  selecting  689, 693
audits
  about  178
  event triggers  179
  setting  166
  viewing  180

B
baseline jobs
  deleting  675
baselines
  create  672
best practices  791

C
CCS
documents  52
CCS Asset Export Task
  creating  417
  installing  413
  scheduling  418
  settings  416
CCS custom standard migration utility  597
CCS ESM policy run options
  about  150
  configuring  152
certificate management console  32
  about  86
certificates
  about creating  84
  binding  92
  creating  89
  DLP Connector  427
  encryption levels  85
  managing  81
  removing  94
  renewing  91
  tasks  85
  unbinding  93
Check
  risk attributes  584
check  556
  concepts  579
  copying and pasting  631
  creating  633
  deleting  633
  expression  581
  formula  581
  mapping to control statements  799
  modifying  636
  moving  632
  renaming  632
  version  569
clarifications
  about  706
  management view  707
  managing  706
  managing requests  708
  reviewing  707
client  44
closed-loop verification
  about  664
collector  32, 37
  requirements  46
columns
  heading  69
common fields  345
common platform
  configuring through ODBC settings  328
default data collector  326
fields  326
  predefined asset types  326
create (continued)
  static asset group 372
  tag category 678
  tags 678
create reconciliation rules
  with manual review 307
  without manual review 306
credentials
  scheduled jobs 164
CSV
  defining file format for evidence collection 833
  exporting resources from Altiris 419
CSV file
  importing assets 353
CSV file format
  data collection 357
  list field format 359
  predefined asset types 356
  user account 183
CSV headers
  exporting 393
custom asset
  importing specific and common fields
    information 338
custom content 790, 792
  about 788
  control statements 791, 794
  framework 793–794
  frameworks 790
  mandate 793–794
  mapping checks to control statements 799
  mapping control statements to extended controls 803
  mapping control statements to mandates 795
  mapping policies to control statements 797
  mapping questions to control statements 801
  regulation 793–794
  regulations 790
custom roles
  about 104
  creating 110
  deleting 112
  editing 111
  entity schema 458
custom rules-based actions
  DLP 436
custom schema 446

D
dashboard
  about tiered 756
  descriptions 741
  job settings 175
  threshold settings 175
dashboard reports
  viewing 784
  viewing details report 784
  viewing trends report 785
dashboard section
  copying and pasting 779
dashboards
  types 736
data collection job 556
data collector
  NDS 144
  NetWare 144
  SQL 142
data collectors
  about configuration 138
  default 288
data filter 582
data location
  configuring 165
data owners 498
Data Processing Service
  advanced settings 119
  assigning 137
  configuring 119
  registering 114–115
    minimum configuration 117
  removing 118, 138
  roles 115, 122
  settings 119
  synchronizing
    reporting database 167
  synchronizing settings 122
data processing service 32, 37–41
  collector 32, 40
  evaluator 32, 41
  load balancer 32, 38
  reporter 32, 39
  requirements 46
data synchronization 737
databases
  jobs 741
  reporting
    synchronizing 167
delete
assets or asset groups 393
reconciliation rules 406
tag 680
tag category 679
details pane
about 62
assets 394
control points 525
reconciliation rules 406
directory 35
objects 36
directory server 32
requirements 46
DLP Connector 422
asset mapping 431
configuring 423
custom rules-based actions 436
installing a certificate 427
logging 440
managing controls 440
pre-defined rules-based actions 433
roles and permissions 422
rule-based actions 432
scheduled task configuration 430
status mapping 430
DLP Connector utilities
    Connector Executor utility 442
    Credentials Removal utility 441
DLP Credentials Removal utility
    using 441
DPS 32, 37–41
collector 32, 37, 40
evaluator 32, 37, 41
load balancer 32, 37–38
reporter 32, 37, 39
requirements 46
settings for ESM 155
dynamic asset groups
    creating 370

E
edit
asset group 376
assets 391
category 679
reconciliation rules 405
email address
    updating 184
email notification
    settings 166
encryption management service
    about 82
entitlements
    settings 171
entity
definition in Control Compliance Suite 457
entity schema
    about 445
    creating 461
ESM
    adding, modifying, removing manager 148
documents 53
policy mapping 571
policy name change 572
target types 565
ESM Check Builder
    adding an error expression 642
    adding the data filters 641
    editing check formula 643
    message expression 640
    specifying content 647
ESM checks
    Advanced Check Builder 644
    creating 638
    Quick Check Builder 639
ESM custom policy migration utility 597
ESM policy
    renaming at the check level 637
    renaming at the section level 623
    renaming at the standard level 618
evaluation job 557
    creating 607
evaluation node
    adding 777
bv-Control Query Results 776
copying and pasting 779
deleting 778
editing 778
Standards Evaluation Results 776
evaluator 32, 37, 41
    requirements 46
evidence
    about 832
    about CSV file format 833
    about CSV file format for predefined asset types 839
    about methods to import 815
evidence (continued)
about ODBC mappings 844
calculating compliance score 818
calculating risk score 818
general configuration sequence 819
importing from CSV files 849
importing from ODBC database 849
importing from RAM 850
mapping questionnaires to evidence 851
setting tasks to roles 833
understanding CSV file headers 833
viewing evidence records 853
evidence database 32
requirements 46
evidence source
about 821
adding 822
contributing compliance score for assets 816
contributing risk score for assets 817
deleting 824
editing 824
using sources of controls 821
using sources of evidence 821
exception 530
approving 542
concepts 529
filters 534
modifying 546
requesting 538
states 533
templates 532
validity 531
exception state 533
Deny 546
Expire 546
In Review 545
Request Clarification 545
exceptions
settings 172
export
CSV headers 393
expression
check 581
field 580
Extended Evidence Sources
about 809
view 810
F
field expression 580
fields of an entity
definition in Control Compliance Suite 457
Filter by pane
about 61
assets 402
customizing 67
Evaluation Result view 728
reconciliation rules 407
using 67
filters
asset system 402
entitlement 524
reconciliation rules 407
reports 741
folders
creating 71
deleting 72
moving 72
refreshing 73
renaming 73
special characters 71
framework
viewing 806
frameworks 791
creating custom 793
custom 788, 790, 792
modifying custom 794
G
gap analysis
performing 807
general
settings 165
Grid view
about 126
H
health and status
about 130
refreshing 133
viewing 131
host file 195
I
imports 507
automatic 510
imports (continued)
  configuring 508
  manual 511
infrastructure jobs
  monitoring 133
initial tasks
  configuring 77
integration interfaces 855

J
job run
  about 711
  canceling 722
  deleting 723
jobs
  about 711
  about filters 714
  count settings 177
  creating through jobs view 721
  deleting 718
  editing 717
  refreshing the view 720
  running 719
  scheduling 718
  searching 720
  types 712
jobs view
  about 715

L
layout
  optimize 73
licenses
  about 180
  adding 181
  expiration date 181
  viewing 182
LiveUpdate
  about 192
  enable and schedule 194
  host file 195
  run 196
  staging
    location 195
  using 193
  view 194
load balancer 32, 37–38
requirements 46

logs
  about 204
  DLP Connector 440
  levels 206
  locations 204
  messages 206
M
management service 43
mandate
  creating custom 793
  modifying custom 794
mandates 790
  mapping custom to control statements 795
manual review 295
  reconciling records 368
  viewing records 368
Map view
  about 123
  icons 125
  navigating 124
menu bar
  about 58
monitor view
  about 63
N
notifications
  configuring 520
  entitlements 516
  events 516
  tokens 521
O
objects
  directory 36
  editing 69
  organizing 36
  searching 70
ODBC
  about entity table mapping 160
  configuring the data collector 158
  format of database table names 363
  importing assets from ODBC database tables 362
  importing assets of custom platform 341
  importing assets of predefined platform 341
ODBC data collector
  about 159
operators 590
   check formula 593
   Field expression 591

P
permissions
   about 96
   assigning 109, 113
   removing 113
platform
   definition in Control Compliance Suite 456
policies
   about 683
   about clarifications 706
   approval 699
   approving 690, 703
   audience 688
   changing 690
   clarification 684
   clarifications 690
   clarifications management 707
   control statements 687
   copying 690, 698
   create 684
   creating 690, 693
   deleting 690, 693, 697
   edit 687
   editing 690
   exception 684
   exceptions 690
   frameworks 791
   importing 690, 693, 695
   life-cycle 684
   managing clarification requests 708
   managing clarifications 706
   mapping to control statements 688, 797
   moving 690, 693, 698
   pasting 698
   policy management view 690
   publish 684
   publishing 690, 704
   regulations 790
   renaming 690
   review 684
   reviewing 698, 700–701
   searching 690
   selecting audience 689, 693
   status 685, 687, 703–705
   submitting for approval 699

policies (continued)
   submitting for review 690, 698
   tags 690
   unpublish 684
   unpublishing 690, 705
   versioning 684
   viewing 690
   viewing reviewer comments 702
policy
   custom 597
   settings 174
policy mapping
   ESM 571
post rule 312
   conditions and actions 283
pre rule 309
   conditions and actions 278
preconditions 582
predefined platforms 235
predefined standards 550
   ESM 551
   Oracle 553
   SQL 553
   UNIX 554
   Windows 554
predefined target type
   Exchange 566
   Oracle 564
   SQL 559
   UNIX 560
   Windows 559
production database 32, 41
   requirements 46
   settings 186
purge
   about 168
   job schedule 170
   settings 169

Q
questions
   mapping to control statements 801
quick start 76

R
RAM. See Response Assessment Module
   adding link 201
   adding property 201
RAM (continued)
documents 54
evidence 196
publishing questionnaire 202
reconciliation rules 276
assets being imported 287
copying and pasting 406
creating 306
deleting 406
editing 405
moving 405
predefined 284
types 276
with manual review 307
without manual review 306
reconciliation rules tasks 404
reconciliation rules
existing assets 287
reference information
adding 651
deleting 653
editing 652
regulation
viewing 806
regulations 790
creating custom 793
custom 788, 790, 792
modifying custom 794
relationships
defined between entities 458
remediation
about 661
automatic 667
closed-loop verification 664
manual 665
settings 176
report templates
adding 752
copying 750
creating 737
customizing 750
deleting 753
exporting 753
importing 752, 754
moving 755
predefined 737
prerequisites 738
updating 754
reporter 32, 37, 39
requirements 46
reporting database 32, 41–42
requirements 46
settings 187
synchronizing 167
reports
CCS 731
copying custom 750
creating 746
customizing 173, 751
data synchronization 737
descriptions 741
editing 755
exporting 749
filters 741
job 741
printing 748
refreshing 748
removing 748
scheduling 746
viewing 747
request approval 513
request changes 514
Response Assessment Module. See description of
risk calculations 657
Adjusted base score 658
average risk score 659
base score 658
risk score 659
risk score 569
calculating from evidence 818
roles
about 96
adding user 107
copying 111
Data Processing Service 122
permissions 113
predefined 97
removing user 107
viewing tasks 108
viewing users 108
roles and permissions
configuring 95
DLP Connector 422
rules-based actions
DLP 432
pre-defined 433
S
S4U
  configuring 190
  constrained delegation 190
scheduled jobs
  setting 164
section 556
  copying and pasting 621
  creating 621
  deleting 623
  moving 622
  renaming 623
  version 569
security
  settings 164
service accounts
  configuring 189
  unconstrained delegation 189
setting
  review cycle 498
settings
  Data Processing Service 118–119, 122
  synchronizing Data Processing Service 122
sites
  assigning Data Processing Service 137
  configuring 134
  creating 136
  deleting 137
  modifying name 138
  planning 136
  removing Data Processing Service 138
  use of 134–136
special characters
  credentials 191
SQL 32
  requirements 46
SQL Server 41–42
  settings 185
standard 550
  copying and pasting 603
  creating 603
  custom 597
  deleting 606
  exporting 605
  filters 571
  Importing 605
  moving 604
  predefined 550
  renaming 606
standard (continued)
  version 569
standards
  settings 177
static asset groups
  creating 372
status mapping
  DLP 430
suppressed ESM messages
  collecting 149
System Topology view
  about 123
T
table pane
  about 61
  managing 68
tag category
  creating 678
  deleting 679
  editing 679
tags 677
  creating 678
  deleting 680
  moving 680
  renaming 680
target type 558
taskbar
  about 62
tasks
  about 97
  accessing 66
third-party controls
  editing 831
  importing 830
third-party evidence
  about 832
  about CSV file format for predefined asset types 839
  setting tasks to roles 833
thresholds
  about setting thresholds 772
tiered dashboard
  about check fields 773
  about predefined roles 769
  about relational operators 773
  about status calculation 774
  about threshold types 772
  about thresholds 772
tiered dashboard  (continued)
about trends configuration 781
about types of evaluation nodes 776
assigning permissions 776
configuring email alerts 780
configuring nodes 775
copying 764
copying and pasting node 779
copying section 779
creating 763
editing 764
editing dashboard update job 767
editing job notification 766
editing job schedule 765
evaluation nodes 781
exporting 767
getting started 757
importing 766
managing 756
managing permission 771
pasting section 779
renaming 765
roles and permissions 768
viewing 758
viewing details tab 761
viewing evaluation results tab 762
viewing permissions 770
viewing reports 784
viewing status tab 759
tree pane
about 60
using 70
trends
configuring 781
viewing reports 785
troubleshooting 901

U
unified data model
asset standards views 893
assets views 891
description 891
entitlements views 893
exception views 896
policies views 894
standards views 892
tag views 897
third-party views 897
user views 896

update
assets 344
update rule 311
conditions and actions 281
user account
adding 183
deleting 184
importing 183
updating 185
User Management
view 183
user-defined templates
prerequisites 738
users
about 183
adding role 107
assigning permission 109
removing role 107
viewing roles 108

V
view
comparison results 673
views 63
certificates 82
Grid 126
Home 63
license 181
LiveUpdate 194
Map 123
My Dashboards 734
My Reports 733
refreshing 70
Report Templates 732
Reporting 65
Settings 64
System Topology 123
User Management 183

W
Web Console
requirements 50
Web console
accessing 45
web console 44
web console server 42