Symantec™ ServiceDesk 7.5 User Guide

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.

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo, Altiris, and any Altiris or Symantec trademarks used in the product 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.

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 website 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, DVDs, 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
Technical Support ........................................................................................................ 3

Section 1 Introducing ServiceDesk .............................................................. 21

Chapter 1 Introducing ServiceDesk ........................................................... 23

- About ServiceDesk ......................................................................................... 23
- What you can do with ServiceDesk ............................................................. 24
- How ServiceDesk works ............................................................................ 26
- What's new in this version ........................................................................... 29
- Where to get more information ............................................................... 31

Chapter 2 Understanding ServiceDesk concepts .................................. 35

- Components of ServiceDesk ...................................................................... 35
- How Process IDs work .............................................................................. 37
- About cascading relationships among process tickets .............................. 38
- About configuration items .......................................................................... 39
- About ServiceDesk and the Configuration Management Database (CMDB) .................................................................................. 39
- About ServiceDesk licenses ...................................................................... 40

Chapter 3 Introducing ServiceDesk solution software ....................... 43

- About ServiceDesk solution software ....................................................... 43
- About the ServiceDesk Solution Console page ....................................... 44
- Accessing the ServiceDesk Solution Console page ................................ 44
- Viewing the ServiceDesk changes, incidents, or problems that are associated with a resource .............................................................. 45
Section 2  Working in the Process Manager portal ................................................................. 49

Chapter 4  Introducing the Process Manager portal .............................................................. 51

- About the Process Manager portal .................................................................................. 52
- Logging on to the Process Manager portal ...................................................................... 53
- Default Process Manager portal pages ............................................................................ 54
- Admin page ....................................................................................................................... 57
- Calendar page .................................................................................................................... 57
- Discussions page .............................................................................................................. 58
- Documents page .............................................................................................................. 59
- Home page ....................................................................................................................... 61
- Knowledge Base page ..................................................................................................... 62
- My Task List page ............................................................................................................ 63
- Quick Search page .......................................................................................................... 64
- Reports page ..................................................................................................................... 65
- Submit Request page ....................................................................................................... 66
- Technician Dashboard page ............................................................................................ 67
  - Options for changing the contents of the Technician Dashboard page ......................... 68
- Tickets page ..................................................................................................................... 69
- Workflow page ................................................................................................................ 71

Chapter 5  Managing portal pages ......................................................................................... 73

- Exporting a Process Manager portal page ......................................................................... 73
- Importing a Process Manager portal page ......................................................................... 74
- Rearranging the sequence of Process Manager portal pages ............................................ 74
- Deleting Process Manager portal pages ........................................................................... 75
- Disabling and enabling Process Manager portal pages .................................................... 76

Chapter 6  Customizing the contents of Process Manager portal pages .............................. 79

- About customizing the contents of Process Manager portal pages .................................... 80
- Setting your opening portal page ...................................................................................... 80
- Enabling the customization of a Process Manager portal page ....................................... 81
- Customizing a Process Manager portal page (administrator) .......................................... 82
- Customizing your Process Manager portal pages (non-administrator) ............................. 82
- Options on the Site Actions drop-down list .................................................................... 83
<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Working in the Process View .................................................. 93</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About the Process View page .............................................. 93</td>
</tr>
<tr>
<td></td>
<td>Process View page (Incident Management) ............................... 94</td>
</tr>
<tr>
<td></td>
<td>Process View page (Problem Management) ............................... 98</td>
</tr>
<tr>
<td></td>
<td>Process View page (Change Management) .................................. 101</td>
</tr>
<tr>
<td></td>
<td>About actions and smart tasks on the Process View pages .......... 104</td>
</tr>
<tr>
<td></td>
<td>About Process Type Actions on the Process View pages ............. 106</td>
</tr>
<tr>
<td></td>
<td>Adding Process Type Actions ............................................... 107</td>
</tr>
<tr>
<td></td>
<td>Editing Process Type Actions ............................................... 110</td>
</tr>
<tr>
<td></td>
<td>Deleting Process Type Actions ............................................ 112</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Performing common actions in the Process Manager portal .......... 113</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Setting permissions .................................................................. 113</td>
</tr>
<tr>
<td></td>
<td>Picking a user ....................................................................... 114</td>
</tr>
<tr>
<td></td>
<td>Capturing a screen image ..................................................... 115</td>
</tr>
<tr>
<td></td>
<td>Screen Capture icons ................................................................ 117</td>
</tr>
<tr>
<td></td>
<td>Changing your password ................................................................ 119</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>Active Directory self-service catalog ................................. 121</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About the Active Directory self-service catalog ....................... 121</td>
</tr>
<tr>
<td></td>
<td>Requesting an Active Directory password reset ........................ 121</td>
</tr>
<tr>
<td></td>
<td>Requesting access to an Active Directory network share ........... 123</td>
</tr>
</tbody>
</table>

| Section 3 | Managing incidents ............................................................ 125 |

<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Introducing Incident Management ........................................ 127</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About Incident Management ................................................ 127</td>
</tr>
<tr>
<td></td>
<td>About the Incident Management process ................................ 128</td>
</tr>
<tr>
<td></td>
<td>Incident statuses .................................................................. 131</td>
</tr>
<tr>
<td></td>
<td>Roles in Incident Management ............................................. 132</td>
</tr>
<tr>
<td></td>
<td>Sources of ServiceDesk incidents ....................................... 133</td>
</tr>
</tbody>
</table>
Change Management process: Planned state .................................... 222
Change Management process: Received State .................................. 223
Change Management process: Reviewed state .................................. 224
Change Management process: Closed state ...................................... 225
Actions in the Change Management process states ........................... 226
Configuring Change Management .................................................. 229
Change request rulesets ............................................................... 231
Configuring change request rulesets .............................................. 232
Creating email templates for Change Management .......................... 234
Editing email templates for Change Management ............................. 236
Deleting email templates for Change Management ........................... 239
About the roles in Change Management .......................................... 239

Chapter 20 Submitting change requests ............................ 241
Sources of change requests .......................................................... 241
Requesting a change ................................................................... 242
About change templates .............................................................. 243
Creating a new change template .................................................... 244
Editing a change template ............................................................ 245
Deleting a change template .......................................................... 246
Using a change template .............................................................. 247

Chapter 21 Scheduling and planning changes ........................... 249
Scheduling the implementation of a change plan .............................. 249

Chapter 22 Approving and implementing changes .......................... 253
Initiating a vote on a change ......................................................... 253
  Monitoring a vote on a change ................................................... 254
  Canceling the vote on a change .................................................. 255
Voting on a change (CAB) ............................................................. 255
Approving a change (change manager) ........................................... 256
Closing a change request ticket ..................................................... 257

Section 5 Managing problems ................................................ 259

Chapter 23 Managing problems ................................................. 261
About Problem Management ....................................................... 262
About the Problem Management process ..................................... 263
Problem statuses ........................................................................ 265
Roles in Problem Management .................................................... 266
Sources of problem tickets ........................................................... 266
Email notifications from Problem Management ............................... 267
Process View page for problem tickets ........................................... 267
About discussions in the Problem Management process ..................... 269
Reporting a problem ................................................................. 270
Create Problem page ................................................................ 271
Submit a New Problem page ......................................................... 272
Adding incidents to a problem ticket .............................................. 273
Working a problem ticket ............................................................. 274
Examination and Analysis page ..................................................... 275
Propose Workaround page, Propose a Fix page ................................. 276
Reviewing a proposed fix or workaround ........................................ 277
Submit Change Request page ........................................................ 278
Reworking a problem ticket .......................................................... 279

Section 6 Working with process tickets ........................................... 281

Chapter 24 Performing common ticket actions ............................... 283
About restricting access to open tasks (leasing) ................................ 283
Breaking the lease on a task .......................................................... 284
About the process time for tickets ................................................. 285
Posting process time to a ticket ..................................................... 285
Performing actions on multiple tickets ........................................... 286
Attaching a file to an existing process ticket .................................... 287

Chapter 25 Assigning and delegating process tickets ....................... 289
Reassigning incidents, problems, or change tickets ........................... 289
Edit Assignments dialog box ......................................................... 292
Delegating a user’s tickets to another user ..................................... 293
Deleting a ticket delegation .......................................................... 294
Delegating your tickets to another user .......................................... 295
Add Delegation dialog box ............................................................ 295
Reassigning incident tickets to a service queue ................................. 296

Chapter 26 Managing the ServiceDesk schedule ............................. 299
About scheduling in ServiceDesk ................................................... 299
Viewing the ServiceDesk schedule ................................................. 300
Searching for a schedule entry ..................................................... 301
Creating a new schedule ............................................................. 302
Add Schedule dialog box ............................................................. 302
Adding an entry to the schedule .................................................... 303
Add Entry dialog box ................................................................. 304

**Section 7** Managing your organization’s knowledge ........................................... 305

**Chapter 27** Introducing Knowledge Management ........................................... 307

- About Knowledge Management .............................................. 307
- Types of knowledge base items ....................................................... 309
- About the Bulletin Board .......................................................... 309
- Knowledge base statuses ............................................................. 310
- Email notifications from Knowledge Management ....................... 311
- About permissions in the knowledge base ..................................... 312

**Chapter 28** Processing requests for knowledge base entries .................................. 313

- Processing requests for knowledge base entries ................................. 313
- Roles in Knowledge Management .................................................. 314
- Sources of knowledge base requests and entries ............................... 315
- Submitting a request for a knowledge base entry ............................. 317
- Accepting or rejecting a knowledge base request ........................... 318
- Create KB Article dialog box ...................................................... 319
- Reviewing a knowledge base entry for final resolution .................. 320

**Chapter 29** Managing the knowledge base .......................................................... 325

- About knowledge base categories ............................................. 325
- Adding a knowledge base category or subcategory .......................... 326
- Moving a knowledge base item to a different category ................... 327
- Creating a knowledge base item from the Knowledge Base page ....... 328
- Add Article dialog box ............................................................... 329
- Add Bulletin dialog box .............................................................. 330
- Add FAQ dialog box ................................................................. 332
- Add Wiki dialog box ................................................................. 333
- Adding entries and links to a wiki article ....................................... 335
- Links in wiki articles ................................................................. 336

**Chapter 30** Using the knowledge base ................................................................. 339

- Searching the knowledge base .................................................. 339
- Viewing an item in the knowledge base ......................................... 339
- What you can do with a knowledge base item .............................. 340
Section 8 Managing the documents in ServiceDesk ............................................................. 343

Chapter 31 Adding and managing documents ............................................................. 345

About Document Management ............................................................. 346
About Document Management in the ServiceDesk processes .................... 347
About document categories .................................................................... 347
Adding a document category .................................................................... 348
Adding a document subcategory ............................................................ 348
Category and Sub Category dialog boxes ............................................... 349
Editing a document category .................................................................... 350
Setting permissions for a document category ........................................... 351
Deleting a document category .................................................................... 351
Displaying the history of a document category ......................................... 352
Creating expected document messages ................................................... 353
Expected Documents dialog box ............................................................. 354
Adding a document to the Document Management system ....................... 355
Add Documents dialog box ................................................................. 356
Add Advanced Document dialog box .................................................... 357
Setting permissions for a document ...................................................... 359
Editing document data ........................................................................... 360
Adding a new document version ............................................................ 360
Promoting a document version .............................................................. 361
Adding a document to additional categories .......................................... 362
Deleting a document ............................................................................. 363

Chapter 32 Viewing documents ................................................................. 365

What you can do with ServiceDesk documents ....................................... 365
Searching for documents .......................................................................... 367
Previewing documents ............................................................................. 368
Viewing a document ................................................................................. 368
Downloading a document .......................................................................... 369
Downloading a document in .zip format ................................................... 369
Emailing a document ............................................................................... 369
Viewing a document’s versions ............................................................... 370
Viewing a document’s history ................................................................. 371
Section 9  Communicating in the Process Manager portal .......................................................... 373

Chapter 33  Emailing in the Process Manager portal ................................................................. 375
Sending an email from a ticket's Process View page ......................................................... 375
About automatic email notifications ................................................................................. 377
About process notifications ............................................................................................. 378

Chapter 34  Holding discussions in the Process Manager portal ............................................. 381
About discussions in the Process Manager portal .......................................................... 381
Adding a discussion in the Process Manager portal ....................................................... 382
Adding a thread to a discussion ....................................................................................... 383
Participating in a discussion in the Process Manager portal ........................................... 384

Section 10  Managing reports .................................................................................................. 387

Chapter 35  Viewing and organizing reports ........................................................................ 389
About ServiceDesk reporting ............................................................................................. 390
Viewing a report ................................................................................................................ 390
What you can do with a report .......................................................................................... 391
Displaying reports in print view ....................................................................................... 392
Setting permissions for a report ........................................................................................ 392
Optimizing reports in the Process Manager portal ............................................................ 393
Copying a report ................................................................................................................ 395
Exporting a report definition ............................................................................................. 396
Importing reports ............................................................................................................... 397
Adding reports to a portal page ......................................................................................... 397
Deleting reports .................................................................................................................. 398
About report categories ..................................................................................................... 398
Adding report categories .................................................................................................. 398
Adding report subcategories .............................................................................................. 399
Deleting report categories ................................................................................................. 399
Setting permissions for a report category ......................................................................... 400
Adding reports to additional categories ........................................................................... 401
Importing a report category ............................................................................................... 401
About child reports ............................................................................................................ 402
Chapter 36  Creating and customizing standard reports ........................................... 403
  Creating a standard report ................................................................. 403
  Setting up or modifying the data in standard reports ......................... 404
  Customizing the layout of grid standard reports ................................. 406
  Customizing the filtering and sorting for standard reports ................. 406
  Setting up or modifying Web Service access for standard reports ....... 407
  Add/Edit Standard Report dialog box .................................................. 408
  Modifying standard reports .............................................................. 411

Chapter 37  Scheduling reports ................................................................. 413
  Scheduling automatic report emails .................................................. 413
  Creating a report schedule ............................................................... 414
  New Report Schedule dialog box ....................................................... 414
  Adding a report to a report schedule ................................................. 415
  Options for scheduling reports and events ....................................... 415

Section 11  Setting up and managing ServiceDesk ...................................... 419

Chapter 38  Configuring ServiceDesk ....................................................... 421
  About configuring ServiceDesk ......................................................... 422
  Before you configure ServiceDesk ..................................................... 423
  Configuring ServiceDesk ................................................................. 423
  Additional ServiceDesk configurations .............................................. 428
  About migrating data to ServiceDesk 7.5 ......................................... 430
  Advanced ServiceDesk customizations .............................................. 430
  About the incident priority .............................................................. 432
  Default priority, urgency, and impact values ..................................... 433
  How the incident priority is calculated ............................................. 434
  Creating and Editing Service Level Agreements (SLAs) ...................... 435
  About configuring the Service Level Agreement (SLA) late date ........... 436
  Default SLA levels ........................................................................... 437
  Configuring business hours .............................................................. 438
  About configuring Data Mapping Routing Tables ................................ 440
  About incident types ........................................................................ 440
  Creating and deleting incident types ............................................... 441
  About the Service Catalog and service items .................................... 442
  Migrating data from ServiceDesk 7.1 SP2 ........................................ 442
  Migrating data from ServiceDesk 7.1 SP1 ........................................ 443
  Migrating data from ServiceDesk 7.0 MR2 ...................................... 444
  About migrating data from Helpdesk Solution 6.x ............................ 444
Chapter 39  Managing security, users, roles, groups, and permissions .............................................. 447

About ServiceDesk security and permissions ................................................................. 448
About group-level permissions .................................................................................... 449
About ServiceDesk authentication .............................................................................. 450
About adding users from Active Directory ................................................................. 451
About adding groups from Active Directory ............................................................... 451
Creating a group ........................................................................................................ 452
Add Group dialog box .............................................................................................. 453
Editing a group .......................................................................................................... 454
Deleting a group ......................................................................................................... 454
Adding users to a group ............................................................................................ 455
Adding or removing permissions for groups ............................................................. 456
Copying permissions between groups ........................................................................ 456
Viewing the list of ServiceDesk permissions ............................................................. 457
Viewing the permissions for a group .......................................................................... 457
Creating an organizational unit ................................................................................. 458
Creating a new user .................................................................................................. 458
Add User dialog box: Clone User tab .................................................................... 460
Adding new ServiceDesk users from Active Directory manually ........................... 460
Editing a user account .............................................................................................. 461
Disabling and enabling a user .................................................................................. 462

Chapter 40  Managing the Active Directory connections ........................................ 465

About Active Directory synchronization ....................................................................... 466
Configuring Active Directory sync profiles .................................................................. 467
Managing Active Directory server connections .......................................................... 469
Adding Active Directory server connections ............................................................... 470
Editing the settings of an Active Directory server connection .................................. 473
Deleting an Active Directory server connection .......................................................... 475
Selecting Active Directory as the authentication method .......................................... 475
Testing an Active Directory server connection .......................................................... 476
New AD Connections Profile and Edit AD connection settings dialog boxes ........ 477
Managing Active Directory sync profile schedules ................................................. 478
Adding Active Directory sync profile schedules ...................................................... 479
Editing an Active Directory sync profile schedule ................................................... 481
Deleting an Active Directory sync profile schedule .................................................. 482
Managing Active Directory sync profiles ................................................................. 483
Adding Active Directory sync profiles ...................................................................... 486
Editing an Active Directory sync profile .................................................................. 489
Deleting an Active Directory sync profile ................................................................. 492
Add Active Directory Sync Profiles and Edit Active Directory Sync Profiles dialog boxes ............................................................. 492
Methods for synchronizing Active Directory sync profiles ................. 493
Running a full Active Directory sync profile synchronization manually .................................................................................... 495
Running update Active Directory sync profile synchronization manually ..................................................................................... 496
Synchronizing all Active Directory sync profiles manually ................. 496
Checking the status of an Active Directory sync profile synchronization ................................................................. 497

Chapter 41 Managing categories and the data hierarchy ................. 499
About Incident Management classifications and the data hierarchy ............................................................................................. 499
Adding an incident classification ...................................................... 500
Deleting an incident classification ..................................................... 501
Importing incident classifications ....................................................... 502
Exporting incident classifications ....................................................... 502

Chapter 42 Customizing forms .......................................................... 505
About customizing forms ................................................................. 505
Editing a form in the Process Manager portal .................................. 507
Setting permissions for a form .......................................................... 508
About the Customer Satisfaction Survey ........................................... 508

Chapter 43 Customizing the email in ServiceDesk ......................... 511
Customizing the email actions for ServiceDesk processes ............... 511
About the contents of email notifications .......................................... 512
About configuring the email monitoring .......................................... 513

Chapter 44 Distributing the ServiceDesk documentation ............... 515
Making the ServiceDesk documentation available to users ............... 515
Configuring the Help link for ServiceDesk documentation ............... 517
Linking to the ServiceDesk documentation from a Links Web part ..................................................................................... 517
Displaying the ServiceDesk documentation in a File Browser Web part ..................................................................................... 519
Adding the ServiceDesk documentation to Document Management .............................................................................. 520
Chapter 45  Performing administrative tasks ................................................. 523
  Commands on the Admin menu ............................................................... 523
  About application properties .................................................................. 528
  About incident close codes ................................................................... 528
  Adding and deleting incident close codes ............................................. 529
  About the Process Manager portal master settings ................................ 530
  Editing the Process Manager portal master settings ............................. 530
  Master Settings: Process Manager Active Directory Settings
    section ............................................................................................... 531
  Creating user relationship types .......................................................... 532

Appendix A  Default permissions in ServiceDesk ........................................ 533
  Default ServiceDesk permissions by category ..................................... 533
  Default ServiceDesk user groups ........................................................ 539
    Default permissions for the All Users group ..................................... 541
    Default permissions for the Application Users group ....................... 542
    Default permissions for the Change Approvers group ..................... 544
    Default permissions for the Change Manager group .......................... 545
    Default permissions for the KB Approvers group ............................. 547
    Default permissions for the KB Editors group .................................... 549
    Default permissions for the Problem Analysts group ....................... 550
    Default permissions for the Problem Reviewers group ...................... 552
    Default permissions for the Service Managers group ....................... 554
    Default permissions for the Support group ....................................... 555

Appendix B  Default categories in ServiceDesk .......................................... 559
  Default categories for incidents and default classifications for
    problems ............................................................................................. 559

Appendix C  ServiceDesk reporting data dictionary .................................... 563
  ServiceDesk reporting data dictionary ................................................ 563

Index ......................................................................................................... 581
Introducing ServiceDesk

- Chapter 1. Introducing ServiceDesk
- Chapter 2. Understanding ServiceDesk concepts
- Chapter 3. Introducing ServiceDesk solution software
Introducing ServiceDesk

This chapter includes the following topics:

- About ServiceDesk
- What you can do with ServiceDesk
- How ServiceDesk works
- What’s new in this version
- Where to get more information

About ServiceDesk

Symantec ServiceDesk improves your infrastructure’s service management.

It is ITIL-based and includes all of the primary ITIL Service Management processes. These processes include Incident Management, Problem Management, Change Management, and Knowledge Management. ServiceDesk also includes a Service Catalog that lets your users choose service items. It also includes an Active Directory Self Service Catalog that lets users easily and securely reset passwords and access network shares.

ServiceDesk uses the Symantec Workflow framework to manage service tickets, provide reports, and integrate with the Configuration Management Database (CMDB).

You can configure ServiceDesk to meet your organization’s specific requirements. These configurations include setting up business hours, routing rules for incidents and changes, and email templates and notification rules. You can implement advanced customizations. These customizations may include creating data types, modifying feeder forms, modifying the Process View page, and adding fields to reports.

For more information, see the following:
What you can do with ServiceDesk

ServiceDesk contains several predefined ITIL-based modules for managing your service environment. These modules can help you manage incidents, changes, problems, and knowledge. In addition, ServiceDesk provides a module for managing your Active Directory self-service request. When installing ServiceDesk, you can select which of the modules that you want to implement.

Figure 1-1  ServiceDesk modules

A ServiceDesk module is a collection of workflow processes, administrative interfaces, automation rules, and portal extensions that address a specific business need for your environment. Each ServiceDesk module represents a core process in ServiceDesk. ServiceDesk contains the following modules to help you organize and manage your service environment:
<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Incident Management**| ■ Contains an ITIL-based Incident Management system.  
■ Includes the Incident Management workflow process, a specialized Process View page, and a report pack. It also includes several administrative interfaces for managing related data like service queues and templates.  
■ Provides a process for submitting and resolving incidents.  
■ Lets the users submit incidents and lets the technical support workers respond to and resolve the incidents.  
■ Includes the ability to create, assign, and manage the subtasks that are related to an incident.  
■ Includes an automation library with conditions and actions for use with the Workflow Rules Engine.  
See “About Incident Management” on page 127. |
| **Problem Management** | ■ Contains an ITIL-based Problem Management system.  
■ Includes the Problem Management workflow process, request forms, and reports.  
■ Provides a process for minimizing the effects of incidents and problems.  
■ Lets you track and diagnose problems and publish known errors to help with future resolutions.  
■ Integrates with the Incident Management and Change Management modules.  
See “About Problem Management” on page 262. |
| **Change Management**  | ■ Contains an ITIL-based Change Management system.  
Provides a process for standardizing the methods and procedures for handling changes in the organization to minimize the effect of those changes on services.  
■ Includes the Change Management workflow process, a specialized Process View page, and a report pack. It also includes several administrative interfaces for managing related data like change advisory boards (CABs) and templates  
■ Provides a process for standardizing the methods and procedures for handling changes in the organization to minimize the effect of those changes on services.  
■ Includes the ability to create, assign, and manage the subtasks that are related to a change request.  
■ Includes an automation library with conditions and actions for use with the Workflow Rules Engine.  
See “About Change Management” on page 220. |
### Introducing ServiceDesk

#### How ServiceDesk works

ServiceDesk is a bundling of ITIL-based ServiceDesk core processes that run on the Workflow engine. ServiceDesk helps you manage incidents, changes, problems, knowledge, and Active Directory domains.

See “What you can do with ServiceDesk” on page 24.

ServiceDesk has several key features to help you manage your service environment.

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Knowledge Base Management**          | ■ Provides a process for managing your knowledge base, which includes gathering, analyzing, storing, and sharing knowledge and information within an organization.  
■ Provides a data repository that stores information on incidents, problems, and known errors.  
■ Provides an area to develop your knowledge base that is based on the information that is gathered from incidents and problem resolution.  
■ Improves your efficiency by reducing the need to rediscover knowledge.  
■ Enables an organization to match new incidents against previous incidents and reuse the organization-established solutions and approaches that you collect in the knowledge base.     
See “About Knowledge Management” on page 307. |
| **Active Directory Self Service Catalog** | ■ Contains a collection of self-service request processes for interacting with an Active Directory domain.  
■ Includes the service catalog items for resetting a domain password and requesting access to a network share, along with the processes to support the requests.  
See “About the Active Directory self-service catalog” on page 121. |

See “About ServiceDesk” on page 23.
See “Components of ServiceDesk” on page 35.
See “What’s new in this version” on page 29.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Ready-to-use ITIL-based process modules | ■ All ServiceDesk processes are ITIL-based, which lets you implement an ITIL solution.  
■ ServiceDesk includes a set of high-quality, ITIL-based processes that have undergone extensive testing and development effort. |
| Process-driven forms                | ■ The default forms that ServiceDesk contains are process-driven rather than data-driven.  
■ The user is not shown all of the available information for the form. Instead, the user is only shown what is relevant for the particular point they are at in the process. The user is only shown the information they need to see to move forward with the process.  
■ This narrowing of focus helps ensure that the process is followed correctly, and makes following the processes easier for new users. |
| Time zone support                   | ■ The date and time that appear in tickets, alerts, and emails are displayed in the appropriate time zone for the current user’s location.  
■ This time zone support allows for world-wide support capabilities and supports virtual help desks |
| Business hours support              | ■ Business hours support allows for accurate Service Level Agreement reporting and accurate reporting of average response time and resolution time.  
■ Lets you define the normal business hours for your organization, which accounts for holidays and weekends. |
| Email templates and notifications   | ■ The email notifications, which automation rule sets trigger, keep users aware of changes to ticket status, and allow users to verify that issues are resolved.  
■ In any process, email notifications can be used to notify the contacts that are associated with a ticket, to assign tasks, and to send alerts. |
| Email Monitoring                    | ■ Email Monitoring monitors a specified inbox for all new and all unread emails.  
■ Processes the emails by creating incidents or routing them to the service manager for evaluation.  
■ Lets you set up an inbox for all new and all unread emails.  
See “About configuring the email monitoring” on page 513. |
| Service Level Agreement (SLA)       | ■ Default SLA time frames can be established and applied based on rule sets.  
■ You can define the SLA time frames in ServiceDesk according to your corporate policy.  
See “Creating and Editing Service Level Agreements (SLAs)” on page 435. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automation rules              | ■ Automation rules let you configure any process that includes a service automation library. The rulesets for a process are referred to as the automation library.  
The Incident Management automation library contains 13 default rulesets.  
The Change Management automation library contains eight default rulesets.  
■ You can configure routing and notification rules for specific events within the Incident Management and the Change Management processes.  
■ For example, you use the automation rules to route (assign) incidents. You can create a rule that routes all emergency and high priority incidents to one service queue. You can then create another rule that routes all other lower priority incidents a different service queue. |
| Escalation rules              | ■ Escalation rules can be configured so that escalations are triggered when certain types of events occur.  
■ For example, an escalation might trigger when an incident approaches the Service Level Agreement limitations. An escalation might trigger when a user has not responded to a Change Management approval task. |
| Customer Survey               | ■ Lets the primary contact for an incident complete a Customer Satisfaction Survey to rate the service and the resolution.  
See “About the Customer Satisfaction Survey” on page 508. |
| Advanced reporting mechanisms | ■ Several out-of-the-box reports are provided, both as reports and Dashboards.  
■ A report builder is included to let you create your own reports and Dashboards.  
■ Report templates can be created to let groups and users customize and save their own reports.  
■ Permissions can be used to manage access to reports.  
■ Reports can be defined and scheduled to run periodically.  
■ Reports can be emailed to a distribution list.  
■ Reports can also be published as a Web service to expose report data. |
| Full-featured knowledge management | ■ A full-featured knowledge management solution is included. |
| Security at a granular level  | ■ You can secure processes, forms, and data at the user, group, role, and organizational unit levels. |

See “About ServiceDesk” on page 23.

See “Components of ServiceDesk” on page 35.

See “What’s new in this version” on page 29.
What's new in this version

In the 7.5 release of ServiceDesk, the following new features are introduced:

**Table 1-3** List of new features in ServiceDesk 7.5

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Microsoft SQL Server 2008 and 2012</td>
<td>SQL Server 2008 SP3, SQL Server 2008 R2 SP2, and SQL Server 2012 are now supported.</td>
</tr>
<tr>
<td>New installation utility</td>
<td>The new ServiceDesk installer simplifies the ServiceDesk install. A new wizard guides you through the following steps:</td>
</tr>
</tbody>
</table>
|                                             | ■ Download of the Workflow installation file  
|                                             | ■ Installation of the Workflow Platform  
|                                             | ■ Installation of the ServiceDesk modules                                                                                                   |
| Ability to select which ServiceDesk Modules (processes) to install | The new installer lets you install any or all of the following ServiceDesk processes:                                                  |
|                                             | ■ Change Management  
|                                             | ■ Incident Management  
|                                             | ■ Problem Management  
|                                             | ■ Knowledge Base Management  
|                                             | ■ Active Directory Self Service Catalog                                                                                     |
| Improved ServiceDesk Implementation Guide    | The Symantec™ ServiceDesk 7.5 Implementation Guide includes the following information:                                                   |
|                                             | ■ Planning and preparing for the installation  
|                                             | ■ ServiceDesk scalability and performance tuning  
|                                             | ■ ServiceDesk installation  
|                                             | ■ Advance customizations                                                                                                                 |
|                                             | For more information, see Symantec™ ServiceDesk 7.5 Implementation Guide.                                                                   |
### List of new features in ServiceDesk 7.5 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business hours can be configured from the <strong>Business Hours</strong> page in the Process Manager portal. To access the <strong>Business Hours</strong> page, click <strong>Admin &gt; Data &gt; Business Hours</strong>.</td>
<td>The Administrator can configure business hours within the Process Manager portal.</td>
</tr>
<tr>
<td>SLA Levels, SLA Escalations, and SLA Milestones can be managed from the <strong>Automation Rules</strong> page in the Process Manager portal. To access the <strong>Automation Rules</strong> page, click <strong>Admin &gt; Process Automation</strong>, then expand <strong>Incident Management</strong>, and click <strong>Service Dashboard</strong>.</td>
<td>The Administrator can configure Service Level Agreements (SLAs) within the Process Manager portal.</td>
</tr>
<tr>
<td>Service Level Agreements can be configured for longer time spans.</td>
<td>Improved Service Level Agreement time span selection.</td>
</tr>
<tr>
<td>Data mapping classifications can be used to set up your Routing Table from the <strong>Data Mapping</strong> page in the Process Manager portal. To access the <strong>Data Mapping</strong> page, click <strong>Admin &gt; Process Automation</strong>, then expand <strong>Incident Management</strong>, click <strong>Service Dashboard</strong>, and then click <strong>Manage Data Mapping</strong>.</td>
<td>The Administrator can manage data mapping within the Process Manager portal.</td>
</tr>
<tr>
<td>Features of the new Incident Management process are as follows:  - Expanded the number of out-of-the-box rulesets.  - Incidents are routed to Service Queues instead of users or groups.  - Ability to create email templates for data and process events  - Ability to create routing rules to route emails for data and process events  - Ability to evoke Workflow from an Incident Management ruleset.</td>
<td>New Incident Management process</td>
</tr>
</tbody>
</table>
### Table 1-3 List of new features in ServiceDesk 7.5 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Additions to Change Management process** | Additions to the Change Management process are as follows:  
  ■ Ability to route change request by risk score  
  ■ Ability to create email templates for data and process events  
  ■ Ability to create routing rules to route emails for data and process events  
  ■ Ability to evoke Workflow from a Change Management ruleset |
| **Improved the reopening a closed incident process.** | Improvements to the reopening a closed incident process are as follows:  
  ■ A new ticket is created for the reopened incident.  
  ■ A reference is provided to the original incident.  
  ■ Ability to assign the ticket to a specific worker or service queue |
| **New Web part for the Technicians for viewing SLA Status** | Technicians can view the SLA Status for initial response and resolution in a separate Web part from within the Incident ticket’s Process View page. The Web part is located in the upper right of the Process View page. |
| **New Web part for the Technicians for viewing the user comments separate from the Process History** | Technicians can view the user comments in a separate Web part from within the Incident ticket’s Process View page. The Web part is located on the left side of the page. |
| **Technicians have the ability to change incident details.** | Technician can change incident details, which include the extended classifications, when they work in incident. |

See “About ServiceDesk” on page 23.

### Where to get more information

Use the following documentation resources to learn about and use this product.
### Table 1-4 Documentation resources

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes</td>
<td>Information about new features and important issues.</td>
<td>The Supported Products A-Z page, which is available at the following URL: <a href="http://www.symantec.com/business/support/index?page=products">http://www.symantec.com/business/support/index?page=products</a> Open your product's support page, and then under Common Topics, click Release Notes.</td>
</tr>
</tbody>
</table>
| Implementation Guide | Information about how to install, configure, and implement this product. | - The Documentation Library, which is available in the Symantec Management Console on the Help menu.  
  - The Supported Products A-Z page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products  
  Open your product's support page, and then under Common Topics, click Documentation. |
| User Guide     | Information about how to use this product, including detailed technical information and instructions for performing common tasks. | - The Documentation Library, which is available in the Symantec Management Console on the Help menu.  
  - The Supported Products A-Z page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products  
  Open your product's support page, and then under Common Topics, click Documentation. |
| Help           | Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format. | The Documentation Library, which is available in the Symantec Management Console on the Help menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways:  
  - Click the page and then press the F1 key.  
  - Use the Context command, which is available in the Symantec Management Console on the Help menu. |

In addition to the product documentation, you can use the following resources to learn about Symantec products.
<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledgebase</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>videos, groups, and ideas for users of Symantec products.</td>
<td></td>
</tr>
</tbody>
</table>

Here is the list of links to various groups on Connect:

- Deployment and Imaging
  http://www.symantec.com/connect/groups/deployment-and-imaging
- Discovery and Inventory
  http://www.symantec.com/connect/groups/discovery-and-inventory
- ITMS Administrator
  http://www.secure.symantec.com/connect/groups/itms-administrator
- Mac Management
  http://www.symantec.com/connect/groups/mac-management
- Monitor Solution and Server Health
  http://www.symantec.com/connect/groups/monitor-solution-and-server-health
- Patch Management
  http://www.symantec.com/connect/groups/patch-management
- Reporting
  http://www.symantec.com/connect/groups/reporting
- ServiceDesk
  http://www.symantec.com/connect/groups/symantec-servicedesk
- Software Management
  http://www.symantec.com/connect/groups/software-management
- Workflow
  http://www.symantec.com/connect/ogproduct/symantec-workflow
- Workspace Virtualization and Streaming
  http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming
Introducing ServiceDesk

Where to get more information
Understanding ServiceDesk concepts

This chapter includes the following topics:

- Components of ServiceDesk
- How Process IDs work
- About cascading relationships among process tickets
- About configuration items
- About ServiceDesk and the Configuration Management Database (CMDB)
- About ServiceDesk licenses

Components of ServiceDesk

The components of ServiceDesk combine to let you use ITIL-based processes to manage service tickets and your organization’s knowledge.
## Components of ServiceDesk

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| ServiceDesk solution software | ■ Installed on the Symantec Management Platform computer.  
■ Lets you manage the ServiceDesk licensing.  
See “About ServiceDesk licenses” on page 40.  
■ Contains the installation file that is used to install the Workflow Platform and ServiceDesk modules on the ServiceDesk server computer.  
■ Contains the ServiceDesk pages that appear in the Symantec Management Console.  
In the Symantec Management Console, you can access the ServiceDesk Solution Console page that lets you download the ServiceDesk installation file.  
■ Lets you integrate between the ServiceDesk application software and the Configuration Management Database (CMDB).  
See “About ServiceDesk solution software” on page 43. |
| Workflow Platform          | ■ Incorporates all the Symantec Workflow technologies that manage service tickets and provide reporting capabilities.  
■ Includes the Workflow Server software, Workflow Designer, Process Manager database, and Process Manager portal.  
■ Installed on the ServiceDesk server computer.  
It must not be installed on the same computer as Helpdesk Solution. |
| ServiceDesk modules        | ■ Contain the predefined, ITIL-based processes. These processes let you manage incidents, changes, problems, and knowledge.  
■ Installed on the ServiceDesk server computer.  
After installation, you must configure these processes to meet the needs of your organization.  
See “What you can do with ServiceDesk” on page 24. |
| Workflow Designer          | ■ Tool that is included with the Workflow Platform.  
■ Lets an administrator implement advanced ServiceDesk customizations to better meet the needs of the organization. |
| Process Manager Portal     | ■ A Web-based interface that resides on the ServiceDesk server and provides access to the ServiceDesk processes.  
■ Lets the users access the Process Manager portal from a Web browser to run the ServiceDesk processes.  
See "About the Process Manager portal" on page 52. |
| Workflow Server software   | ■ Includes the workflow extensions that are required to run the ServiceDesk core processes.  
■ Must run on the ServiceDesk server computer. |
Table 2-1 Components of ServiceDesk (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Process Manager database                      | ■ Stores the Process Manager details such as groups, users, and permissions and stores persistent Workflow data.  
■ Must reside on the SQL Server computer.                                                                                                                                                                                                                                          |
| Configuration Management Database (CMDB)      | ■ A repository of the information that is related to all the components or resources of an information system.  
■ In the ITIL context, the CMDB represents the authorized configurations of the significant components (configuration items) of the IT environment.                                                                                                                                 |
|                                               | See “About ServiceDesk and the Configuration Management Database (CMDB)” on page 39.                                                                                                                                                                                                                                                      |
| Configuration item (CI)                       | ■ Component of your organization’s infrastructure that is under the control of Configuration Management.  
■ Can represent hardware, software, or associated documentation.                                                                                                                                                                                                                                                                         |
|                                               | See “About configuration items” on page 39.                                                                                                                                                                                                                                                                                                 |


How Process IDs work

The process ID, sometimes called the incident ID, is a unique, alphanumeric value that is generated when a process is first run. For example, when you create an incident, a process ID is created for that incident. When you create a problem, a process ID is created for that problem. You can search for process IDs. The process IDs let you view all the events and items that are associated with that process.

A process ID’s value is broken up into segments. You can use these segments to identify information about the process and the process ID.

Table 2-2 Segments of the process ID

<table>
<thead>
<tr>
<th>Segment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Represents the process type.</td>
</tr>
<tr>
<td></td>
<td>The prefixes that are used in the process ID are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ CM: Change Management</td>
</tr>
<tr>
<td></td>
<td>■ EM: Email Monitoring</td>
</tr>
<tr>
<td></td>
<td>■ IM: Incident Management</td>
</tr>
<tr>
<td></td>
<td>■ KB: Knowledge Management</td>
</tr>
<tr>
<td></td>
<td>■ PM: Problem Management</td>
</tr>
<tr>
<td></td>
<td>■ SDM: Migrated Incidents from Helpdesk Solution</td>
</tr>
</tbody>
</table>
### Table 2-2  Segments of the process ID (continued)

<table>
<thead>
<tr>
<th>Segment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>A numerical value that is generated automatically and incremented for each subsequent process of the same type. By default, the number is six digits long.</td>
</tr>
<tr>
<td>Task number</td>
<td>A numerical value that is appended to the process ID when a task is created for a specific process. The number is incremented every time the task is worked. For example, a new incident is assigned process ID IM-000009. The first task that is created for the incident is assigned task ID IM-000009-1. After the support technician works the incident, the next task that is created is assigned task ID IM-000009-2.</td>
</tr>
</tbody>
</table>

### About cascading relationships among process tickets

In ServiceDesk, you can associate incidents, problems, and changes, with each other. These relationships are called cascading because when one type of ticket is resolved, a related ticket is closed.

Examples of these relationships are as follows:

- When a specific issue is reported frequently, a support technician or other worker can create a problem ticket to fix the root cause.
- When the problem ticket is reviewed and approved, the problem reviewer creates a change request to initiate the problem correction.
- When the change is completed and verified, the associated problem ticket and its associated incidents are closed.

The tickets for the core process types can have the following relationships:

- **Incident and problem**  
  A support technician or a problem analyst can create a ticket to resolve a systemic problem that is the cause of multiple incidents. When the problem ticket is closed, the associated incidents are closed.

- **Problem and change**  
  When the resolution of a problem requires a fix, the problem reviewer can associate the problem with a change request. When the change is completed and closed, the associated problem is closed.
Incident and change  When the resolution of an incident requires a change, the support technician can associate the incident with a change request. When the change is completed and closed, any associated incidents are closed.

See “About the Incident Management process” on page 128.
See “About the Problem Management process” on page 263.
See “About the Change Management process” on page 221.

About configuration items

A configuration item (CI) is a component of your organization’s infrastructure that is under the control of Configuration Management. A configuration item can represent hardware, software, or associated documentation. For example, configuration items can include services, servers, equipment, network components, desktop and mobile computers, applications, licenses, telecommunication services, and facilities.

When you work a change request, you can associate it with one or more configuration items. ITIL recommends that each change should reference one or more configuration items.

The configuration items are modeled in the Configuration Management Database (CMDB).

See “About ServiceDesk and the Configuration Management Database (CMDB)” on page 39.
See “Components of ServiceDesk” on page 35.

About ServiceDesk and the Configuration Management Database (CMDB)

The Configuration Management Database (CMDB) is a repository of the information that is related to all the components or resources of an information system. In the ITIL context, the CMDB represents the authorized configurations of the significant components (configuration items) of the IT environment. For example, the CMDB can contain information about hardware, software, associated documentation, assets, contracts, and users.

For more information about CMDB Solution 7.1 SP2, see the Altiris™ CMDB Solution 7.1 SP2 User Guide.
The CMDB lets you manage the resources throughout their lifecycle, which helps your organization understand the relationships between these resources and track their configuration.

In the Symantec Management Platform, configuration items are typically referred to as resources.

See “About configuration items” on page 39.

The CMDB is a standard component of the Symantec Management Platform. CMDB Solution, which is a requirement for installing ServiceDesk, provides additional capabilities for managing the data in the CMDB.

For a CMDB implementation to be successful, the CMDB must be able to automatically discover and update information about the organization’s resources. The Symantec Management Platform provides the tools to perform these tasks.

Examples of the resource management tasks that can be performed are as follows:

- Automatically discover resources such as computers and software.
  For example, the Symantec Management Platform can discover the computers in an organization and add them to the CMDB.

- Import resources.

- Create resources manually.

- Create associations between resources.
  For example, associations can be created between users, computers, and departments.

- Create customized actions and rules to manage and manipulate data.

See “Components of ServiceDesk” on page 35.

About ServiceDesk licenses

The ServiceDesk licenses that you purchased determine the number of people who can work in the ServiceDesk portal at one time. A license is consumed when a logged-on user has a ServiceDesk Process View page open to work a ticket for any of the ServiceDesk processes.

The ServiceDesk licensing is IP-based. Therefore, a user can run multiple instances of ServiceDesk on one computer but consume only one license.

When all the licenses are in use, the next user who tries to edit a ticket is denied access until a license becomes available.

A license is released in the following instances:

- When a user closes a Process View page.
Note that it might take a few minutes for the license to become available.

- When a **Process View** page is open and inactive for a certain amount of time, and the Web session times out. IIS settings determine the timeout period.

Certain activities do not consume a license, as follows:

- The user enters and submits a ticket.

- The user is engaged in the ServiceDesk activities that are not related to a ticket. For example, a license is not consumed when the user browses documents or reads a knowledge base article.

- The primary contact has the **Process View** page open for any of the tickets that they submitted.

See “**Components of ServiceDesk**” on page 35.

See “**About ServiceDesk solution software**” on page 43.
Introducing ServiceDesk solution software

This chapter includes the following topics:

- About ServiceDesk solution software
- About the ServiceDesk Solution Console page
- Accessing the ServiceDesk Solution Console page
- Viewing the ServiceDesk changes, incidents, or problems that are associated with a resource

About ServiceDesk solution software

The ServiceDesk solution software is a component of the ServiceDesk product. It is different from the ServiceDesk software, which provides the interface for managing service tickets and performing other service tasks. The ServiceDesk solution software is installed on the Symantec Management Platform and the ServiceDesk software is installed on the ServiceDesk server.

See “Components of ServiceDesk” on page 35.

The ServiceDesk solution software provides the following functions:

- Management of the ServiceDesk licenses
  The Symantec Installation Manager (SIM) installs the ServiceDesk solution software on the Symantec Management Platform and applies the ServiceDesk licenses. The ServiceDesk solution software manages the consumption of the ServiceDesk licenses.
  See “About ServiceDesk licenses” on page 40.
Download of the installation file that is used to install ServiceDesk on the ServiceDesk server.
In the Symantec Management Console, you can access the ServiceDesk Solution Console page that lets you download the ServiceDesk installation file to the ServiceDesk server. The ServiceDesk server is different from the Symantec Management Platform.
On the ServiceDesk Solution Console page, you can also download the Screen Capture Utility Installer.

Creation of ServiceDesk incidents for the specific resources that are defined in the CMDB (Configuration Management Database).

Integration between ServiceDesk and the CMDB.
See “About ServiceDesk and the Configuration Management Database (CMDB)” on page 39.

About the ServiceDesk Solution Console page

The ServiceDesk Solution Console page lets you perform the following tasks:

- View the number of ServiceDesk licenses that are available.
- Download the ServiceDesk installation.
- View all incidents that are associated with a resource and that have been reported from the ServiceDesk server.

The ServiceDesk Solution Console page appears in the Symantec Management Console.

See “Accessing the ServiceDesk Solution Console page” on page 44.

The ServiceDesk solution software is a component of the ServiceDesk product
See “About ServiceDesk solution software” on page 43.

The ServiceDesk solution software lets you view all changes, incidents, or problems that are associated with a resource.

See “Viewing the ServiceDesk changes, incidents, or problems that are associated with a resource” on page 45.

Accessing the ServiceDesk Solution Console page

The ServiceDesk Solution Console page displays your ServiceDesk licenses, lets you download installation files for ServiceDesk, and provides information about incidents.
To access the ServiceDesk Solution Console page

1. In the Symantec Management Console, on the Settings menu, click **All Settings**.
2. In the left pane, expand **Service and Asset Management > ServiceDesk** and then click **ServiceDesk**.

### Viewing the ServiceDesk changes, incidents, or problems that are associated with a resource

The ServiceDesk solution software lets you view all changes, incidents, and problems that are associated with a resource. These changes, incidents, and problems have been reported from the ServiceDesk server. For example, you want to perform a software update on several computers and want to schedule a task or policy to perform this action. You may want to check to see if any changes, incidents, or problems exist that are associated with the computers. If you discover any changes, incidents, or problems, you may want to reschedule the software update for that computer.

An incident is a ServiceDesk ticket that reports an issue with a resource. Incidents can originate from user help calls or emails, support technicians, and external systems. A change is a ServiceDesk ticket that request a change. Change requests can originate when support technicians see a pattern of similar issues or when the resolution of a problem requires a fix or change. A problem is a ServiceDesk ticket that reports known errors or systemic issues within the IT infrastructure. Problems can originate when problem analysts review incidents and find any errors that reoccur frequently or support workers report problems within an incident.

You can also obtain this information about incidents from the ServiceDesk Solution Console page.

See “Accessing the ServiceDesk Solution Console page” on page 44.

To view the ServiceDesk changes, incidents, or problems that are associated with a resource

1. In the Symantec Management Console, on the Manage menu, click **Organizational Views and Groups**.
2. In the left pane, expand **Organizational Views**.
3. Under **Organizational Views**, navigate to and click the organizational group that contains the resource.
4 In the right pane, select the resource, and then in the **Actions** drop-down list, select any of the following options:

- **Show Changes**
  
  Lets you view a report that displays any changes that are associated to the resource.

- **Show Incidents**
  
  Lets you view a report that displays any incidents that are associated to the resource.

- **Show Problems**
  
  Lets you view a report that displays any problems that are associated to the resource.
5 When the resources dialog box opens, review the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the affected resource.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the change, incident, or problem that is associated to the resource.</td>
</tr>
<tr>
<td>ClassGuid</td>
<td>ClassGuid for the change, incident, or problem. Lets you see the classification for the change, incident, problem.</td>
</tr>
<tr>
<td>ChangeID, IncidentID, ProblemID</td>
<td>Change, incident, or problem ticket ID number. For example, when you create an incident for a resource in ServiceDesk, the incident is assigned a ticket number.</td>
</tr>
<tr>
<td>ChangeTitle, IncidentTitle, ProblemTitle</td>
<td>Title of the change, incident, or problem that is associated to the resource.</td>
</tr>
<tr>
<td>URLToChange, URLToIncident, URLToProblem</td>
<td>URL for the change, incident, or problem ticket. Lets you view the change, incident, or problem ticket.</td>
</tr>
<tr>
<td>ChangeCreatedDate, IncidentCreatedDate, ProblemCreatedDate</td>
<td>Date that the change, incident, or problem was created for the resource.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority of the incident or the problem resolution. Priority determines the resolution timeline for the incident or problem.</td>
</tr>
</tbody>
</table>

Note that if your reports were customized, the information in the reports that you see might be different.

6 When you finish viewing the information, you can close the resource dialog box.
Introducing ServiceDesk solution software

Viewing the ServiceDesk changes, incidents, or problems that are associated with a resource
Section 2

Working in the Process Manager portal

- Chapter 4. Introducing the Process Manager portal
- Chapter 5. Managing portal pages
- Chapter 6. Customizing the contents of Process Manager portal pages
- Chapter 7. Working in the Process View
- Chapter 8. Performing common actions in the Process Manager portal
- Chapter 9. Active Directory self-service catalog
Introducing the Process Manager portal

This chapter includes the following topics:

- About the Process Manager portal
- Logging on to the Process Manager portal
- Default Process Manager portal pages
- Admin page
- Calendar page
- Discussions page
- Documents page
- Home page
- Knowledge Base page
- My Task List page
- Quick Search page
- Reports page
- Submit Request page
- Technician Dashboard page
- Tickets page
- Workflow page
About the Process Manager portal

The Process Manager portal is a Web-based interface that provides access to the ServiceDesk software. Personnel who use ServiceDesk access the portal from their Web browsers and use it to run the ServiceDesk core processes and perform other ServiceDesk activities.

Examples of the tasks that users can perform in the Process Manager portal are as follows:

- Administrators can configure settings for the appearance, operation, and management of the portal.
- Users can create incidents and view knowledge sources such as the knowledge base.
- Process workers can work on incidents, create and work on tickets for other processes, contribute articles, and participate in discussions.

When you log on to Process Manager, the permissions that you are granted determine the elements of the portal that are available to you. If you cannot access a particular portal page or other feature, you probably do not have the appropriate permissions.

See “Logging on to the Process Manager portal” on page 53.

<table>
<thead>
<tr>
<th>Table 4-1</th>
<th>Screen elements of the Process Manager portal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Process Manager portal</td>
<td>The browser window that appears when you open Process Manager. To access the Process Manager portal from the ServiceDesk server, double-click the Process Manager shortcut on the desktop. You can also access the Process Manager portal from the Start menu; expand Symantec &gt; Process Manager and click Process Manager.</td>
</tr>
<tr>
<td>Site Actions drop-down list</td>
<td>A drop-down list that can appear at the top of the Process Manager portal window. It appears only when you have permission to edit the current Process Manager portal page.</td>
</tr>
<tr>
<td>Link</td>
<td>The clickable text that appears at the upper right and lower left of the Process Manager portal window. Examples of links are Help, Account, and Logout.</td>
</tr>
<tr>
<td>Tab bar</td>
<td>The horizontal row of tabs that appears near the top of the Process Manager portal window. The pages that appear on the tab bar are root pages.</td>
</tr>
<tr>
<td>Tab</td>
<td>A clickable segment of the tab bar. Clicking a tab opens a page or displays one or more menu commands.</td>
</tr>
</tbody>
</table>
Table 4-1 Screen elements of the Process Manager portal (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu bar</td>
<td>The horizontal row of menu commands that appears beneath the tab bar. The contents of the menu bar depend on the tab that you click. Some tabs do not have a menu because they perform a single action. The pages that appear on the menu bar are subpages. Whenever you log on to the Process Manager portal, the portal opens to a specific page. Initially, your permissions determine which page opens. However, you can set a different page to open when you log on. See “Logging on to the Process Manager portal” on page 53.</td>
</tr>
<tr>
<td>Menu command</td>
<td>A clickable segment of the menu bar. Clicking a menu command opens a page or displays one or more menu subcommands.</td>
</tr>
<tr>
<td>Page or portal page</td>
<td>The entire area that appears beneath the menu bar when you click a tab or a menu command. Most of the work in ServiceDesk is performed on a portal page or on a page that is accessed from a portal page. You can customize portal pages for the entire organization or for users, groups, permissions, or organizational units. Administrators have permission to customize portal pages and to grant customization permissions to other ServiceDesk users. See “About customizing the contents of Process Manager portal pages” on page 80.</td>
</tr>
<tr>
<td>Section or Web part</td>
<td>The segments that appear on a Process Manager portal page in the form of Web parts that let you perform actions or enter data. You can customize a portal page by adding, editing, or deleting one or more Web parts. See “Adding a Web part to a Process Manager portal page” on page 85. See “Editing or deleting a Web part on a Process Manager portal page” on page 86.</td>
</tr>
</tbody>
</table>

Logging on to the Process Manager portal

The Process Manager portal is a Web-based interface that lets users submit incidents and lets ServiceDesk workers perform their service-related work. See “About the Process Manager portal” on page 52.

During the setup of the Process Manager portal, each user is assigned a user name and initial password. We recommend that you change your password after you log on to the portal for the first time. See “Changing your password” on page 119.
The permissions that you are granted control all aspects of your use of the Process Manager portal. Your permissions determine which parts of the portal that you can access and what you can do in each part.

If you cannot see or work in a particular feature, you probably do not have the appropriate permissions. Your ServiceDesk administrator can help you with any permissions issues.

When you log on to the Process Manager portal, the portal opens to a specific page. Initially, your permissions determine which page opens. However, you can set a different page to open when you log on.

See “Setting your opening portal page” on page 80.

To log on to the Process Manager portal

1. Open your Web browser.
2. In the Address bar, type the URL that has been provided for your Process Manager portal, as in the following example:
   
   http://ServiceDesk/ProcessManager

3. On the Login page, type your Email Address or Username and Password.
4. (Optional) Check Remember for Autologin.
   
   This option creates a cookie on your local computer, which automatically logs you on to the Process Manager portal. The cookie expires in one year.
5. Click Login.

Default Process Manager portal pages

The Process Manager portal contains a series of default portal pages. The role-based permissions that you have been granted determine the portal pages and actions that are available to you. If you cannot access a particular portal page or feature, you probably do not have the appropriate permissions.

See “About the Process Manager portal” on page 52.

You can perform all of the ServiceDesk functions on the default pages, which are ready to use. However, you might want to customize the pages or add new pages to meet your organization’s specific requirements.

See “About customizing the contents of Process Manager portal pages” on page 80.

If any page was customized, its appearance and contents might differ from the default page. Your Process Manager portal might contain pages other than or in addition to the default pages.
### Table 4-2  Default Process Manager portal pages

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin</strong> pages</td>
<td>Let the administrator configure settings for the Process Manager portal.</td>
</tr>
<tr>
<td></td>
<td>To access a specific Admin page, select its menu command in the Admin tab.</td>
</tr>
<tr>
<td></td>
<td>See “Commands on the Admin menu” on page 523.</td>
</tr>
<tr>
<td>Calendar</td>
<td>Lets the change manager plan changes and releases that coordinate with the existing schedule.</td>
</tr>
<tr>
<td></td>
<td>It also lets users view the scheduled changes that might affect them.</td>
</tr>
<tr>
<td></td>
<td>See “Calendar page” on page 57.</td>
</tr>
<tr>
<td>Documents Category View</td>
<td>Lets you view, download, email, and perform other actions with documents in the document management system.</td>
</tr>
<tr>
<td></td>
<td>Your permissions determine which documents you can view and what actions you can take with those documents.</td>
</tr>
<tr>
<td></td>
<td>See “Documents page” on page 59.</td>
</tr>
<tr>
<td>Home</td>
<td>Serves as the primary workspace for viewing the tickets that you submitted and performing other general ServiceDesk activities.</td>
</tr>
<tr>
<td></td>
<td>See “Home page” on page 61.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>Lets you view and manage knowledge base items.</td>
</tr>
<tr>
<td></td>
<td>You can edit existing items and you can add new items outside of the normal knowledge base process.</td>
</tr>
<tr>
<td></td>
<td>See “Knowledge Base page” on page 62.</td>
</tr>
<tr>
<td>Knowledge Base subpage</td>
<td>Lets you start, view, and participate in discussions.</td>
</tr>
<tr>
<td>Discussion</td>
<td>See “Discussions page” on page 58.</td>
</tr>
<tr>
<td>Knowledge Base Schedules</td>
<td>Lets you view the Calendar page.</td>
</tr>
<tr>
<td>Schedules menu command</td>
<td>See “Calendar page” on page 57.</td>
</tr>
<tr>
<td>My Task List</td>
<td>Lets you view and work on the tasks that are assigned to you.</td>
</tr>
<tr>
<td></td>
<td>The My Task List page is the primary workspace for working on your tasks.</td>
</tr>
<tr>
<td></td>
<td>See “My Task List page” on page 63.</td>
</tr>
<tr>
<td>Quick Search</td>
<td>Lets you search for incidents using the Incident Management Quick Search report.</td>
</tr>
<tr>
<td></td>
<td>See “Quick Search page” on page 64.</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Reports            | Lets you view, create, delete, copy, email, and perform other actions with reports in ServiceDesk.  
See “Reports page” on page 65.                                                                                                                                                                                                                                                                                                                                                                              |
| Submit Request     | Lets you submit tickets and perform other self-service actions. For example, a user can submit an incident and a support technician can submit a change request.  
Lets you perform administrative actions such as managing service queues and manage cabs.  
See “Submit Request page” on page 66.                                                                                                                                                                                                                                                                                                              |
| Technician Dashboard| Provides an example of how you might set up your Technician Dashboard page.  
You can use this page to provide a high-level, graphical view of the number and status of incidents, changes, and problems. Support technicians can then use this information to spot trends and potential problems in the resolution of incidents.  
You can select which reports appear on this page. Reports are actionable, which provides more value than a view of the state of the environment.  
For example, if a Web part contains a report in the form of a graph, you can click the graph to open a report view. You can also drill down to the items in the report.  
For example, if a Web part lists tasks, you can open a task and work it.  
You can also add custom Web parts to start processes, take further action, or help you perform other tasks.  
See “Technician Dashboard page” on page 67.                                                                                                                                                                                                                                                                                                      |
| Tickets            | Displays the current tickets. By default, it lists the tickets that are assigned to you but it can also display other tickets. You can work tickets from this page.  
See “Tickets page” on page 69.                                                                                                                                                                                                                                                                                                                                                                             |
| Workflow           | The Workflow page provides administrators and managers with a comprehensive view of the current tasks and processes.  
The Workflow page has the following views:  
- **Workflow Task List**  
  Lists all the tasks that are assigned to you.  
- **Workflow Process List**  
  Lists all the active processes and their associated tickets. The processes are arranged in workflow category order.  
See “Workflow page” on page 71.                                                                                                                                                                                                                                                                                  |
Admin page

The Admin page lets you access all the administrative functions that are available in ServiceDesk. Only administrators or other users with the appropriate permissions can access the options on the Admin page.

See “Commands on the Admin menu” on page 523.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

Calendar page

The Calendar page lets managers plan changes and releases that coordinate with the existing schedule.

By considering the entire schedule, the managers can avoid unforeseen schedule conflicts. It also lets users view the scheduled changes that might affect them.

See “About scheduling in ServiceDesk” on page 299.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Board</td>
<td>Lets you view the scrolling Bulletin Board messages that have been posted. By default, the Bulletin Board is set to hide if there are no messages. For example, the message can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public, or they can be restricted to specific users, groups, permissions, or organizational units. See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>Schedules</td>
<td>Lists the all the schedules that have been defined. You can add, edit, and delete schedules, and you can select the schedules that appear on the Schedule Entries calendar. See “Creating a new schedule” on page 302.</td>
</tr>
</tbody>
</table>
Table 4-3  Default sections on the Calendar page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Catalog</td>
<td>Lets you view and use the services in the Service Catalog for which you have permission. The service</td>
</tr>
<tr>
<td></td>
<td>items are organized in categories in a tree view. You can click the service item name to perform</td>
</tr>
<tr>
<td></td>
<td>the action. See “About the Service Catalog and service items” on page 442.</td>
</tr>
<tr>
<td>Schedule Entries</td>
<td>Displays the calendar. The monthly view is the default. This section also displays the results of a</td>
</tr>
<tr>
<td></td>
<td>schedule entry search.</td>
</tr>
</tbody>
</table>

See “Viewing the ServiceDesk schedule” on page 300.

Discussions page

The Discussions page in the Process Manager portal lets you start, view, and participate in discussions. The Discussions page displays the discussions that you have permission to view, and lets you expand the discussion posts.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

Table 4-4  Default options on the Discussions page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Opens a drop-down list of options that let you edit or delete the selected discussion item. The</td>
</tr>
<tr>
<td></td>
<td>option to delete is not available if the item has one or more posts or responses.</td>
</tr>
<tr>
<td>Delete</td>
<td>Appears on the Actions drop-down list and lets you delete the selected discussion item. This option</td>
</tr>
<tr>
<td></td>
<td>is not available if the item has one or more posts or responses. However, you can still delete the</td>
</tr>
<tr>
<td></td>
<td>thread or the main discussion. First, you must delete the lowest level of the discussion, and then</td>
</tr>
<tr>
<td></td>
<td>work backwards to the highest level. By deleting this information, you also delete the posting</td>
</tr>
<tr>
<td></td>
<td>history.</td>
</tr>
<tr>
<td>Add Discussion</td>
<td>The location of this symbol determines its action as follows:</td>
</tr>
<tr>
<td>Add Thread</td>
<td></td>
</tr>
<tr>
<td>Add Post</td>
<td></td>
</tr>
</tbody>
</table>
Table 4-4  Default options on the **Discussions** page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Symbol]</td>
<td>The location of this symbol determines its action as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Edit Discussion Info</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Edit Thread Info</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Edit Thread Item</strong></td>
</tr>
<tr>
<td><strong>Search</strong></td>
<td>Lets you type the search text. The search results display any discussions</td>
</tr>
<tr>
<td></td>
<td>whose posts contain the search text.</td>
</tr>
<tr>
<td><strong>Show Discussions Rated</strong></td>
<td>Lets you filter the list of discussions that appears. The users who read the discussion posts can provide the ratings.</td>
</tr>
<tr>
<td><strong>Reply</strong></td>
<td>Opens the <strong>Reply</strong> dialog box, where you can type and save a reply to the</td>
</tr>
<tr>
<td></td>
<td>selected discussion item.</td>
</tr>
</tbody>
</table>

---

**Documents page**

The **Documents** page in the Process Manager portal lets you view, download, email, and perform other actions with documents in the Document Management system. Your permissions determine which documents you can view and what actions you can take with those documents. For example, you might have permissions to view certain documents, but not to delete or edit the document data for those documents.

Any documents that are added to incidents, changes, problems, and releases are automatically saved in the Document Management system. They are saved to hidden folders, which the administrator can access. They are organized in process order and then in ID order.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.
### Table 4-5  Default sections on the **Documents** page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Board</td>
<td>Lets you view the scrolling Bulletin Board messages. By default, the Bulletin Board is set to hide if there are no messages. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, or organizations. See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>Search Documents</td>
<td>Lets you search the Document Management system for documents. This search is conducted on the document name only. See “Searching for documents” on page 367.</td>
</tr>
<tr>
<td>Browse</td>
<td>Lets you select the category for which to display the documents. You can display folders for the categories that are designated as hidden by checking Show hidden folders. You can also create a new document category. See “Adding a document category” on page 348.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Lets you perform a more advanced search in the Document Management system by specifying different areas to search. This search is conducted on keywords.</td>
</tr>
<tr>
<td>Service Catalog</td>
<td>Lets you view and use the services in the Service Catalog for which you have permission. The service items are organized in categories in a tree view. You can click the service item name to perform the action. See “About the Service Catalog and service items” on page 442.</td>
</tr>
<tr>
<td>Tag Cloud</td>
<td>Lets you search for knowledge base items by their tags. When you add a document, you can add tags to the document. The tags are displayed in the Tag Cloud section along with the number of documents that have that tag.</td>
</tr>
<tr>
<td>Documents</td>
<td>Displays the documents that are in the category that you selected under <strong>Browse</strong>. Your permissions determine the documents that appear. You can open and view a document and perform several actions on the document. See “Viewing a document” on page 368. See “What you can do with ServiceDesk documents” on page 365.</td>
</tr>
</tbody>
</table>
The **Home** page is the primary workspace for viewing the tickets that you submitted and performing other general ServiceDesk activities.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

### Table 4-6 Default sections on the **Home** page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Board</td>
<td>Lets you view the scrolling Bulletin Board messages that have been posted. By default, the Bulletin Board is set to hide if there are no messages. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>Search KB</td>
<td>Lets you search the knowledge base for articles. See “Searching the knowledge base” on page 339.</td>
</tr>
</tbody>
</table>
| My Requests   | Lets you see the **My Request** report. This report displays every request that you created along with its ticket number, name, age, percent complete, and status. You can select a ticket number to display the ticket’s **Process View** page.  

See “About the Process View page” on page 93.

Initially, the page displays the **My Request** default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the **Report Settings** option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report. 

See “Options for customizing a Process Manager portal page list” on page 89. 

See “Changing the report for a Process Manager portal page list” on page 91. |
Knowledge Base page

The Knowledge Base page lets you view and manage knowledge base items. You can edit existing items and you can add new items outside the normal knowledge base process.

The Knowledge Base page appears by default when you click the Knowledge Base tab.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

Table 4-7 Default sections on the Knowledge Base page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Board</td>
<td>Lets you view the scrolling Bulletin Board messages that have been posted. By default, the Bulletin Board is set to hide if there are no messages. For example, the message can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public, or they can be restricted to specific users, groups, permissions, or organizational units. See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>Search Articles</td>
<td>Lets you search for knowledge base items. The body text of the items is searched for the search text that you enter.</td>
</tr>
<tr>
<td>Article Category List</td>
<td>Lets you select the category for which to display knowledge base items. You can include the items that are designated as obsolete by checking Show Obsolete Articles. You can also create a new knowledge base category. See “Adding a knowledge base category or subcategory” on page 326.</td>
</tr>
<tr>
<td>Service Catalog</td>
<td>Lets you view and use the services in the Service Catalog for which you have permission. The service items are organized in categories in a tree view. You can click the service item name to perform the action. See “About the Service Catalog and service items” on page 442.</td>
</tr>
<tr>
<td>Tag Cloud</td>
<td>Lets you search for knowledge base items by their tags. When you add an article, wiki, bulletin board, or FAQ to the knowledge base, you can add tags to the item. The tags are displayed in the Tag Cloud section along with the number of items that have that tag.</td>
</tr>
</tbody>
</table>
Table 4-7  Default sections on the Knowledge Base page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Articles</td>
<td>Displays the articles that are in the category that you selected under Categories. Your permissions determine the articles that appear and what you can do with them. See “What you can do with a knowledge base item” on page 340.</td>
</tr>
</tbody>
</table>

My Task List page

The My Task List page lets you view and work on the tasks that are assigned to you. The My Task List page is the primary workspace for working on your tasks.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

Table 4-8  Default sections on the My Task List page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Board</td>
<td>Lets you view the scrolling Bulletin Board messages that have been posted. By default, the Bulletin Board is set to hide if there are no messages. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>Recent Items</td>
<td>Displays the items that you recently viewed, opened, or worked on. You can select a recent item to open it. By default, the last 10 items are displayed. If you want to change the number of items, click Show Options. In the Max Recent Items Count field, change the number of items and click Apply. You can bookmark an item that is important to you. If you click the star symbol next to an item, that item is locked to the list even if 10 newer items exist.</td>
</tr>
</tbody>
</table>
Table 4-8  Default sections on the My Task List page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find Task</td>
<td>Lets you find a task by specifying its task number.</td>
</tr>
<tr>
<td></td>
<td>You can view only the tasks for which you have the appropriate permissions.</td>
</tr>
<tr>
<td>Find Ticket</td>
<td>Lets you find a ticket by specifying its Process ID.</td>
</tr>
<tr>
<td></td>
<td>You can view only the tasks for which you have the appropriate permissions.</td>
</tr>
<tr>
<td>Tasks Viewer</td>
<td>Lets you see the Open Processes Grouped By Project Have Current Tasks Assigned To Me report. This report displays the tasks that are assigned to you.</td>
</tr>
<tr>
<td></td>
<td>You can select a task number to display the task’s Process View page. If you have tasks in multiple processes, you must expand the appropriate process heading for the task that you want to work with.</td>
</tr>
<tr>
<td></td>
<td>See “About the Process View page” on page 93.</td>
</tr>
<tr>
<td></td>
<td>Initially, the page displays the Open Processes Grouped By Project Have Current Tasks Assigned To Me default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the Report Settings option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing a Process Manager portal page list” on page 88.</td>
</tr>
<tr>
<td></td>
<td>See “Changing the report for a Process Manager portal page list” on page 91.</td>
</tr>
</tbody>
</table>

**Quick Search page**

The QuickSearch page lets you view and search the Incident Management Quick Search report. The Incident Management Quick Search report is the default report for this portal page.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.
### Table 4-9  Default sections on the Quick Search page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Settings Incidents</td>
<td>The links under Incidents let you select how you want to search for incidents in the Incident Management Quick Search report. For example, you want to search for incidents by priority. Click Priority is any. In the Priority dialog box, select the priority, and then click OK. The Incident Management Quick Search report now displays only the incidents with that priority. To reset the Incident Management Quick Search report so that you can view all the incidents, click Priority is any. In the Priority dialog box, check Any, and then click OK. The Incident Management Quick Search report now displays all incidents again.</td>
</tr>
<tr>
<td>Report Settings Process Management</td>
<td>The links under Process Management let you search for incidents in the Incident Management Quick Search report by permissions or by the report process ID.</td>
</tr>
<tr>
<td>Incident Management Quick Search report</td>
<td>Displays all incidents that have been submitted. You can select a ticket number to display the ticket’s ProcessView page.</td>
</tr>
</tbody>
</table>

### Reports page

The **Reports** page lets you view, create, delete, copy, email, and perform other actions with reports in ServiceDesk. Your permissions determine which reports you can view, and what actions you can take with those reports. For example, you might have permission to view certain reports, but not to delete those reports or edit the report definitions.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

### Table 4-10  Default sections on the Reports page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Search</td>
<td>Lets you search for a specific report. This search is conducted on the report name and the results are shown from all categories.</td>
</tr>
<tr>
<td>Report Categories</td>
<td>Lets you select the category for which to display the reports. You can also import a report category to the list from another ServiceDesk instance, and you can add a new report category. See “Adding report categories” on page 398. See &quot;Importing a report category&quot; on page 401.</td>
</tr>
</tbody>
</table>
### Table 4-10  Default sections on the Reports page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Templates</td>
<td>Lets you create a new report from a predefined template. You can also edit, export, and delete a report template.</td>
</tr>
<tr>
<td>Reports</td>
<td>Displays the reports that are in the category that you selected under Report Categories. Your permissions determine the reports that appear. You can select a report to view or select any of several report actions. For example, you can edit, print, and export a report. You can also add a new report.</td>
</tr>
</tbody>
</table>

### Submit Request page

The Submit Request page in the Process Manager portal lets you submit tickets and perform other self-service actions. This page also lets you perform administrative actions such as managing service queues and manage cabs. The service items that are available depend on your permissions. For example, a user can submit an incident and a support technician can submit a change request.

A service item is a repeatable self-service action that performs a common task. The default service items represent common ServiceDesk actions. For example, the actions to submit an incident or to submit a request for a knowledge base article are default service items.

You can create custom service items. For example, you might use a service item to request new equipment or to perform a self-service fix for an incident that you submitted.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

### Table 4-11  Default sections on the Submit Request page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Service Item</td>
<td>Lets you search for a specific service item by Title or Description.</td>
</tr>
</tbody>
</table>
Table 4-11  Default sections on the Submit Request page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Catalog</td>
<td>Lets you view and use the services in the Service Catalog that you have permission for. The service items are categorized in folders.</td>
</tr>
<tr>
<td></td>
<td>See “About the Service Catalog and service items” on page 442.</td>
</tr>
<tr>
<td></td>
<td>When you select a folder, the service items in that category appear at the right of the portal page. You can click the service item name to perform the action.</td>
</tr>
<tr>
<td></td>
<td>You can hide the description that appears under each service item by checking the Hide Description check box in this section.</td>
</tr>
<tr>
<td>New Request (right side)</td>
<td>Displays the service items for the folder that you selected under Service Catalog. The service items that are available depend on your permissions.</td>
</tr>
</tbody>
</table>

Technician Dashboard page

The Technician Dashboard page provides an example of how you might set up your Technician Dashboard page. You can use this page to provide a high-level, graphical view of the number and status of incidents in the organization. Support technicians can use this information to spot trends and potential problems in the resolution of incidents.

You can refine or change the contents of any of the data sections for this viewing session. These changes are lost when you click away from the Technician Dashboard page.

See “Options for changing the contents of the Technician Dashboard page” on page 68.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

The contents of the Technician Dashboard page can be customized permanently to display the information that is most useful to your technicians. For example, a section can be edited to display a different report or other sections can be added, deleted, or moved.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.
**Table 4-12** Default sections on the **Technician Dashboard** page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes Scheduled This Month</td>
<td>Displays the <strong>Changes Scheduled This Month</strong> report. This report displays the number of changes that are scheduled this month. You can select change ticket to open.</td>
</tr>
<tr>
<td>Open Change Tickets by Status</td>
<td>Displays the <strong>List Open Change Tickets by Status</strong> report. This report displays the number of open change tickets by status. You can select a change ticket to open.</td>
</tr>
<tr>
<td>Open Incidents by Queue</td>
<td>Displays the <strong>List Open Incidents by Queue</strong> report. This report displays the number of open incidents for each queue. You can expand each queue to view the individual incidents, and you can select an incident ticket to open.</td>
</tr>
<tr>
<td>Incidents This Month by Status</td>
<td>Displays the <strong>List Open Incidents This Month by Status</strong> report. This report displays the number of incidents that have been submitted this month by status. You can select an incident ticket to open.</td>
</tr>
<tr>
<td>Problems By Location</td>
<td>Displays the <strong>List Open Problems by Location</strong> report. This report displays the number of open incidents for each location. You can expand each location group to view the individual incidents, and you can select an incident to open.</td>
</tr>
</tbody>
</table>

**Options for changing the contents of the Technician Dashboard page**

The **Technician Dashboard** page, lets you refine, change, or perform actions on the page contents.

On the **Technician Dashboard** page, within each data section (Web part), you can perform the following actions:

- Edit the **Report Settings** to change the date range, number of records, or other criteria.
- Select a different report to display.
- Search for text in the report data.
- Perform an action on the entire group of incidents.
  For example, you can add a comment to all the incidents that are displayed. See “Performing actions on multiple tickets” on page 286.
- Refresh the contents of a section.
- Generate a preview of the section’s data in a new window, from which you can print or save the data.
- Export the section’s data to an Excel worksheet.
- Export the data to a CSV (comma-separated values) file that you can import into another program.
- Subscribe to the data as an RSS feed.

Some of the sections do not contain all of these options or actions.

The contents of the Technician Dashboard page can be customized permanently to display the information that is most useful to your technicians. For example, a Web part can be edited to display a different report or other Web parts can be added, deleted, or moved.

See “About customizing the contents of Process Manager portal pages” on page 80.

ServiceDesk contains an extensive catalog of Web parts that you can add to the dashboard pages. You can view the available Web parts when you click Admin > Portal > Web Parts Catalog.

# Tickets page

The Tickets page displays the current tickets. By default, it lists the tickets that are assigned to you but it can also display other tickets. For example, a support manager might view the Tickets page to monitor the progress of all open tickets.

The Start New Ticket section lets you create a ticket from the Tickets page instead of requiring you to go to another page. Also, the My Queues section lets you work your own tasks from the Tickets page.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

<table>
<thead>
<tr>
<th>Table 4-13</th>
<th>Default sections on the Tickets page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Bulletin Board</td>
<td>Lets you view the scrolling Bulletin Board messages that have been posted. By default, the Bulletin Board is set to hide if there are no messages. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>This section is not labeled.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-13  Default sections on the Tickets page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Recent Items**   | Displays the items that you recently viewed, opened, or worked on. You can select a recent item to open it.  
By default, the last 10 items are displayed. If you want to change the number of items, click **Show Options**. In the **Max Recent Items Count** field, change the number of items and click **Apply**.  
You can bookmark an item that is important to you. If you click the star symbol next to an item, that item is locked to the list even if 10 newer items exist. |
| **My Queues**      | Displays your tasks by user group and priority. You can sort the tasks by task number or priority, and you can search the tasks for specific text. You can select a task number to display the task’s **Process View** page. |
| **Find Ticket**    | Lets you find a ticket by specifying its process ID.                                                                                           |
| **Start New Ticket** | Lets you create a new ticket. The types of tickets or other service items that you can create depend on your permissions.                        |
| **My Open Tickets** | Lets you see the **My Open Tickets** report. This report displays the open tickets that are assigned to you.  
You can select a ticket number to display the ticket’s **Process View** page. If you have tickets in multiple processes, you must expand the appropriate process heading for the ticket that you want to work with.  
See “About the Process View page” on page 93.  
Initially, the page displays the **My Open Tickets** default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the **Report Settings** option appears, you can click it to change the appearance or contents of the report. The type of ticket and your permissions determine the options that are available. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report.  
See “Customizing a Process Manager portal page list” on page 88.  
See “Changing the report for a Process Manager portal page list” on page 91.  
The **Select a group action** drop-down list lets you perform certain actions on multiple tickets.  
See “Performing actions on multiple tickets” on page 286. |
Workflow page

The Workflow page provides administrators and managers with a comprehensive view of the current tasks and processes.

The Workflow page has the following views:

- **Workflow Task List**
  Lists all the tasks that are assigned to you.

- **Workflow Process List**
  Lists all the active processes and their associated tickets. The processes are arranged in workflow category order.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of Process Manager portal pages” on page 80.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Board</td>
<td>Lets you view the scrolling Bulletin Board messages that have been posted. By default, the Bulletin Board is set to hide if there are no messages.</td>
</tr>
<tr>
<td>This section is</td>
<td>For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer.</td>
</tr>
<tr>
<td>not labeled.</td>
<td>Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units.</td>
</tr>
<tr>
<td></td>
<td>See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>Open Task</td>
<td>Lets you open a specific task by specifying its <strong>Task ID</strong>.</td>
</tr>
<tr>
<td>Open Process</td>
<td>Lets you open a specific process by specifying its <strong>Process ID</strong>.</td>
</tr>
<tr>
<td>Service Catalog</td>
<td>Lets you view and use the services in the Service Catalog that you have permission for. The service items are organized in categories in a tree view. You can click the service item name to perform the action.</td>
</tr>
<tr>
<td></td>
<td>See “About the Service Catalog and service items” on page 442.</td>
</tr>
</tbody>
</table>
### Table 4-14  Default sections on the Workflow page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tasks Viewer</strong></td>
<td><em>(Workflow Task List only)</em></td>
</tr>
<tr>
<td></td>
<td>Displays the tasks that are assigned to you.</td>
</tr>
<tr>
<td></td>
<td>You can select a task number to display the task’s Process View page. If you have tasks in multiple processes, you must expand the appropriate process heading for the task that you want to work with.</td>
</tr>
<tr>
<td></td>
<td>See “About the Process View page” on page 93.</td>
</tr>
<tr>
<td></td>
<td>Initially, the page displays the default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the Report Settings option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing a Process Manager portal page list” on page 88.</td>
</tr>
<tr>
<td></td>
<td>See “Changing the report for a Process Manager portal page list” on page 91.</td>
</tr>
<tr>
<td><strong>Process Viewer</strong></td>
<td><em>(Workflow Process List only)</em></td>
</tr>
<tr>
<td></td>
<td>Displays all the processes that are currently running.</td>
</tr>
<tr>
<td></td>
<td>You can select a task number to display the task’s Process View page. If you have tasks in multiple processes, you must expand the appropriate process heading for the task that you want to work with.</td>
</tr>
<tr>
<td></td>
<td>See “About the Process View page” on page 93.</td>
</tr>
<tr>
<td></td>
<td>Initially, the page displays the default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the Report Settings option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing a Process Manager portal page list” on page 88.</td>
</tr>
<tr>
<td></td>
<td>See “Changing the report for a Process Manager portal page list” on page 91.</td>
</tr>
</tbody>
</table>
Managing portal pages

This chapter includes the following topics:

- Exporting a Process Manager portal page
- Importing a Process Manager portal page
- Rearranging the sequence of Process Manager portal pages
- Deleting Process Manager portal pages
- Disabling and enabling Process Manager portal pages

Exporting a Process Manager portal page

You can export the definition for a Process Manager portal page to a file in AXD, XML, or XSL format. No actual data is exported. The exported file can be imported to create a new page in the Process Manager portal.

For example, you might export a customized portal page so that it can be imported into other ServiceDesk installations within your organization. You might also share a portal page with a business partner or other company that uses ServiceDesk.

See “Importing a Process Manager portal page” on page 74.

To export a Process Manager portal page

1. In the Process Manager portal, click Admin > Portal > Manage Pages.
2. In the Pages List section, select the page to export.
   
   Note that the Export page option is not available for some default Process Manager portal pages.
3. In the Page section, click Export Page.
4. Use your Web browser to save the file.
Importing a Process Manager portal page

You can import a Process Manager portal page to replace an existing page that has the same page ID or create a new page. For example, you can import a customized page into other ServiceDesk installations within your organization without having to redo the customization in each installation. The exported file must be in AXD, XML, or XSL format.

See “Exporting a Process Manager portal page” on page 73.

The new page contains the same layout, settings, and permissions as the original page. After you import the page, you can move it to the appropriate sequence in the page order.

See “Rearranging the sequence of Process Manager portal pages” on page 74.

To import a Process Manager portal page

1. In the Process Manager portal, click Admin > Portal > Manage Pages.
2. At the upper right of the Pages List section, click the Import Page symbol (white page with a green plus sign).
3. In the Import Page dialog box, in Select File, specify the file to import.
4. If the page that you import has the same page ID as an existing page, select one of the following options:
   - Overwrite existing page
   - Create new copy
     The new page has the same name as the existing page with the same page ID.
5. Click Import.
6. (Optional) Move the new page to the appropriate place in the page sequence. If the new page does not appear in the correct place
   See “Rearranging the sequence of Process Manager portal pages” on page 74.

Rearranging the sequence of Process Manager portal pages

You can organize the tab bar or menu bar of the Process Manager portal by changing the sequence of the portal pages that appear there. You can rearrange the existing portal pages and the pages that you create. You can also change subpages to root pages and root pages to subpages.

See “About the Process Manager portal” on page 52.
Caution: A subpage’s permission settings must be the same as or more restrictive than the root page’s permission settings. Because a subpage does not inherit the permissions of its root page, you must set the permissions for the subpage separately.

To rearrange the sequence of Process Manager portal pages

1. In the Process Manager portal, click **Admin > Portal > Manage Pages**.
2. In the **Pages List** section, select the page to move.
3. Under the **Page** section, select any of the following options:
   - **Move Up**
   - **Move Down**
   - **Move Level Up**
     Moves a subpage up to the next level.
   - **Make as Sub Page**
     Displays a list of the existing pages, from which you select the root page to place the subpage under.
4. Continue to move the page until it is in the correct position.
5. Move additional pages if needed.

Deleting Process Manager portal pages

Process Manager portal pages can be deleted. For example, you might delete a default page that does not apply to your organization or a page that is no longer used. When a portal page is deleted, any users who have the page open are not able to save any information on that page. Also, no one can access the page from that point forward.

**Warning:** If you delete a Process Manager default portal page, that page is permanently removed from your environment. The only way to bring that page back in to your environment is to reinstall ServiceDesk.

An alternative to deleting a page is to disable it. That way, you can revert to using that page at any time by enabling it.

See “Disabling and enabling Process Manager portal pages” on page 76.
To delete a Process Manager portal page

1. In the Process Manager portal, click **Admin > Portal > Manage Pages**.
2. In the **Pages List** section, select the page to delete.
3. Click **Delete Page**.
4. In the confirmation dialog box, click **OK**.

Disabling and enabling Process Manager portal pages

You can disable and enable Process Manager portal pages. You can disable Process Manager portal pages so that users cannot access them from the portal pages menu. For example, you might disable a default portal page that does not apply to your organization.

When you disable a portal page, you remove it from the Process Manager portal pages menu, but that page stays in your environment. When you click **Admin > Portal > Manage Pages** that page still appears in the list of pages in the **Pages List** section. You can always revert to using that portal page at any time by enabling the page.

As a best practice, Symantec recommends that you disable portal pages rather than delete them.

**Warning:** If you delete a Process Manager default portal page, that page is permanently removed from your environment. The only way to bring that page back into your environment is to reinstall ServiceDesk.

See “**Deleting Process Manager portal pages**” on page 75.

After you let users use a portal page, you can still disable that page. The page is not removed from your environment; therefore, users may still have access to the page as follows:

- If a user has the disabled page open, the user can save information on that page.
  - If the user logs off or navigates away from that page, the user cannot access that page again. The page does not appear on the portal pages menu.

- If the disabled portal page is set as the home page, the user can access it when first logging on to the Process Manager portal.
  - If the user navigates away from that page, the user cannot access the page again during that session in the Process Manager portal. As long as that page is set as the home page, the user can access it each time the user logs on to the portal.
If the disabled portal page is bookmarked, the user can access that page from the list of bookmarks.

If the user knows the URL for the disabled portal page, the user can access that page by typing the page URL in the browser.

**To disable or enable Process Manager portal pages**

1. In the Process Manager portal, click **Admin > Portal > Manage Pages**.
2. In the **Page List** section, select the page that you want to disable or enable.
3. Click **Edit Page**.
4. In the **Edit Page** dialog box, perform one of the following actions:
   - Uncheck **Enabled** to remove the page from the portal pages menu.
   - Check **Enabled** to add the page to the portal pages menu.
5. Click **Save**.

Note that if you uncheck **Enabled** and click **Save**, the portal page no longer appears in your portal pages menu. If you check **Enabled** and click **Save**, the portal page reappears in your portal pages menu.
Managing portal pages

Disabling and enabling Process Manager portal pages
Customizing the contents of Process Manager portal pages

This chapter includes the following topics:

- About customizing the contents of Process Manager portal pages
- Setting your opening portal page
- Enabling the customization of a Process Manager portal page
- Customizing a Process Manager portal page (administrator)
- Customizing your Process Manager portal pages (non-administrator)
- Options on the Site Actions drop-down list
- Adding a Web part to a Process Manager portal page
- Editing or deleting a Web part on a Process Manager portal page
- Sharing a Process Manager portal page
- Customizing a Process Manager portal page list
- Options for customizing a Process Manager portal page list
- Changing the report for a Process Manager portal page list
About customizing the contents of Process Manager portal pages

The Process Manager portal consists of pages, from which all ServiceDesk activities are performed. The portal pages can be customized to meet your specific requirements.

Examples of the customizations that can be made are as follows:

- An administrator configures a different My Task List page for each group.
- An individual adds a search capability to their own Home page.
- A support manager customizes their Tickets page and then shares it with the rest of the support group.
- An administrator customizes a Process View page for a specific type of worker. For example, a high-level support technician might need additional actions.

Administrators can perform all the customization actions and can grant customization permissions to other ServiceDesk users. Non-administrator users typically have fewer options for customizing portal pages.

See “Enabling the customization of a Process Manager portal page” on page 81.

Customizing portal pages consists of the following actions:

- Adding and deleting pages
- Specifying which pages can be customized
- Adding, editing, and deleting the Web parts that appear on a page
- Sharing pages with other users

See “Customizing a Process Manager portal page (administrator)” on page 82.

You can also set a portal page to be the page that opens whenever you log on to the Process Manager portal.

See “Setting your opening portal page” on page 80.

Setting your opening portal page

Whenever you log on to the Process Manager portal, the portal opens to a specific page.

See “Logging on to the Process Manager portal” on page 53.
Initially, your permissions determine which page opens. However, you can set a different page to open when you log on. This page does not necessarily have to be the one that is labeled the **Home** page.

**To set your opening page**

1. In the Process Manager portal, open the page that you want to make your home page.
2. At the bottom of the portal page, click **Make Home Page**.

---

**Enabling the customization of a Process Manager portal page**

Before anyone can customize a Process Manager portal page, the administrator must enable that page for customization. Enabling a page for customization consists of setting the appropriate privileges and permissions.

See “About customizing the contents of Process Manager portal pages” on page 80.

**Table 6-1** Process for enabling the customization of a Process Manager portal page

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set customization privileges for a user or group.</td>
<td>The privilege setting for groups is <strong>Portal.PersonalCustomization</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The privilege setting for users is <strong>PersonalCustomization</strong>, which is under the <strong>Portal</strong> category.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set customization permissions on the page.</td>
<td>For each page, set permissions for adding, editing, or deleting the page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On the Administrator tab, under <strong>Portal &gt; Manage Pages</strong>, you can edit the page to enable it for customization as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Allow User Personalization</strong> setting enables the <strong>Modify My Page</strong> option on the portal page. That option lets a user edit their own page without affecting that page for other users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The page’s <strong>Permissions</strong> settings let you allow users, groups, permissions, or organizational units to view, edit, or delete the page.</td>
</tr>
</tbody>
</table>
Customizing a Process Manager portal page (administrator)

By default, the administrator can customize any portal page that is able to be customized.

See “About customizing the contents of Process Manager portal pages” on page 80.

See “Optimizing reports in the Process Manager portal” on page 393.

To customize a Process Manager portal page

1. In the Process Manager portal, open the page that you want to customize.
2. In the upper right of the page, in the Site Actions drop-down list, select an action to perform.
   
   See “Options on the Site Actions drop-down list” on page 83.
3. When you finish the customization, you can close the page.

Customizing your Process Manager portal pages (non-administrator)

You can customize a portal page if you have permission to do so. The pages that you are most likely to customize are the Task List page and the Home page. For example, you might want to place a schedule or another report on your Home page.

Before anyone can customize a Process Manager portal page, the administrator must enable that page for customization.
To customize a Process Manager portal page

1. In the Process Manager portal, open the page that you want to customize.

2. In the upper right of the page, in the Site Actions drop-down list, select one of the following options:

   - **Modify Page**: Lets you add, edit, and delete the Web parts that are on the page.
   - **Modify My Page**: The Modify Page option changes the page for everyone who has access to it. The Modify My Page option changes your version of the page only.
     
     See “Adding a Web part to a Process Manager portal page” on page 85.
     
     See “Editing or deleting a Web part on a Process Manager portal page” on page 86.
   - **Reset to Default**: Discards any changes that you made to the portal page and reverts it to its original configuration. This option only appears if you select Modify My Page to modify the portal page.
     
     Note that if you select Modify Page, the option to Reset to Default does not appear, which means any changes that you make cannot be undone.
   - **Share Page**: Lets you specify a user, group, permission, or organizational unit can view your customized version of the portal page.
     
     See “Sharing a Process Manager portal page” on page 87.

   This drop-down list appears only on the pages that you have the permission to customize. The options that are available depend on your permissions.

   See “Options on the Site Actions drop-down list” on page 83.

3. When you finish the customization, you can close the page.

For information about optimizing your reports on your portal pages to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

## Options on the Site Actions drop-down list

You can use the options in the Site Actions drop-down list to customize a Process Manager portal page. This drop-down list appears only on the pages that you have the permission to customize. The options that are available to you in the Site Actions drop-down list depend on your permissions.
The options that are available also depend on where you are in the editing process. For example, when you are on a main portal page, the **Edit Page** option does not appear in the **Site Actions** drop-down list. After you click **Site Actions > Modify Page** and the page opens for editing, the **Edit Page** option becomes available in the **Site Actions** drop-down list.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Root Page</strong></td>
<td>Lets you add a new portal page, which is visible from the top level of the Process Manager portal. The page name appears on the tab bar in the Process Manager portal. Typically, only administrators have permission to create new pages.</td>
</tr>
<tr>
<td><strong>Add Sub Page</strong></td>
<td>Lets you add a new subpage, which is one or more levels under a root page. A subpage can appear on the menu of a root page. For example, the Knowledge Base page is a root page. You open it by clicking the Knowledge Base tab. The Discussions page is a subpage. You open it by clicking the Discussions command on the Knowledge Base tab. Typically, only administrators have permission to create new pages.</td>
</tr>
<tr>
<td><strong>Add Web Part</strong></td>
<td>Lets you add one or more Web parts to the page. The sections on a Process Manager portal page are in the form of Web parts. See “Adding a Web part to a Process Manager portal page” on page 85.</td>
</tr>
<tr>
<td><strong>Browse</strong></td>
<td>Exits the editing mode and displays the page with the changes that you made.</td>
</tr>
<tr>
<td><strong>Clear</strong></td>
<td>Deletes all the Web parts from a portal page. <strong>Warning:</strong> This action cannot be undone. Use caution when you select this option because you are not prompted to confirm this action before the deletion occurs.</td>
</tr>
<tr>
<td><strong>Edit Definition</strong></td>
<td>Opens the Edit Page, which lets you configure customization settings and customization privileges for the current portal page. When you select <strong>Save Page</strong> or <strong>Cancel</strong>, it takes you to the <strong>Manage Pages</strong> page. This page also lets you customize privileges and configure settings for the portal page that you select in the <strong>Pages List</strong> pane. Typically, only administrators have permission to edit page definitions. See “Enabling the customization of a Process Manager portal page” on page 81.</td>
</tr>
<tr>
<td><strong>Edit Page</strong></td>
<td>Lets you edit and delete the Web parts that are on the page. See “Editing or deleting a Web part on a Process Manager portal page” on page 86.</td>
</tr>
<tr>
<td><strong>Modify Page</strong></td>
<td>Lets you add, edit, and delete the Web parts that are on the page. The page is changed for everyone who has access to it.</td>
</tr>
<tr>
<td><strong>Modify My Page</strong></td>
<td>Lets you add, edit, and delete the Web parts that are on the page. Only your page is changed. This option appears only if the page is configured to allow it.</td>
</tr>
</tbody>
</table>
Table 6-2  Options on the Site Actions drop-down list (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page List</td>
<td>(Administrator only) Displays the Pages List page that lets you configure settings and customization permissions for any portal page.</td>
</tr>
</tbody>
</table>
| Reset to Default| Discards any changes that were made to the portal page and reverts it to its original configuration. Portal page changes can be reverted as follows:  
  - A user can discard the changes that they made with the Modify My Page option.  
  - A user can discard the changes that someone else made with the Modify My Page and Share Page options.  
  - A user cannot discard the changes that someone else made with the Modify Page option.  
  If you have the permission to do so, you can delete the individual web parts that someone else added. |
| Share Page      | Lets you specify a user, group, permission, or organizational unit that can view your customized version of a portal page. For example, the support manager can customize the Task List page and then share it with members of the Support 1 group.  
  You can also provide additional permissions for this page as follows:  
  - Let others edit this page.  
  - Provide view, edit, and delete permissions to a specific user, group, permission, or organizational unit.  
    For example, the administrator customizes a page, lets all users in a group view the page, and then lets a specific user edit the page. |

Adding a Web part to a Process Manager portal page

The sections on a Process Manager portal page are in the form of Web parts. You can customize a portal page by adding one or more Web parts.

After you add a Web part, you can edit its properties.

See “Editing or deleting a Web part on a Process Manager portal page” on page 86.

To add a Web part to a portal page

1. In the Process Manager portal, open the page that you want to customize.
2. In the upper right of the page, in the Site Actions drop-down list, select one of the following options:
   - Modify Page  Changes the page for everyone who has access to it.
   - Modify My Page  Changes your version of the page only.
3. After the page refreshes, in the Site Actions drop-down list, click Add Web Part.

4. In the Catalog Zone pop-up, select the catalog that contains the Web part to add.

5. In the Catalog Zone pop-up, under the catalog name, select the check box for each Web part that you want to add.

6. In the Catalog Zone pop-up, in the Add to drop-down list, select the page zone to add the Web part to.

   The zones that are available depend on the page’s Template Page setting, which the administrator sets.

7. Click Add.

8. (Optional) To add another Web part, repeat from step 4.

9. When you finish adding Web parts, in the Catalog Zone pop-up, click Close.

**Editing or deleting a Web part on a Process Manager portal page**

The sections on a Process Manager portal page are in the form of Web parts. You can customize a portal page by editing or deleting one or more Web parts.

**To edit a Web part on a portal page**

1. In the Process Manager portal, open the page that you want to customize.

2. In the upper right of the page, in the Site Actions drop-down list, select one of the following options:

   - **Modify Page** Changes the page for everyone who has access to it.
   - **Modify My Page** Changes your version of the page only.

3. In the upper right of the Web part that you want to edit, select one of the following options:

   - **Edit symbol (note pad and pencil)** Opens the Editor Zone.
     Lets you edit the properties of the Web part.

   - **Delete symbol (red X)** Lets you delete the Web part.
4 If you clicked **Edit**, in the **Editor Zone**, edit the properties of the Web part, and then select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply</strong></td>
<td>Saves the changes without closing the <strong>Editor Zone</strong>.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Saves the changes and closes the <strong>Editor Zone</strong>. Select this option when you finish editing the properties for the current Web part.</td>
</tr>
</tbody>
</table>

5 (Optional) To edit or delete another Web part, repeat from step 3.

6 When you finish editing the Web parts, you can close the page.

---

**Sharing a Process Manager portal page**

You can share your version of a Process Manager portal page with others to let them see any customizations that are on your page. Typically, you share the pages that you or someone else has customized.

You can share pages by providing the view, edit, and delete permissions to specific users, groups, permission, or organizational unit. For example, the administrator can customize a page and let all users in a certain group view the page. Then the administrator can let only one specific user within that group edit the page.

The users’ portal permissions override any share permissions that you might provide. For example, a user who does not normally have permission to view the **Tickets** page cannot view a shared version of that page.

**To share a Process Manager portal page**

1 In the Process Manager portal, open the page that you want to share.

2 (Optional) Customize the page.
   - See “**Customizing a Process Manager portal page (administrator)**” on page 82.
   - See “**Customizing your Process Manager portal pages (non-administrator)**” on page 82.

3 In the upper right of the page, in the **Site Actions** drop-down list, click **Share Page**.

4 Under **Page Permissions**, review the users, groups, or other entities that have permissions for this page.
5 Under **Share Page**, select an option in each of the following subsections:

**Share With**
- Select the type of entity to give permissions for sharing this page.
- The **Users With Permissions** option lets you select the permissions that the user must have to view, edit, or delete the page.

**Sharing Type**
- Select the type of share permissions to give.
- The **Custom (Advanced)** option provides additional ways to customize the permissions.

6 Under **Share Page**, click **Next**.

7 Specify the user, group, or other entity to share this page with, and then click **Share Page**.

8 When you are returned to the page, you can continue to edit it or close it.

### Customizing a Process Manager portal page list

Several Process Manager portal pages contain the lists that you use to analyze or perform ServiceDesk activities. You can customize the lists that appear on your pages so that they display the information in the manner that is most useful to you. For example, on the **My Task List** page, you might want to change the task list so that it displays only your overdue tasks.

Examples of portal page lists are as follows:

- On the **My Task List** page, the task list that appears in the **Task Viewer** section. See “**My Task List page**” on page 63.

- On the **Home** page, the request list that appears in the **My Requests** section. See “**Home page**” on page 61.

- On the **Tickets** page, the tickets that appear in the **My Open Tickets** section. See “**Tickets page**” on page 69.

The primary way to customize a portal page list is to change the report that determines the contents of the list. You can also sort and filter the list to display a more specific subset of information. Some changes that you make are active until the page refreshes or for the current session only. Some changes are lost when you log off the Process Manager portal. However, you can select a new report that persists beyond a single session.

See “**Changing the report for a Process Manager portal page list**” on page 91.
For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

**To customize a Process Manager portal page list**

1. In the Process Manager portal, open the page that contains the list that you want to edit.

2. On the portal page, in the section that contains the list, you can customize the list in the following ways:
   - Sort the columns.
   - Search and filter the list.
   - Limit the number of records that appear.
   - Select a new report.
   - Refresh the report.

   See “Options for customizing a Process Manager portal page list” on page 89.

3. When you finish customizing the list, you can close the page or work on it.

**Options for customizing a Process Manager portal page list**

You can customize a portal page list so that it displays information in the manner that is most useful to you.

Examples of portal page lists are as follows:

- The task list that appears in the **Task Viewer** section on the **My Task List** page. See “My Task List page” on page 63.

- The request list that appears in the **My Requests** section on the **Home** page. See “Home page” on page 61.

- The tickets that appear in the **My Open Tickets** section on the **Tickets** page. See “Tickets page” on page 69.

**Table 6-3** Options for customizing a Process Manager portal page list

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjust column width.</td>
<td>You can adjust the width of a column to better see the contents in the column.</td>
</tr>
<tr>
<td>Sort the columns.</td>
<td>You can click any column heading to sort by that heading.</td>
</tr>
</tbody>
</table>
Table 6-3 Options for customizing a Process Manager portal page list (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the results of the list:</td>
<td>You can search the list to filter the results. For example, to list only those items that have to do with printers, you can search for “printer”. You can filter a list by using either of the following options: <strong>Search symbol</strong> You can click the <strong>Search</strong> symbol to open a search box. If you want to see all the items in the list again, click the <strong>Refresh</strong> symbol. <strong>Text contains</strong> You can expand the <strong>Report Settings</strong> section and click <strong>Text contains</strong> to open a search dialog box. You might not see the <strong>Support Settings</strong> section because it appears for certain reports only. If you want to see all the items in the list again, click <strong>Text contains</strong>, delete your search text, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Limit the number of records that appear.</td>
<td><strong>Return 50 first records</strong> You can change the number of records that appear in the list. Typically, the list contains the first 50 records that match the report criteria. You can change the number of records that appear by expanding the <strong>Report Settings</strong> section, clicking the <strong>Return 50 first records</strong> link, and specifying a new number. You might not see the <strong>Support Settings</strong> section because it appears for certain reports only. Other options might appear depending on the type of ticket.</td>
</tr>
<tr>
<td>Change the report.</td>
<td><strong>Change Report symbol</strong> You can select a new report to display the list in a different configuration. For example, you select a report that displays all your open tasks. You can select a new report. Click the <strong>Change Report</strong> symbol. A list of folders opens, which contains the reports that are available. See &quot;Changing the report for a Process Manager portal page list&quot; on page 91.</td>
</tr>
<tr>
<td>Output the report.</td>
<td><strong>Actions symbol</strong> You can output the report in the following ways: <strong>Print Preview</strong> <strong>Export to Excel</strong> <strong>Export to CSV</strong> <strong>RSS</strong></td>
</tr>
</tbody>
</table>
Changing the report for a Process Manager portal page list

Each list on a Process Manager portal page is associated with a default report that determines the contents of the list. You can change the report to display the list in a different configuration. For example, you can select a report that displays all your open tasks.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

When you change the report for a list, it becomes the new report for the list. The next time you log on, this report populates the list.

If you want to see the original default report, do one of the following actions:

- Use the Change Report symbol to change the report back to the default report. This action requires you to know the name of the default report.
- Edit the Web part. This action requires you to use the Editor Zone to change the report back to the default report.

Changing the report for a list does not save any additional filtering of the list.

To change the report for a Process Manager portal page list

1. In the Process Manager portal, open the page that contains the list to edit.
2. On the page, under the list section, click the Change Report symbol.
3. Select the report group, and then select the report to use.
   To quickly find a report, you can type search text in the box and click Find.
4. When you finish customizing the list, you can close the page or work on it.

---

Table 6-3 Options for customizing a Process Manager portal page list (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh the report display. Refresh symbol</td>
<td>You can refresh the display after you select a new report.</td>
</tr>
</tbody>
</table>
Customizing the contents of Process Manager portal pages

Changing the report for a Process Manager portal page list
Working in the Process View

This chapter includes the following topics:

- About the Process View page
- Process View page (Incident Management)
- Process View page (Problem Management)
- Process View page (Change Management)
- About actions and smart tasks on the Process View pages
- About Process Type Actions on the Process View pages
- Adding Process Type Actions
- Editing Process Type Actions
- Deleting Process Type Actions

About the Process View page

A Process View page is the primary interface for working an incident, problem, or change request ticket. Each type of ticket has its own Process View page. The corresponding Process View page appears when you open a ticket.

The Process View page consists of multiple sections (Web parts) that display general information about the ticket and provide the actions that you can perform. The default Process View page layout is similar for all tickets. The actions that you can perform and the information that you can access depend on the type of ticket and your permissions.

The default Process View page are as follows:

- Process View page for working an incident ticket
See “Process View page (Incident Management)” on page 94.

- **Process View** page for working a problem ticket
  See “Process View page (Problem Management)” on page 98.

- **Process View** page for working a change request ticket

## Process View page (Incident Management)

The Incident Management’s **Process View** page is the primary interface for working an incident ticket. This **Process View** page appears when you open an incident ticket. The **Process View** page consists of multiple sections (Web parts) that display general information about the incident and any actions that you can perform.

Examples of the general information that the Incident Management’s **Process View** page provides are as follows:

- The incident's process history
- The Service Level Agreement status
- The current assignments

Examples of the actions that the Incident Management’s **Process View** page lets you perform are as follows:

- Work the incident or a subtask.
- Manage the subtasks.
- Search the knowledge base.

The actions that are available to you and the information that you can access on the **Process View** page depend on the following conditions:

- Where the ticket is in the resolution process
- Your involvement in the process
- Your permissions

If your Incident Management's **Process View** page was customized, its appearance and contents might differ from the default **Process View** page.
<table>
<thead>
<tr>
<th>Table 7-1</th>
<th>Default sections on the Incident Management's Process View page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Comments | Displays only the comments from the Process History section. Lets you do the following actions:  
- Sort the comments by date  
- Filter the list of comments  
- Open the comment in its own dialog box  
The dialog box provides a link that lets you open the Edit Comment dialog box and edit the comment. You can modify the title and comment. You can select a different View Level. You can also make the comment a user level comment. This option is available for the Admin selection in the View Level drop-down list |
| Current Assignments | Displays the current tasks and subtasks in the incident resolution process and to whom each task is assigned. You can view details about the assignee if you have permission to do so. |
| Description and Resolution | Displays the description of the incident as entered during the creation of the incident or as modified by the technician who works the ticket. Displays the resolution of the incident. Provides a link that lets you add a comment to the Process History. The link opens the Add Comment to Process dialog box that lets you do the following:  
- You can add a title and comment.  
- You can select a View Level.  
- You can add a user level comment. This option is active when you select Admin in the View Level drop-down list. |
| Incident Request Attachments | Displays any documents that are attached to the incident. Provides a link that lets you open the documents, edit the document, delete the document, and perform other actions. It also lets you attach additional documents. |
### Table 7-1 Default sections on the Incident Management's Process View page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Contacts</strong></td>
<td>Displays the primary contacts for the ticket by default. You can view details about the contact or add a new contact if you have permission to do so. Typically, the primary contact is the person who reports or submits the incident. Sometimes, the primary contact is someone other than the reporter or submitter.</td>
</tr>
<tr>
<td><strong>Process History</strong></td>
<td>Displays a record for each action that has occurred within the process. For example, a record can represent a status change, a task, or a user comment. Within the Process History section, you can click the link in an individual record to open the record in a new dialog box. The dialog box lets you review and edit the information.</td>
</tr>
<tr>
<td><strong>Process References</strong></td>
<td>List the items that are related to the process. Provides the links that you can use to discover more information about those items. You can view details about the related processes or add new references if you have permission to do so.</td>
</tr>
<tr>
<td><strong>Quick Service Links</strong></td>
<td>Lets you view and use the services in the Service Catalog for which you have permission. The service items are organized in categories in a tree view. You can click the service item name to perform the action. See “About the Service Catalog and service items” on page 442.</td>
</tr>
<tr>
<td><strong>Related Processes</strong></td>
<td>Lists any other tickets that can be associated with the incident. For example, this section might list a problem to which the incident has been added.</td>
</tr>
<tr>
<td><strong>SLA Status</strong></td>
<td>Displays the Service Level Agreement (SLA) status and SLA late dates for initial response and incident resolution. You can pause, resume, delete, or reset the resolution and initial response SLAs.</td>
</tr>
</tbody>
</table>
### Table 7-1 Default sections on the Incident Management's Process View page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start/Stop Process Timing</strong></td>
<td>Displays the amount of time that has been recorded for a ticket to date and lets you post additional time. ServiceDesk tracks the following times:</td>
</tr>
<tr>
<td></td>
<td><strong>Total Process Time</strong></td>
</tr>
<tr>
<td></td>
<td>The amount of time that was spent on the incident to date, including the time that was recorded automatically and the time that workers posted.</td>
</tr>
<tr>
<td></td>
<td><strong>User Process Time</strong></td>
</tr>
<tr>
<td></td>
<td>The total amount of offline time that the workers have posted to the incident to date.</td>
</tr>
<tr>
<td></td>
<td><strong>Current User Process Time</strong></td>
</tr>
<tr>
<td></td>
<td>The amount of time that accumulates for the worker who has the incident’s Process View page open.</td>
</tr>
<tr>
<td></td>
<td>See “About the process time for tickets” on page 285.</td>
</tr>
</tbody>
</table>

- **Tasks and Actions** displays the following items:
  - List of the tasks or subtasks in the process which are assigned to you and the actions you can take to complete the tasks.
  - **Work Tasks Assigned To Others** checkbox
    - If this checkbox appears, you can check it and work the tasks that are assigned to others.
  - List of the Change and Problem Management actions that you can perform, such as requesting a change.
  - List of the smart tasks that you can perform, such as managing subtasks or placing an incident on hold.
  - **Process Actions** subsection
    - List of the Process Type Actions that you can perform from the Process View page, such as managing service queues and searching the knowledge base.

See “About actions and smart tasks on the Process View pages” on page 104.

See “About Process Type Actions on the Process View pages” on page 106.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket Overview</td>
<td>Provides a quick view of the ticket’s identifying details and statistics. Contains the following action links:</td>
</tr>
<tr>
<td></td>
<td>■ Refresh</td>
</tr>
<tr>
<td></td>
<td>■ Add Comment Opens the Add Comment to Process dialog box. You can add a title and comment. You can select a View Level. You can also add a user level comment. This option is active when you select Admin in the View Level drop-down list.</td>
</tr>
<tr>
<td></td>
<td>■ Print On a new tab in your browser, opens a printable version of the Process View page. You can use your Web browser to print the page.</td>
</tr>
</tbody>
</table>

See “About the Process View page” on page 93.

**Process View page (Problem Management)**

The Problem Management's **Process View** page is the primary interface for working a problem ticket. This **Process View** page appears when you open a problem ticket. The **Process View** page consists of multiple sections (Web parts) that display general information about the problem and any actions that you can perform.

Examples of the general information that the Problem Management's **Process View** page provides are as follows:

■ The problem's history
■ The related processes
■ The assignments

Examples of the actions that the Problem Management’s **Process View** page lets you perform are as follows:

■ Work the problem.
■ Change the priority.
■ Remove the problem.
The actions that are available to you and the information that you can access on the Process View page depend on the following conditions:

- Where the ticket is in the resolution process
- Your involvement in the process
- Your permissions

If your Problem Management's Process View page was customized, its appearance and contents might differ from the default Process View page.

Table 7-2 Default sections on the Problem Management's Process View page

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Contacts</td>
<td>Displays the users who are associated with the ticket or who work on the ticket. These users can be anyone who works on the ticket as well as anyone who is added at any phase of the process. You can view details about the contact or add a new contact if you have permission to do so.</td>
</tr>
<tr>
<td>Assignments</td>
<td>Displays the following items:</td>
</tr>
<tr>
<td></td>
<td>- List of the actions that you can take to effectively work the ticket.</td>
</tr>
<tr>
<td></td>
<td>- Work Tasks Assigned To Others checkbox</td>
</tr>
<tr>
<td></td>
<td>If this checkbox appears, you can check it and work the ticket.</td>
</tr>
<tr>
<td></td>
<td>- List of the smart tasks that you can perform, such as adding an incident or starting a discussion.</td>
</tr>
<tr>
<td></td>
<td>See “About actions and smart tasks on the Process View pages” on page 104.</td>
</tr>
<tr>
<td>Description</td>
<td>(Read only) Displays the description that was entered during the task’s initial creation.</td>
</tr>
<tr>
<td>Documents</td>
<td>Displays any documents that are attached to the process or task and lets you attach additional documents.</td>
</tr>
<tr>
<td>History</td>
<td>Displays a record for each action that has occurred within the process. For example, a record can represent a status change, a task, or a user comment.</td>
</tr>
</tbody>
</table>
Table 7-2  Default sections on the Problem Management's *Process View* page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions</td>
<td>Lists the workers and groups who have permission to participate in the process and what they can do. You can edit or delete existing permissions, and you can add new permissions. Permissions are not checked when you make changes in this section. If the people who you enter do not have the appropriate permissions, they cannot participate in the process regardless of what you enter.</td>
</tr>
<tr>
<td>Primary Contacts</td>
<td>Displays the primary contact for the ticket. Typically, the primary contact is the person who reports the problem. Sometimes, the primary contact is someone other than the submitter.</td>
</tr>
</tbody>
</table>
| Process Time      | Displays the amount of time that has been recorded for a ticket to date and lets you post additional time.  
ServiceDesk tracks the following times:  
  - **Current User Process Time**  
    The amount of time that accumulates for the worker who has the incident’s *Process View* page open.  
  - **User Process Time**  
    The total amount of offline time that the workers have posted to the incident to date.  
  - **Total Process Time**  
    The amount of time that was spent on the incident to date, including the time that was recorded automatically and the time that workers posted.  
See “About the process time for tickets” on page 285. |
| Related Items     | List the items that are related to the process. Provides the links that you can use to discover more information about those items. You can view details about the related processes or add new references if you have permission to do so. |
| Related Processes | Lists any other tickets that can be associated with the current problem ticket. |
### Table 7-2  Default sections on the Problem Management's Process View page (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch View</strong></td>
<td>Lets you switch between the <strong>Full Process View</strong> and the <strong>Basic Process View</strong>. The <strong>Full Process View</strong> is the default view. The <strong>Basic Process View</strong> is a simplified view that eliminates many of the options that normally appear. This view is useful for reviewing the process tickets that have extensive history.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Top section</th>
<th>Provides a quick view of the ticket’s identifying details and statistics. Contains the following action links:</th>
</tr>
</thead>
</table>
| The title bar displays the title of the problem. | ■ **Refresh**  
■ **Add Comment**  
  Opens the **Add Comment to Process** dialog box.  
  You can add a title and comment.  
  You can select a **View Level**.  
  You can also add a user level comment. This option is active when you select **Admin** in the **View Level** drop-down list.  
■ **Print**  
  On a new tab in your browser, opens a printable version of the **Process View** page.  
  You can use your Web browser to print the page.                                                                                     |

See “About the Process View page” on page 93.

---

**Process View page (Change Management)**

The Change Management’s **Process View** page is the primary interface for working a change request ticket. This **Process View** page appears when you open a change request ticket. The **Process View** page consists of multiple sections (Web parts) that display general information about the change request and any actions that you can perform.

Examples of the general information that the Change Management's **Process View** page provides are as follows:

- The change request's process history
- The implementation plan
- The current assignments
Examples of the actions that the Change Management's Process View page lets you perform are as follows:

- Complete a change task.
- Plan change actions.
- Implement a change.

The actions that are available to you and the information that you can access on the Process View page depend on the following conditions:

- Where the ticket is in the resolution process
- Your involvement in the process
- Your permissions

If your Change Management's Process View page was customized, its appearance and contents might differ from the default Process View page.

<table>
<thead>
<tr>
<th>Table 7-3</th>
<th>Default sections on the Change Management's Process View page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Add Process Comment</td>
<td>Contains a link that lets you add a process comment. The link opens the Add Comment to Process dialog box. This dialog box lets you do the following actions:</td>
</tr>
<tr>
<td></td>
<td>- Add a title and comment.</td>
</tr>
<tr>
<td></td>
<td>- Select a View Level.</td>
</tr>
<tr>
<td></td>
<td>- Add a user level comment. This option is active when you select Admin in the View Level drop-down list.</td>
</tr>
<tr>
<td>Backout Plan</td>
<td>(Read only) Displays information about the back-out plan for the change implementation, such as details about the plan, status, and who developed the plan.</td>
</tr>
<tr>
<td>Change Request Attachments</td>
<td>Displays any documents that are attached to the process or task. Lets you open the documents. It also lets you attach additional documents</td>
</tr>
<tr>
<td>Current Assignments</td>
<td>Displays the current tasks in the change process and to whom each task is assigned. You can view details about the assignee if you have permission to do so.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Implementation Plan</td>
<td>(Read only) Displays information about the change implementation plan, such as details about the plan, status, and who developed the plan.</td>
</tr>
<tr>
<td>Process Contacts</td>
<td>Displays the primary contacts for the ticket by default. You can view details about the contact or add a new contact if you have permission to do so.</td>
</tr>
<tr>
<td></td>
<td>Typically, the process contact is the person who requests the change. Sometimes, the process contact is someone other than the change requestor.</td>
</tr>
<tr>
<td>Process History</td>
<td>Displays a record for each action that has occurred within the process. For example, a record can represent a status change, a task, or a user comment.</td>
</tr>
<tr>
<td></td>
<td>Within the Process History section, you can click the link in an individual record to open the record in a new dialog box. The dialog box lets you review and edit the information.</td>
</tr>
<tr>
<td>Process References</td>
<td>List the items that are related to the process. Provides the links that you can use to discover more information about those items.</td>
</tr>
<tr>
<td></td>
<td>You can view details about the related processes or add new references if you have permission to do so.</td>
</tr>
<tr>
<td>Related Processes</td>
<td>Lists any other tickets that can be associated with the change request. For example, this section might list any additional incidents that require the same change.</td>
</tr>
<tr>
<td>Request Details</td>
<td>(Read only) Displays the description and justification that was entered during the change request's initial creation.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tasks and Actions</td>
<td>Displays the following items:</td>
</tr>
<tr>
<td></td>
<td>■ List of the tasks in the process which are assigned to you and the actions you can take to complete the tasks.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Work Tasks Assigned To Others</strong> checkbox</td>
</tr>
<tr>
<td></td>
<td>If this checkbox appears, you can check it and work the tasks that are assigned to others.</td>
</tr>
<tr>
<td></td>
<td>■ List of the additional actions that you can perform, such as managing planning tasks or delegating the implementation plan.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Process Actions</strong> subsection</td>
</tr>
<tr>
<td></td>
<td>List of the <strong>Process Type Actions</strong> that you can perform from the <strong>Process View</strong> page, such as managing CABs and searching the knowledge base.</td>
</tr>
<tr>
<td></td>
<td>See “About actions and smart tasks on the Process View pages” on page 104.</td>
</tr>
<tr>
<td></td>
<td>See “About Process Type Actions on the Process View pages” on page 106.</td>
</tr>
<tr>
<td>Testing Plan</td>
<td>(Read only) Displays the information about the testing plan for the change implementation, such as details about the plan, status, and who developed the plan.</td>
</tr>
<tr>
<td>Ticket Overview</td>
<td>Provides a quick view of the ticket’s identifying details and statistics.</td>
</tr>
<tr>
<td></td>
<td>Contains the following action links:</td>
</tr>
<tr>
<td></td>
<td>■ Refresh</td>
</tr>
<tr>
<td></td>
<td>■ Print</td>
</tr>
<tr>
<td></td>
<td>On a new tab in your browser, opens a printable version of the <strong>Process View</strong> page.</td>
</tr>
<tr>
<td></td>
<td>You can use your Web browser to print the page.</td>
</tr>
</tbody>
</table>

See “About the Process View page” on page 93.

### About actions and smart tasks on the Process View pages

The **Process View** pages for working an incident, a problem, or a change request ticket include actions and smart tasks as quick links. These links let you take
immediate actions or launch other processes that can help you with your task or process. The actions and smart tasks on the Process View pages save time and can improve the turnaround of incident and problem resolution and change implementation.

The actions that appear on the Process View page vary for different processes. Each Process View page includes the actions and smart tasks that are most relevant and useful for its particular process.

For example, when a technician views an incident, some process-specific step may need to be taken to resolve it. The technician may want to relate the incident to a problem or suggest self-service. Actions and smart tasks provide a quick way for the incident technician to launch those tasks from within the Process View page. When a change implementer views a change request, some process-specific step may need to be taken to implement the change. The change implementor may need to delegate the test plan or the back-out plan to another worker.

Examples of the actions and smart tasks that might appear on the incident ticket's Process View pages are as follows:

- Reassign Ticket
- Manage Subtasks
- Work Incident
- Suggest Self Service
- View Forward Schedule Change
- Reassign Ticket

Examples of the actions and smart tasks that might appear on the problem ticket's Process View pages are as follows:

- Work Problem
- Add Incident
- Remove Problem
- Invite Participant

Examples of the actions that might appear on the change request ticket's Process View pages are as follows:

- Delegate Backout Plan
- Complete Task
- Manage Planning Tasks
- Reassign
Implement Right Away

See “Process View page (Incident Management)” on page 94.

See “Process View page (Problem Management)” on page 98.


About Process Type Actions on the Process View pages

Process Type Actions are links to processes that you can perform from the incident and the change request tickets’ Process View page. The Incident and Change Management Process View pages include a set of default Process Type Actions as quick links. These actions are in the Tasks and Actions section in the Process Actions subsection. These actions save time and can improve the turnaround of incident resolution and change implementation.

See “Process View page (Incident Management)” on page 94.


For example, a technician may want to search the Microsoft TechNet Website for help to resolve this incident. The change implementer may want to search the knowledge base to help create a back-out plan. Process Type Actions provide a quick way for the incident technician or change implementer to launch those tasks from within the Process View page.

Permissions control the ability to access Process Type Actions.

The following default Process Type Actions are available for you to use on the incident ticket's Process View page:

- Edit Incident
- Manage Related Configuration Items
- Search KB
- Create Bulletin Board Entry
- Submit KB
- Search TechNet
- Manage Service Queues
- Manage Subtask Templates
- Reopen Incident
- Search Knowledge Base
Send Email
This action does not appear until you create your Incident Management email templates.
See “Creating email templates for Incident Management” on page 195.

The following default Process Type Actions are available for you to use on the change request ticket’s Process View page:

- Edit Change Plan
- Manage CABs
- Manage Templates
- Manage Related Configuration Items
- Manage Related Processes
- Add Bulletin Board Entry
- Search Knowledge Base
- Send Email
  This action does not appear until you create your Change Management email templates.
  See “Creating email templates for Change Management” on page 234.

In the Process Manager portal, on the Process Type Action page, you can add and delete Process Type Actions from the Process View pages and you can edit the Process Type Actions.

See “Adding Process Type Actions” on page 107.

See “Editing Process Type Actions” on page 110.

See “Deleting Process Type Actions” on page 112.

You can create your own Process Type Actions to meet your specific needs. You can create your own external workflow projects in Workflow Designer. Then, you can create new Process Type Actions on the Process Type Action page and link them to your workflow projects and launch them from the Process View page.

## Adding Process Type Actions

Process Type Actions let you quickly do external processes directly from the incident and the change request tickets’ Process View pages. ServiceDesk provides a set of default Process Type Actions.

See “About Process Type Actions on the Process View pages” on page 106.
You can add your own **Process Type Actions**. For example, you can add an action that lets technicians do a Google search directly from the **Process View** page.

You can add actions to the Incident Management and Change Management **Process View** pages.

**To add a Process Type Action**

1. In the Process Manager portal, on the **Admin** tab, click **Data > Process Type Actions**.

2. On the **Process Type Action** page, add an action to one of the following:

   - **Incident Management Process View page**: To the right of **Incident Management**, click the **Process Type Actions** symbol (orange lightning) and then click **Add Action**.

   - **Change Management Process View page**: To the right of **Change Management**, click the **Process Type Actions** symbol (orange lightning) and then click **Add Action**.
3. In the **Add Process Type Action** dialog box, type the following information about the action and make any of the following selections:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Name</td>
<td>Type the name of your <strong>Process Type Action</strong>.</td>
</tr>
<tr>
<td>Action URL</td>
<td>Type the URL of the .asmx page for the process. If your <strong>Process Type Action</strong> is a published workflow project, set this value to the URL of the process as it appears in IIS.</td>
</tr>
<tr>
<td>Height</td>
<td>Type the height (in pixels) of the <strong>Process Type Action</strong> dialog box that opens in the <strong>Process View</strong> page.</td>
</tr>
<tr>
<td>Width</td>
<td>Type the width (in pixels) of the <strong>Process Type Action</strong> dialog box that opens in the <strong>Process View</strong> page.</td>
</tr>
<tr>
<td>Is Contact Action</td>
<td>Set the action as a contact action. If you select this property, your <strong>Process Type Action</strong> appears on the <strong>Process View</strong> page for any user who has contact permissions for the process.</td>
</tr>
<tr>
<td>Is View Action</td>
<td>Set the action as a view action. If you select this property, your <strong>Process Type Action</strong> appears on the <strong>Process View</strong> page for any user who has view permissions for the process.</td>
</tr>
<tr>
<td>Is Edit Action</td>
<td>Set the action as an edit action. If you select this property, your <strong>Process Type Action</strong> appears on the <strong>Process View</strong> page for any user who has edit permissions for the process.</td>
</tr>
<tr>
<td>Is Admin Action</td>
<td>Set the action as an admin action. If you select this property, your <strong>Process Type Action</strong> appears on the <strong>Process View</strong> page for any user who has Admin permissions for the process.</td>
</tr>
<tr>
<td>Only Valid when process is active</td>
<td>Set the action to only be available on the <strong>Process View</strong> page when the incident or the change request is active. If you select this property, once ticket is in the Closed State, your <strong>Process Type Action</strong> no longer appears on its <strong>Process View</strong> page.</td>
</tr>
<tr>
<td>Open in New Window</td>
<td>Set the process to open in a new window.</td>
</tr>
</tbody>
</table>

4. Click **Save**.
Editing Process Type Actions

Process Type Actions let you quickly do external processes directly from the incident and the change request tickets' Process View pages. ServiceDesk provides a set of default Process Type Actions.

See “About Process Type Actions on the Process View pages” on page 106.

You can edit Process Type Actions. For example, you can adjust the dimensions of the action's dialog box from where the technicians do a Google search directly from the Process View page.


To edit a Process Type Action

1. In the Process Manager portal, on the Admin tab, click Data > Process Type Actions.

2. On the Process Type Action page, edit an action on one of the following:

   - **Incident Management Process View page**
     Expand Incident Management.
     To the right of the Process Type Action that you want to edit, click the Actions symbol (orange lightning) and then click Edit Action.

   - **Change Management Process View page**
     Expand Change Management.
     To the right of the Process Type Action that you want to edit, click the Actions symbol (orange lightning) and then click Edit Action.
3. In the **Edit Process Type Action** dialog box, edit the following information about the action and change any of the following selection, as necessary:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Name</strong></td>
<td>Edit the name of your Process Type Action.</td>
</tr>
<tr>
<td><strong>Action URL</strong></td>
<td>Edit the URL of the .asmx page for the process.</td>
</tr>
<tr>
<td></td>
<td>If your Process Type Action is a published workflow project, set this value to the URL of the process as it appears in IIS.</td>
</tr>
<tr>
<td><strong>Height</strong></td>
<td>Adjust the height (in pixels) of the Process Type Action dialog box that opens in the Process View page.</td>
</tr>
<tr>
<td><strong>Width</strong></td>
<td>Adjust the width (in pixels) of the Process Type Action dialog box that opens in the Process View page.</td>
</tr>
<tr>
<td><strong>Is Contact Action</strong></td>
<td>Set the action as a contact action.</td>
</tr>
<tr>
<td></td>
<td>If you select this property, your Process Type Action appears on the Process View page for any user who has contact permissions for the process.</td>
</tr>
<tr>
<td><strong>Is View Action</strong></td>
<td>Set the action as a view action.</td>
</tr>
<tr>
<td></td>
<td>If you select this property, your Process Type Action appears on the Process View page for any user who has view permissions for the process.</td>
</tr>
<tr>
<td><strong>Is Edit Action</strong></td>
<td>Set the action as an edit action.</td>
</tr>
<tr>
<td></td>
<td>If you select this property, your Process Type Action appears on the Process View page for any user who has edit permissions for the process.</td>
</tr>
<tr>
<td><strong>Is Admin Action</strong></td>
<td>Set the action as an admin action.</td>
</tr>
<tr>
<td></td>
<td>If you select this property, your Process Type Action appears on the Process View page for any user who has Admin permissions for the process.</td>
</tr>
<tr>
<td><strong>Only Valid when process is active</strong></td>
<td>Set the action to only be available on the Process View page when the incident or the change request is active.</td>
</tr>
<tr>
<td></td>
<td>If you select this property, once ticket is in the Closed State, your Process Type Action no longer appears on its Process View page.</td>
</tr>
<tr>
<td><strong>Open in New Window</strong></td>
<td>Set the process to open in a new window.</td>
</tr>
</tbody>
</table>

4. Click **Save**.
Deleting Process Type Actions

Process Type Actions let you quickly do external processes directly from the incident and the change request tickets’ Process View pages. ServiceDesk provides a set of default Process Type Actions.

You can delete obsolete or unused Process Type Actions from the Incident Management and Change Management Process View pages.

To delete a Process Type Action

1. In the Process Manager portal, on the Admin tab, click Data > Process Type Actions.

2. On the Process Type Action page, delete an action on one of the following:

<table>
<thead>
<tr>
<th>Incident Management Process View page</th>
<th>Change Management Process View page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand Incident Management.</td>
<td>Expand Change Management.</td>
</tr>
<tr>
<td>To the right of the Process Type Action that you want to delete, click the Actions symbol (orange lightning) and then click Delete Action.</td>
<td>To the right of the Process Type Action that you want to delete, click the Actions symbol (orange lightning) and then click Delete Action.</td>
</tr>
</tbody>
</table>

3. In the confirmation dialog box, click OK.

See “Editing Process Type Actions” on page 110.
See “Adding Process Type Actions” on page 107.
Performing common actions in the Process Manager portal

This chapter includes the following topics:

- Setting permissions
- Picking a user
- Capturing a screen image
- Screen Capture icons
- Changing your password

Setting permissions

Throughout the Process Manager portal, an administrator or other user who has the appropriate permissions can set permissions to provide access to various items. For example, permissions can be set on documents, knowledge base articles, Service Catalog categories, reports, portal pages, and schedules.

To set permissions

1. Access the Permissions page or tab.
   This step might vary depending on your task. Typically, you click a Permissions tab on the item’s editing page.

2. On the Permissions page, click Add New Permission.

3. In the Permission Type drop-down list, select one of the following:
4 Type the name of the entity to apply the permissions to.
You can also click **Pick** to select the appropriate entity.

5 If you clicked **Pick**, select a specific entity as follows:
   - In the **User Picker** dialog box, select a user.
     See “Picking a user” on page 114.
   - In the **Group Picker** dialog box, provide the group name, click **Search**, and then click the **Select** link to the right of the appropriate group.
   - In the **Permission Picker** dialog box to the right of the appropriate permission, click the **Select** link.
   - In the **Organization Picker** dialog box, expand the organizations if necessary, and then select an organization.

6 To set permission for a single action, in the appropriate column, click the red X symbol to change it to a green check mark symbol.

7 To set the same permission for all the actions, select one of the following options under the appropriate column:
   - **Allow All**
   - **Deny All**
   - **Inherit All**

8 Click **Add**.

9 To set permissions for another entity, repeat step 2 through step 8.

10 When you finish setting permissions, on the **Permissions** page, click **Save**.

---

**Picking a user**

As you use the Process Manager portal, you occasionally need to select a user. For example, you select a user to grant permissions to, reassign a ticket to, or add to a group.

You search for and select a user in the **User Picker** dialog box.
To pick a user

1. In the Process Manager portal, at the point where you must select a user, click **Pick**.

   Typically, this location is the **Add User** dialog box.

2. In the **User Picker** dialog box, provide the criteria for a user search.

   For example, you can type part of the user’s email address or name, or select the group or organization to which the user belongs.

3. Click **Search**.

4. In the **User Picker** dialog box to the right of the appropriate user, click the **Select** link.

   At this stage, the user is not added yet.

5. When you are returned to the point where you selected the **Pick** option, click **Add** to add the user that you selected.

6. To add more users, repeat step 1 through step 5.

7. When you finish adding users, click **Close**.

Capturing a screen image

ServiceDesk provides a Screen Capture utility that lets users capture images of their computer screens.

The Screen Capture utility is available from the Windows **Start** menu and from an incident. For example, a user can capture an error message and attach it to an incident.

Before you can capture a screen image, the Screen Capture Utility must be installed on your computer.
Capturing a screen image

1. Open the **Screen Capture** window in any of the following ways:

   - On the **Create a New Incident** page:
     - Click **Take Screenshot**.
     - See “Reporting an incident in ServiceDesk” on page 139.
   - On the **Reason for Re-Opening Issue** page:
     - Click **Take Screenshot**.
   - On the Windows **Start menu**:
     - Click **Symantec > Workflow Designer > Tools > Screen Capture Util**.

2. (From an incident only) If the **Screen Capture** window does not open automatically, on the **Screen Capture** page, click one of the following links:

   - **To install the Screen Capture Utility, please click here.** Installs the Screen Capture utility if it is not installed.
   - **If the Screen Capture Utility does not open automatically, please click here.** Opens the **Screen Capture** window.
     - If the window does not open, then it probably is not installed on your computer.

3. In the **Screen Capture** window, select one of the following options to capture the image:

   - **Capture Region**
     - Capture a specific part of the screen, which you select. For example, you might select an error message or a portion of the screen that shows the options you selected before an error occurred.
   - **Capture Screen**
     - Captures the entire screen, minus the **Screen Capture** window.
   - **Capture Delayed**
     - Lets you set an amount of time to wait before the image is captured.

4. (Optional) Use any of the screen capture icons to edit the image as needed.
   - See “**Screen Capture icons**” on page 117.
5 When the image is finished, select one of the following icons:

- **Send to Process Manager**
  
  If you accessed the Screen Capture window from an incident, this option places the image on the Screen Capture page.
  
  When you click **Completed** on the Screen Capture page, the file is saved and attached to the incident.

- **Save to File**
  
  Displays the **Save As** dialog box, where you can type a name for the file, and then click **Save**.
  
  You can attach the saved file to the current process ticket, to any other process ticket, or to any other document.

- **Copy to Clipboard**
  
  Copies the captured image to the clipboard so you can paste it into a different image or any other document.

6 When you finish the capture, you can close the Screen Capture window to return to your starting point. Click the red square in the upper right corner.

### Screen Capture icons

The Screen Capture window lets you capture an image on your computer screen so you can attach it to a task or a process ticket. The icons that appear on this page represent the screen capture operations that you can perform. Some of these icons appear only during specific operations. For example, the editing icons do not appear until you capture a screen image.

See “Capturing a screen image” on page 115.

#### Table 8-1: Options in the Screen Capture window

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Add Note](image) | **Add Note**  
Lets you add text to a captured image.  
When you click this symbol, additional icons appear at the left of the Screen Capture window to let you format the note. |
| ![Panning arrows](image) | Panning arrows let you move the image up, down, left, and right within the Screen Capture window when the image is larger than the window. |
### Table 8-1 Options in the **Screen Capture** window (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Capture Delayed Icon" /></td>
<td><strong>Capture Delayed</strong>&lt;br&gt;Lets you set an amount of time to wait before the image is captured.</td>
</tr>
<tr>
<td><img src="image" alt="Capture Region Icon" /></td>
<td><strong>Capture Region</strong>&lt;br&gt;Captures a specific part of the screen, which you select. For example, you might select an error message or a portion of the screen that shows the options you selected before an error occurred.</td>
</tr>
<tr>
<td><img src="image" alt="Capture Screen Icon" /></td>
<td><strong>Capture Screen</strong>&lt;br&gt;Captures the entire screen, minus the <strong>Screen Capture</strong> window.</td>
</tr>
<tr>
<td><img src="image" alt="Change Border Color Icon" /></td>
<td><strong>Change Border Color</strong></td>
</tr>
<tr>
<td><img src="image" alt="Change Border Width Icon" /></td>
<td><strong>Change Border Width</strong></td>
</tr>
<tr>
<td><img src="image" alt="Change Fill Icon" /></td>
<td><strong>Change Fill</strong></td>
</tr>
<tr>
<td><img src="image" alt="Change Font Icon" /></td>
<td><strong>Change Font</strong></td>
</tr>
<tr>
<td><img src="image" alt="Change Font Color Icon" /></td>
<td><strong>Change Font Color</strong></td>
</tr>
<tr>
<td><img src="image" alt="Copy to Clipboard Icon" /></td>
<td><strong>Copy to Clipboard</strong>&lt;br&gt;Lets you paste the copied image into any other application.</td>
</tr>
<tr>
<td><img src="image" alt="Crop Image Icon" /></td>
<td><strong>Crop Image</strong></td>
</tr>
<tr>
<td><img src="image" alt="Draw Rectangle Icon" /></td>
<td><strong>Draw Rectangle</strong></td>
</tr>
<tr>
<td><img src="image" alt="Open File Icon" /></td>
<td><strong>Open File</strong></td>
</tr>
</tbody>
</table>
### Table 8-1 Options in the Screen Capture window (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Pan Image](image) | **Pan Image**  
Lets you move the image around within the Screen Capture window. |
| ![Paste](image) | **Paste**  
Lets you paste the contents of your Clipboard into the image. Use this option with the Copy to Clipboard option. |
| ![Redo](image) | **Redo**  
This icon is available only after you undo a change in the captured image. |
| ![Save to File](image) | **Save to File** |
| ![Send to Process Manager](image) | **Send to Process Manager** |
| ![Undo](image) | **Undo**  
This icon is available only after you make a change in the captured image. |

## Changing your password

ServiceDesk users who have permission to change their passwords can do so in the Process Manager portal.

**Note:** If you use Active Directory to authenticate the users who log on to ServiceDesk, those users cannot change their passwords in the Process Manager portal.

### To change your password

1. In the upper right of the Process Manager portal, click **Account**.
2. On the account page, at the far right of the **User Information** title bar, click the **Actions** symbol (orange lightning), and then click **Change Password**.
3. In the **Change Password** dialog box, type the following information:
   - Your current password
   - Your new password
- Your new password again to confirm the new password

4. Click **Change Password**.
This chapter includes the following topics:

- About the Active Directory self-service catalog
- Requesting an Active Directory password reset
- Requesting access to an Active Directory network share

About the Active Directory self-service catalog

The Active Directory Self Service Catalog provides end users with a collection of request processes for interacting with the Active Directory domain. The associated workflow project files are also available for each Active Directory self-service catalog request.

With the Active Directory self-service catalog, you can perform the following actions in the Process Manager portal:

- Request an Active Directory password reset
  See “Requesting an Active Directory password reset” on page 121.
- Request access to an Active Directory network share
  See “Requesting access to an Active Directory network share ” on page 123.

Requesting an Active Directory password reset

Reset Password lets you submit a request for an end user in need of an Active Directory password reset. Reset Password is an Active Directory self-service catalog item.
See “About the Active Directory self-service catalog” on page 121.

**Note:** The manager - direct report relationship must be set in Active Directory. If this relationship is not set, the request fails.

---

**To request an Active Directory password reset**

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Request** page, under **Service Catalog**, click **IT Services**.
3. Click **Reset Password**.
4. In the **Specify AD Server** dialog box, in the drop-down list, select the Active Directory server to which you want to connect.
5. In the **Request Form** dialog box, provide the following information as follows:
   - **User**: Type the name of the user who needs a password reset.
   - **Notification Method**: Select one of the following notification methods:
     - **Email the user's manager for approval**
       An email is sent to the user’s manager to the email address on file in Active Directory.
     - **Call the user**
       The designated Active Directory administrator contacts the user at the phone number on file in Active Directory.
       If the administrator fails to make the contact by phone, the manager email runs next.
6. When you are finished, click **Continue**.
7. In the **Confirm Request** dialog box, verify the request and the user details.
8. When you are finished, click **Confirm**.
9. In the **Thank You** dialog box, note the request ID.
10. Click **Close**.

See “Requesting access to an Active Directory network share” on page 123.
Requesting access to an Active Directory network share

Request Access to Network Share lets you create a request for permissions to a shared folder that is on an Active Directory domain. Request Access to Network Share is an Active Directory self-service catalog item. See “About the Active Directory self-service catalog” on page 121.

To request access to an Active Directory network share

1. In the Process Manager portal, click Submit Request.
2. On the Submit Request page, under Service Catalog, click IT Services.
3. Click Request Access to Network Share.
4. In the Specify AD Server dialog box, in the drop-down list, select the Active Directory server to which you want to connect.
5. In the Request Form dialog box, under Recipient Information, select one of the following options:

<table>
<thead>
<tr>
<th>Request for</th>
<th>The Requester and the Recipient fields are pre-populated with the same name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Myself</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>■ Click Search for User.</td>
</tr>
<tr>
<td></td>
<td>■ In the Select User dialog box, search for and select the user.</td>
</tr>
<tr>
<td></td>
<td>The Recipient field is populated with the selected user’s name.</td>
</tr>
</tbody>
</table>

6. In the Request Details section, provide the following information:

<table>
<thead>
<tr>
<th>Name of Shared Folder</th>
<th>In the drop-down list, select the shared folder to which you want access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Permissions</td>
<td>In the drop-down list, select the type of permissions that you want for the folder</td>
</tr>
<tr>
<td>Needed by Date</td>
<td>In the drop-down list, select the date by which you need access to the shared folder</td>
</tr>
<tr>
<td>Reason for Request</td>
<td>Type the reason that you need access to the shared folder.</td>
</tr>
</tbody>
</table>
7 When you are finished, click **Continue**.

8 In the **Review Request** dialog box, verify the request details.

9 When you are finished, click **Submit**.

10 In the **Thank You** dialog box, note the request ID.

11 Click **Close**.

See “**Requesting an Active Directory password reset**” on page 121.
Managing incidents

- Chapter 10. Introducing Incident Management
- Chapter 11. Submitting incidents (user method)
- Chapter 12. Submitting incidents (technician method)
- Chapter 13. Creating incidents from user emails
- Chapter 14. Resolving incidents
- Chapter 15. Creating incident subtasks
- Chapter 16. Managing incident service queues
- Chapter 17. Managing email templates
- Chapter 18. Routing and escalating incidents
Introducing Incident Management

This chapter includes the following topics:

- About Incident Management
- About the Incident Management process
- Incident statuses
- Roles in Incident Management
- Sources of ServiceDesk incidents
- Email notifications from Incident Management
- Process View page for incidents

About Incident Management

Incident Management is one of the core ITIL-based processes, and one that ServiceDesk users work with the most frequently. With the Incident Management process, users can manage and quickly resolve incidents themselves, and analysts can manage, track, and prioritize issues.

See “What you can do with ServiceDesk” on page 24.

The goal of Incident Management is to recover from incidents and restore service to users as quickly as possible.

Incident Management includes the following key features:

- The Automation rules designer lets you execute actions based on 13 potential decision points.
The 13 decision points, or rulesets, let you create rules for routing, email, and other actions. When the ruleset is initiated, the rules execute automatically.

In addition to the 13 default rulesets, you can create your own rulesets based on your organization's requirements.

An intuitive form for users to submit incidents from the self-service portal.

The ability to include information about the user and the user's assets in the incident data in the incident form.

The inclusion of specialized tasks that help the technician diagnosing the issue and provide opportunities to either resolve or escalate the issue.

Opportunities to use the knowledge base to help the technician resolve an incident and to provide additional information to the user.

The inclusion of the user in the Incident Management process, by letting the user decide if an issue is resolved to their satisfaction. The user can also provide feedback on their service experience.

The Incident Management process provides information to the other ServiceDesk processes as follows:

- A collection of incidents that can be used in Problem Management to identify root causes of incidents. When the root causes are identified, they can be resolved to prevent further incidents from occurring.

- Information from the incidents, which is used in Change Management to determine how to standardize methods and procedures for efficient handling of all changes.

- Serves as a source of information for future knowledge base articles.

See “About the Incident Management process” on page 128.

About the Incident Management process

The goal of Incident Management is to recover from incidents and return the user to an operational state as quickly as possible.

ServiceDesk can be configured to send email notifications to users and other workers when certain actions are taken in the Incident Management process.

See “Email notifications from Incident Management” on page 133.
### Incident Management process

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>An incident is submitted.</td>
<td>An incident is a ServiceDesk ticket that reports an issue. Incidents can originate from user help calls or emails, support technicians, and external systems. See “Sources of ServiceDesk incidents” on page 133.</td>
</tr>
<tr>
<td>Step 2</td>
<td>The incident data is analyzed and assigned to a support technician for resolution.</td>
<td>This step is an internal process. When the incident is submitted, the following actions occur: ■ Its data is stored. ■ Any configuration items that pertain to the incident are noted. For example, a specific computer or printer can be associated with the incident. ■ Its priority is calculated. ■ Its priority is evaluated and it is assigned to the Default Incident Queue that is associated with the Support Group. If assignment rules have been created, then they are evaluated to determine where to assign the incident.</td>
</tr>
<tr>
<td>Step 3</td>
<td>A support technician works the incident.</td>
<td>The incident appears in the task list for the technician, group, or organization. If the incident is assigned to a specific technician, the technician receives an email notification. See “Resolving an incident from the advanced incident form” on page 169. See “Resolving an incident from a task” on page 170. In addition to viewing and resolving the incident, the technician can perform other actions. Examples of incident actions are as follows: ■ Reassign the ticket. ■ Set ownership of the ticket. ■ Edit the incident. ■ Manage the related configuration items. ■ Search the Microsoft TechNet website. ■ Manage the service queues. ■ Manage the subtask templates. ■ Reopen the incident. ■ Search the knowledge base. ■ Create a bulletin board entry. ■ Submit a knowledge base article.</td>
</tr>
</tbody>
</table>
### Table 10-1 Incident Management process (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>(Optional) A support technician escalates the incident.</td>
<td>An incident can be escalated when it is close to missing its required resolution date or when it must be resolved at a higher level. A support technician can escalate an incident from the incident’s Process View page. If routing rules are defined for escalating an incident, any incident that meets those criteria is escalated automatically. See “About incident routing and escalation” on page 201.</td>
</tr>
<tr>
<td>Step 5</td>
<td>The incident is resolved.</td>
<td>The support technician can resolve the incident or another process can resolve the incident automatically. For example, if the incident is associated with a change request and the change request is closed, the incident is resolved automatically. This type of automatic resolution is called a cascading closure. In some case, other processes might need to occur before the incident can be resolved. For example, when an incident has subtasks, one or more support technicians must resolve the subtasks before the incident is resolved.</td>
</tr>
<tr>
<td>Step 6</td>
<td>The user reviews the resolution and confirms or re-opens the incident.</td>
<td>The incident resolution appears in the user's task list and the user receives an email notification. The user views the incident’s history, comments, and other information. If the support technician provided instructions for self-service or for testing, the user follows the instructions. If the resolution fixes the issue, the user confirms the fix and provides customer feedback. The incident is marked as Closed. See “Reviewing and closing a resolved incident and submitting feedback on an incident resolution” on page 148. If the resolution does not fix the problem, the user re-opens the incident. The incident is re-assigned. See &quot;Reopening an incident&quot; on page 149. If the user does not respond within three days, the incident’s status is changed from Resolved to Closed. <strong>Note:</strong> The Incident Management verification period is set to three days and cannot be changed.</td>
</tr>
</tbody>
</table>
Table 10-1  Incident Management process (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 7 | (Optional) The support technician performs the post-resolution activities. | The user’s response appears in the support technician’s task list and the technician receives an email notification. If the user closes the incident, the support technician can take any of the following actions:  
  - Submit the resolution details to the knowledge base team to be integrated into an article or FAQ.  
  - Re-open the incident.  
    See “Reopening an incident” on page 149.  
    If the user or the technician re-opens the incident, the resolution steps are repeated. |

Incident statuses

The incident status accurately reports the progression and outcome of the stages of the Incident Management process. The percentage represents the level of completion that the process has reached. For example, if the status percentage is 60, it means that the process is 60 percent complete.

The status and percentage appear in several places in the Process Manager portal. For example, they appear at the top of the ticket’s Process View page.

Table 10-2  Incident statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Completion percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received</td>
<td>The incident was submitted and is ready to be worked.</td>
<td>10%</td>
</tr>
<tr>
<td>Assigned</td>
<td>The incident was assigned to a designated person or group for resolution.</td>
<td>20%</td>
</tr>
<tr>
<td>Hold</td>
<td>The incident is scheduled for later and is placed on hold. Typically, this status means that more research or analysis needs to be performed.</td>
<td>25%</td>
</tr>
<tr>
<td>Resolved</td>
<td>A resolution for the entire incident was provided and the incident is ready for the user’s approval. The resolution must apply to the entire incident, not to a single subtask.</td>
<td>80%</td>
</tr>
</tbody>
</table>
Table 10-2  Incident statuses (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Completion percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed</td>
<td>All manual actions and automated actions within the process are complete and the incident is closed.</td>
<td>100%</td>
</tr>
</tbody>
</table>

Roles in Incident Management

ServiceDesk employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes.

The roles in the Incident Management process are tasked with submitting incidents and resolving them as quickly as possible.

See “About the Incident Management process” on page 128.

Table 10-3  Roles in Incident Management

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user can be anyone in or outside the organization who submits an incident. The user typically has limited access to the ServiceDesk processes.</td>
</tr>
<tr>
<td>Support technician</td>
<td>The support technician is a worker in the organization’s support department who manages incidents. Organizations can set up their own levels of technicians. For example, first-level technicians can monitor incoming incidents, take support calls, and resolve incidents. If the problem cannot be resolved immediately or if it requires research or escalation, the technician can assign the incident to a second-level technician. The second-level technicians can perform incident analysis and resolve or escalate incidents. An incident can be assigned to a user, group, or organization. When an incident is assigned to a group or organization, it is added to a queue from which workers can select it. Some organizations might use a third level of support. Typically this level represents an external vendor or a manufacturer of hardware or software.</td>
</tr>
</tbody>
</table>
Sources of ServiceDesk incidents

The creation of an incident triggers the Incident Management process. An incident can originate from several sources.

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Manager portal</td>
<td>A user reports an issue by creating an incident in the Process Manager portal.  See “Reporting an incident in ServiceDesk” on page 139.</td>
</tr>
<tr>
<td>User emails</td>
<td>A user can send an email to the ServiceDesk inbox and if it passes certain checks, it becomes an incident. See “Submitting an incident by email” on page 141.</td>
</tr>
<tr>
<td>Support technicians</td>
<td>Typically, a support technician creates an incident in response to a request from a user, either by telephone or email. See “About advanced incidents” on page 151.</td>
</tr>
<tr>
<td>External systems</td>
<td>Your organization can make a web service call to Incident Management and pass in the data that is required to create an incident in ServiceDesk. For example, you might create incidents from Microsoft SharePoint, Microsoft InfoPath, Lotus Notes, Microsoft Systems Management Server (SMS), Adobe LifeCycle, and HP OpenView.</td>
</tr>
</tbody>
</table>

Email notifications from Incident Management

You can send email notifications about incident events. Any action that is taken to create or work an incident ticket can be used as a trigger. You must configure Incident Management to send email notifications. Email notifications for Incident Management are handled through the Process Automation rules.

See “About the Incident Management process” on page 128.

For example, you can create a rule that sends an email notification to the members of the service queue when an incident is submitted.

You can set up the following types of notifications:

- Automatic notifications
  - You configure the automation rules that send out email notifications.
- Manual notifications
You send an email from the incident's Process View page.

You can track all email communications in the history of the ticket. For the emails to be included in the history of the ticket, you must add the reply code to the email template.

Some examples of incident events that you can use to trigger email notifications are as follows:

<table>
<thead>
<tr>
<th>Event</th>
<th>Email recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>An incident is submitted.</td>
<td>The submitter or the user on whose behalf someone submitted the incident</td>
</tr>
<tr>
<td>An incident is assigned to a specific service queue</td>
<td>The members of the queue</td>
</tr>
<tr>
<td>An incident or subtask is assigned to a specific support technician or group.</td>
<td>The assigned technician or group members</td>
</tr>
</tbody>
</table>

The first step is to create your email templates.

See “Creating email templates for Incident Management” on page 195.

The next step is to configure your email notification rules.


**Process View page for incidents**

The Process View page is the primary interface for working a task. The Process View page appears when you select a task from your Task List or from another list in the Process Manager portal.

The default sections on the Process View page are similar for all types of tasks. If your organization uses customized Process View pages, your views might look different.

See “About the Process View page” on page 93.

In addition to the common actions that you can perform for all tasks, the incident Process View page contains additional, incident-specific actions. The actions that are available depend on your permissions and the state of the incident. For example, if the incident has been escalated to a higher level, the Resolve Incident action is no longer available to you.

Groups of actions on an incident’s Process View page:

- **Incident**
  
  See Table 10-5.
- Incident Hold Task
  This section appears only in an incident that has been postponed.
  See Table 10-6.

- Change and Problem Management Tools
  See Table 10-7.

- Smart Tasks
  See Table 10-8.

- Process Actions
  See Table 10-9.

### Table 10-5 Incident actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reassign Ticket</td>
<td>Lets you assign an incident to a different service queue and choose whether to remove or retain any existing assignments.</td>
</tr>
<tr>
<td>Set Ownership</td>
<td>Lets you assign an incident to someone else or take over ownership. You can also remove the incident from a service queue.</td>
</tr>
<tr>
<td>Work Incident</td>
<td>Lets you begin the incident resolution process.</td>
</tr>
<tr>
<td></td>
<td>Also lets you change the incident’s details, including any extended classifications.</td>
</tr>
<tr>
<td></td>
<td>See “Resolving an incident from a task” on page 170.</td>
</tr>
<tr>
<td>Work Tasks Assigned to Others</td>
<td>Lets you work on a task that is assigned to someone else if you have the appropriate permissions.</td>
</tr>
<tr>
<td></td>
<td>For example, a level-one support technician starts to work on an incident but leaves for lunch before the incident is resolved. The incident must be resolved before the technician is due to return. Another worker who is at the same level or higher can open the incident, select this option, and resolve the incident.</td>
</tr>
</tbody>
</table>

### Table 10-6 Incident Hold Task actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove from Hold</td>
<td>Lets you reopen an incident that has been postponed so that it can be worked.</td>
</tr>
<tr>
<td></td>
<td>See “Reopening a postponed incident” on page 173.</td>
</tr>
</tbody>
</table>
### Table 10-7 Change and Problem Management Tools

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create or Relate to a Problem</td>
<td>Lets you create a problem ticket based on the incident if the incident represents a recurring issue. See “Creating a problem ticket from an incident” on page 174. Lets you search for and view existing problem tickets. Lets you associate the incident with an existing problem ticket, if you find a problem ticket that addresses your incident.</td>
</tr>
<tr>
<td>Find Recent Changes</td>
<td>Displays any change requests that were completed within the last 14 days. The support technician can use this list to determine whether the current issue has been fixed.</td>
</tr>
<tr>
<td>Request Change</td>
<td>Lets you create a change request based on the incident if the incident represents a recurring issue. See “Creating a change request from an incident” on page 176.</td>
</tr>
<tr>
<td>View Forward Schedule Change</td>
<td>Displays the Forward Schedule of Change. The ITIL Forward Schedule of Change (FSC) is an integrated view of all the approved changes and their release dates. See “Calendar page” on page 57. A support worker might view the FSC to determine if any scheduled activity might be the cause of an incident. For example, several users report that they cannot access email. By viewing the FSC, the support technician learns that the organization's email service is down for scheduled maintenance. The support technician can tell the users why the email is not available and when they can expect the service to be restored.</td>
</tr>
</tbody>
</table>

### Table 10-8 Smart Tasks

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach Process</td>
<td>Lets you add additional incidents, changes, and problems to this incident.</td>
</tr>
<tr>
<td>Hold Management</td>
<td>Lets you change the task’s due date. When you postpone an incident, it is removed from the incident service queue until the scheduled date arrives. See “Scheduling an incident for later (postponing)” on page 172.</td>
</tr>
<tr>
<td>Manage Subtasks</td>
<td>Lets you create one or more subtasks to record, assign, and track any additional actions that are required to resolve the incident. See “Creating a subtask for an incident” on page 180.</td>
</tr>
<tr>
<td>Suggest Self Service</td>
<td>Lets you direct the submitter to a knowledge base article or a Service Catalog option that contains resolution instructions.</td>
</tr>
</tbody>
</table>
### Table 10-8  **Smart Tasks (continued)**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Previous Submissions</td>
<td>Displays the submitter's past incidents. Viewing the user's submissions can let you see trends for the user or gather the history that might help analyze the current incident.</td>
</tr>
</tbody>
</table>

### Table 10-9  **Process Actions**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Incident</td>
<td>Lets you edit all of the incident details from within one form, including any extended classifications.</td>
</tr>
<tr>
<td>Manage Related Configuration Items</td>
<td>Opens the <strong>Add Equipment</strong> page, which lets you add or delete the equipment that is related to the process. You can also access the quick tools for a piece of equipment.</td>
</tr>
<tr>
<td>Search KB</td>
<td>Lets you search the knowledge base for an article that is related to the ticket and then attach the article.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Searching the knowledge base</strong>” on page 339.</td>
</tr>
<tr>
<td>Create Bulletin Board Entry</td>
<td>Lets you request a bulletin board entry.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>About the Bulletin Board</strong>” on page 309.</td>
</tr>
<tr>
<td>Submit KB</td>
<td>Lets you submit a knowledge base article to add to the knowledge base.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>About Knowledge Management</strong>” on page 307.</td>
</tr>
<tr>
<td>Search Technet</td>
<td>Lets you search this external database for any information that might relate to the incident or its resolution.</td>
</tr>
<tr>
<td>Manage Service Queues</td>
<td>Lets you set up and manage your service queues.</td>
</tr>
<tr>
<td>Manage Subtask Templates</td>
<td>Lets you set up and manage subtask templates.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>About subtask templates</strong>” on page 180.</td>
</tr>
<tr>
<td>Reopen Incident</td>
<td>Lets you reopen a closed incident.</td>
</tr>
<tr>
<td>Search Knowledge Base</td>
<td>Lets you search the knowledge base for an article that is related to the ticket and then attach the article.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Searching the knowledge base</strong>” on page 339.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Send Email | Lets you send an email message regarding the ticket.  
See “Sending an email from a ticket's Process View page” on page 375.  
The Send Email action does not appear until you create your Incident Management email templates.  
See “Creating email templates for Incident Management” on page 195. |
Submitting incidents (user method)

This chapter includes the following topics:

- Reporting an incident in ServiceDesk
- Submitting an incident by email
- Create a New Incident page
- Attaching a file to a new incident
- Attach File to Incident dialog box
- Capturing a screen image in an incident
- Finding and reviewing your incidents
- Confirming an incident’s resolution
- Reviewing and closing a resolved incident and submitting feedback on an incident resolution
- Reopening an incident

**Reporting an incident in ServiceDesk**

A user who has a problem and cannot find a resolution in the organization’s knowledge base can create an incident to report the problem. The user creates the incident in ServiceDesk using the general incident form. This form contains the minimum amount of information that is required to create an incident.

When you create an incident, you can perform the following actions:
- Attach a file to the incident.  
  See “Attaching a file to a new incident” on page 144.
- Capture a screen image and attach it to the incident. 
  See “Capturing a screen image” on page 115.

If your ServiceDesk administrator allows it, you can also submit an incident by email.

See “Submitting an incident by email” on page 141.

**To submit an incident in ServiceDesk**

1. In the Process Manager portal, click *Submit Request*.

2. On the *Submit Request* page, in the *New Request* section, under *Service Catalog*, click *IT Services* and then on the right side of the page, click *Report Incident*.

3. In the *Create a New Incident* dialog box, provide the necessary information about the incident.

   See “Create a New Incident page” on page 142.

4. (Optional) To create an incident on behalf of another user, to the right of the *Who does this issue affect?* field, click *Search for User*.

   Search for and add the user.

5. When you are finished, click *Continue*.

   See “Create a New Incident page” on page 142.

6. To search the knowledge base or Service Catalog for any articles or self-service items that are related to your problem, click *Search the Knowledge Base*.

   See “Searching the knowledge base” on page 339.

   After you search knowledge base, select one of the following options:

   - **Answer Found**  
     If you found an answer to your problem in the knowledge base, this option lets you exit the incident submission process.

   - **Continue with Incident**  
     If you did not find an answer to your problem in the knowledge base, this option lets you return to the *Create a New Incident* page.
7 If ServiceDesk has a record of the equipment that is assigned to you, the Select Equipment page appears. Select any equipment that this issue affects, and then click Continue.

For example, if the incident involves a printer jam, you can select the printer that is jammed.

8 If you selected Blocking Critical Business as the urgency, on the Critical Business Details page, provide more information about the urgency, and then click Continue.

9 If the title or description of your incident matches that of a knowledge base article, the process suggests the articles that might provide a resolution. Your options are the same as in step 6.

10 On the Review Request page, verify that the information is correct, and then click Submit.

If the information is not correct, you can click Edit to return to the incident.

11 When the Thank You dialog box opens, make a note of the incident ID.

This number identifies the incident in any future communications.

12 Click Close to exit the incident submission process or Start Another to open a new incident.

Submitting an incident by email

A user who has a problem and cannot find a resolution in the organization’s knowledge base can report the incident by email. The incident is created automatically and assigned to a service queue.

Your ServiceDesk administrator determines whether this feature is available.

When you create a new email message to report an incident, be sure to include the following information:
To submit an incident by email

- Create and send an email message that contains the following information:
  
  **Address**  
  Use the address that your support organization provides.

  **Subject**  
  Include the phrase **New Incident**.

  **Message body**  
  Provide details about the issue or provide any other information that your support organization requires. You might be provided with an email template to follow.

  If you leave the message body blank, this email might be classified as junk.

Create a New Incident page

This page lets you create an incident.

See “Reporting an incident in ServiceDesk” on page 139.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who does this issue affect?</strong></td>
<td>Lets you specify whether this issue affects you or someone else.</td>
</tr>
<tr>
<td><strong>Search For User</strong></td>
<td>Opens the <strong>Select User</strong> dialog box, where you can search for, view, and select the person who this issue affects.</td>
</tr>
<tr>
<td><strong>What is your issue?</strong></td>
<td>Lets you type a brief description of the issue. Make this description as specific as possible. For example, instead of “email problem,” you might type “Cannot receive external email.” This description becomes the incident title, which identifies this incident in any incident lists in the Process Manager portal.</td>
</tr>
<tr>
<td><strong>Details that might help resolve this issue</strong></td>
<td>Lets you type additional information to describe the issue. For example, you might describe the steps to reproduce the issue or provide more information about what happened. The toolbar that appears in this section provides common text formatting tools.</td>
</tr>
<tr>
<td><strong>Needed By Date</strong></td>
<td>Lets you select the date on which this issue must be resolved. When you check this check box, a drop-down list appears. It lets you select the date from a calendar pop-up.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Location Affected</strong></td>
<td>Lets you specify the location that the incident affects. The affected user’s location appears by default.</td>
</tr>
<tr>
<td></td>
<td>When you click the <strong>Search</strong> symbol (magnifying glass), the Affected Location dialog box opens, and you can select a different location if necessary.</td>
</tr>
<tr>
<td></td>
<td>For example, you might encounter a problem with your email access during a visit to another corporate office.</td>
</tr>
<tr>
<td></td>
<td>The location is for informational purposes only.</td>
</tr>
<tr>
<td><strong>Department Affected</strong></td>
<td>Lets you specify the department that the incident affects. The affected user’s department appears by default.</td>
</tr>
<tr>
<td></td>
<td>When you click the <strong>Search</strong> symbol (magnifying glass), the <strong>Search for Affected Department</strong> dialog box opens, and you can select a different department if necessary.</td>
</tr>
<tr>
<td></td>
<td>The department is for informational purposes only.</td>
</tr>
<tr>
<td><strong>Urgency</strong></td>
<td>Lets you specify the severity of the issue.</td>
</tr>
<tr>
<td></td>
<td>The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>No Immediate Urgency</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Preventing Some Non-Urgent Work</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Blocking Critical Business</strong></td>
</tr>
<tr>
<td></td>
<td>Your organization or your manager might provide guidelines for when to use each of these options.</td>
</tr>
<tr>
<td><strong>Who is affected?</strong></td>
<td>Lets you specify how many people this issue affects. This information is combined with the urgency information to determine the incident’s priority.</td>
</tr>
<tr>
<td></td>
<td>The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Single User</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Entire Team or Group</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Entire Department</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Unsure</strong></td>
</tr>
<tr>
<td><strong>Attach File</strong></td>
<td>Lets you attach one or more files that provide additional information about the incident. For example, you can attach an error log file or a screen image that you captured.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Attaching a file to a new incident</strong>” on page 144.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Attach File to Incident dialog box</strong>” on page 145.</td>
</tr>
<tr>
<td></td>
<td>Any files that you attach appear in the <strong>Supporting Documents or Images</strong> list.</td>
</tr>
<tr>
<td><strong>Remove File</strong></td>
<td>Lets you remove a file that is attached to the incident. The attached files are listed under <strong>Supporting Documents or Images</strong>.</td>
</tr>
</tbody>
</table>
Table 11-1  Options on the Create a New Incident page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Take Screenshot            | Starts the Screen Capture utility so that you can capture an image of your computer screen, which you can attach to an incident. The Screen Capture utility also lets you edit the image.  
See “Capturing a screen image” on page 115.  
See “Screen Capture icons” on page 117.                                                                 |
| Search the Knowledge Base  | Lets you search the knowledge base for any articles that are related to your issue. You might find an article that answers your question and eliminates the need to submit an incident.  
See “Searching the knowledge base” on page 339.                                                                 |

Attaching a file to a new incident

During incident entry, you can attach one or more files to an incident to provide additional information about the issue. For example, you can attach an error log file or a screen image that you captured. Files larger than 4 MB are not supported.

See “Capturing a screen image” on page 115.

You can also attach a file to an incident after it has been created.

See “Attaching a file to an existing process ticket” on page 287.

The files that you attach to an incident are added to the Documents tab in the Process Manager portal. The files appear in a folder whose name is the incident number.

**To attach a file to an incident**

1. On the Create a New Incident page, click Attach File.

   See “Reporting an incident in ServiceDesk” on page 139.

2. In the Attach File to Incident dialog box, in File to Add, select a file.

3. (Optional) To add another file, click Add Another, and then select a file.

   Repeat this step for every additional file that you want to add.

4. When you finish adding files, click Add and Close.

5. On the Create a New Incident page, continue to enter information about the incident.

   See “Create a New Incident page” on page 142.
Attach File to Incident dialog box

This dialog box lets you attach one or more files to an incident to provide additional information about the issue. This dialog box appears when you choose to attach a file during the incident entry.

See “Attaching a file to a new incident” on page 144.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File to Add</td>
<td>Specify the file to add. You can add documents, spreadsheets, text files, logs, and many other file formats.</td>
</tr>
<tr>
<td>Current Attachments</td>
<td>Displays the files that are already attached to the ticket. To remove a file from the ticket, next to the file that you want to remove, click Remove.</td>
</tr>
<tr>
<td>Add Another</td>
<td>Adds the file to the Current Attachments list and lets you specify another file to attach without leaving the Attach File to Incident dialog box.</td>
</tr>
<tr>
<td>Add and Close</td>
<td>Adds the current attachments and closes the dialog box.</td>
</tr>
</tbody>
</table>

Capturing a screen image in an incident

When you create an incident, you can capture an image of your computer screen to help the ServiceDesk workers analyze the problem. For example, if an error message appears when you try to use an application, you can capture the message and attach it to the incident.

Before you can capture a screen image, you must have the Screen Capture Utility installed.

For more information, see the topics about installing the Screen Capture Utility in the Symantec ServiceDesk 7.5 Implementation Guide.

To capture a screen image in an incident

1 In the Create a New Incident dialog box, click Take Screenshot.

   See “Reporting an incident in ServiceDesk” on page 139.

2 If the Internet Explorer Security dialog box opens click Allow.
3 If the Screen Capture utility does not open automatically, in the **Screen Capture** dialog box, click one of the following links:

- **If the Screen Capture Utility does not open automatically, please click here.** Opens the Screen Capture utility. If the utility does not open, then it probably is not installed on your computer.
- **To install the Screen Capture Utility, please click here.** Installs the Screen Capture utility if it is not installed.

4 In the **Screen Capture** utility, select one of the icons to capture the image.

See “**Screen Capture icons**” on page 117.

5 (Optional) You can edit the image in the following ways:

- Add a note.
- Draw a rectangle.
- Crop the image.

6 When the image is finished, select one of the following symbols:

   **Send to Process Manager**

   Places the image on the **Screen Capture** page. When you click **Completed** on the **Screen Capture** page, the file is saved and attached to the incident.

   **Save to File**

   Displays the **Save As** dialog box, where you can type a name for the file, and then click **Save**.

   You can attach the saved file to this incident, to any other incident or ticket, or to any other document.

   **Copy to Clipboard**

   Copies the captured image to the clipboard so you can paste it into a different image or any other document. You can return to the **Screen Capture** page and click **Cancel** to return to the incident.

7 When you finish the capturing the image, in the upper right corner of the **Screen Capture** utility, click the **Close** symbol (red square).
8 In the **Screen Capture** dialog box, click **Cancel**.

9 In the **Create a New Incident** dialog box, you can continue the incident entry.

## Finding and reviewing your incidents

You can review the incidents that you create. Although you cannot edit an incident, you can perform other actions that are related to the incident.

If the incident is open or in progress and you have the appropriate permissions, you can perform the following actions:

- Add a comment.
- Add or remove bulletin board entries.
- Add, remove, or manage the equipment that is associated with the incident.
- Send an email.
- Search the knowledge base.

If the incident is closed, you can only view it.

**To find and review an incident**

1 In the Process Manager portal, click **Home**.

2 (Optional) On the **Home** page, under **My Requests**, if the incident is not listed, click the **Search** symbol. Next, in the search field, type one or more keywords, and then click **Find In Report Data**.

3 On the **Home** page, under **My Requests**, select the incident by its ticket number.

4 On the incident’s **Process View** page, view the incident or take whatever actions are necessary.

5 When you finish, close the incident’s **Process View** page.

## Confirming an incident’s resolution

After an incident is resolved, it appears in the affected user’s task list for review of its history, comments, and other information about its resolution.

Until you complete the confirmation task, the incident is considered to be 90 percent complete and open. If you do not respond within a specified number of days, the incident’s status is changed from Resolved to Closed. Your ServiceDesk administrator determines the number of days that are allowed.
Table 11-3  Confirming an incident’s resolution process

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Review the task and if necessary, take any steps that the support technician recommends.</td>
<td>You might need to take steps to resolve the issue yourself if the support technician provided instructions for doing so. For example, you might be directed to a knowledge base article or a Service Catalog option that contains resolution instructions.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Test to confirm that the issue is fixed.</td>
<td>This step is important whether you resolved the issue, or it was resolved for you.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If the issue is not fixed or if you are dissatisfied with the resolution, re-open the incident.</td>
<td>When you re-open the incident, it is returned to a support technician. See “Reopening an incident” on page 149. After you re-open the incident, wait for another task to notify you that it is resolved.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If the issue is fixed, close the incident.</td>
<td>If you are satisfied with the resolution, you can mark the incident as resolved. The incident is closed. See “Reviewing and closing a resolved incident and submitting feedback on an incident resolution” on page 148. When you confirm that an incident is resolved, you might be asked to complete a Customer Satisfaction Survey.</td>
</tr>
</tbody>
</table>

Reviewing and closing a resolved incident and submitting feedback on an incident resolution

After an incident is resolved, it appears in the affected user’s task list for review of its history, comments, and other information about its resolution. If the resolution fixes the issue, you can confirm the fix. If the Customer Satisfaction Survey appears, you can also provide feedback on the incidents resolution.

See “Confirming an incident’s resolution” on page 147.
To review and close a resolved incident and submit feedback on an incident resolution

1. In the Process Manager portal, click **My Task List**.
2. On the **My Task List** page, under **Tasks Viewer**, under **Project Name**, expand **SD.IncidentManagementSimple**.
3. In the list of tasks, find and open the task that requires feedback.
4. On the incident’s **Process View** page, review the information that appears under **Process History**, and then expand the **Documents** section and read any documents as appropriate.
5. Expand the **Tasks and Actions** section, and then click **Click here to review and close your incident**.
6. In the **Issue Resolved** dialog box, review the details about the resolution and if you are satisfied with the resolution, click **Issue Resolved**.
7. If the **Welcome** page of the Customer Satisfaction Survey appears, follow the on-screen instructions to provide feedback and when you finish, click **Continue**.
8. When the **Thank You** dialog box appears, you can close the dialog box, and then you can close the incident’s **Process View** page.

## Reopening an incident

After an incident is resolved, it appears in the affected user’s task list for review of its history, comments, and other information about its resolution. If the issue has been resolved you confirm the incident’s resolution. If the issue is not fixed or if you are dissatisfied with the resolution, you can reopen the incident.

Reopening an incident creates a duplicate incident that refers back to the original one. The duplicate incident is returned to a support technician. The technician either resolves the issue or escalates it to a higher level of support. When the incident is resolved again, you are asked to verify the resolution and provide feedback.

See “**Confirming an incident’s resolution**” on page 147.

See “**Reviewing and closing a resolved incident and submitting feedback on an incident resolution**” on page 148.

To reopen an incident

1. In the Process Manager portal, click **My Task List**.
2. On the **My Task List** page, under **Task Viewer**, under **Project Name**, expand **SD.IncidentManagementSimple**.
3 In the list of tasks, find and open the task that requires feedback.

4 On the incident’s Process View page, expand the Tasks and Actions section, and then click Click here to review and close your incident.

5 In the Issue Resolved dialog box, review the details about the resolution and if you are not satisfied with the resolution, click Reopen Issue.

6 In the Reason for Re-Opening this Issue field, type an explanation of why you need to reopen the incident.

   Provide details about the steps that you took to test the fix and the results of your test.

7 (Optional) You can attach files to the incident to support your explanation. The options are as follows:

   **Add File**
   
   Lets you attach one or more files that provide additional information about the incident. For example, you can attach an error log file or a screen image that you captured.

   See “Attaching a file to a new incident” on page 144.

   **Remove**
   
   Lets you remove a file that is attached to the incident. The attached files are listed under Supporting Documents.

8 In the Issue Resolved dialog box, click Continue to submit the reopened incident.
Submitting incidents (technician method)

This chapter includes the following topics:

- About advanced incidents
- About incident templates
- Creating an incident for a user with the advanced incident form
- Creating an incident from a template
- Create Incident page: advanced form
- Resolution page
- Creating an incident template
- Incident Template page

About advanced incidents

Support technicians or other workers who submit incidents on behalf of users can use the advanced incident form, which collects additional details. The advanced incident form lets you perform the following actions:

- Use a template to quickly populate the incident.
- Categorize the incident.
- Verify the configuration items for the user.
- Assign the incident to a worker or group.
- Set the impact and priority.
About incident templates

Incident templates are special incident forms containing predefined, standard values for common issues. Using templates speeds the entry of incidents and helps to standardize and increase the accuracy of the incident information.

For example, users frequently call support to restart a server, reset a password, or clear a printer jam. You can create an incident template that contains the appropriate category, type, title and description, and a reference to a related knowledge base article. The next time a user calls with that problem, the support technician can use the template to help create an incident with the correct values.

Before you create an incident template, be sure of its purpose. Incident templates are meant to handle Incident Management issue only, such as to report break or fix issues. Create Service Catalog processes for other types of requests that occur frequently. For example, you might create a Service Catalog process that requests software or equipment or that requests HR to process a new hire.

Incident templates are available only for the advanced incident form that the support technicians use. The templates are created and used within the advanced incident form. A template can be associated with a specific user or it can be shared globally. Incident templates can be edited and updated at any time based upon the changes that occur within your environment.

See “About the Service Catalog and service items” on page 442.
See “Creating an incident template” on page 159.
See “Creating an incident from a template” on page 154.
Creating an incident for a user with the advanced incident form

A support technician typically creates an incident in response to a help call from a user. The technician can also create an incident on their own behalf. The support technician uses the advanced incident form. This form lets the technician enter more information than the general incident form that users typically submit.

Before you create an incident template, be sure of its purpose. Incident templates are meant to handle Incident Management issue only, such as to report break or fix issues. Create Service Catalog processes for other types of requests that occur frequently. For example, you might create a Service Catalog process that requests software or equipment or that requests HR to process a new hire.

See “About advanced incidents” on page 151.

See “Reporting an incident in ServiceDesk” on page 139.

See “About the Service Catalog and service items” on page 442.

To create an incident for a user with the advanced incident form

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Requests** page, under **Service Catalog**, click **IT Services**.
3. On the right side of the page, click **Submit Incident (Advanced)**.
4. (Optional) Use a template to create the incident.
   - On the **Create Incident** page, under **Select Template**, select a template from the drop-down list, and then click **Use Template**.

See “Creating an incident from a template” on page 154.
5 On the Create Incident page, enter the information about the issue.

See “Create Incident page: advanced form” on page 155.

If you plan to create a new template, enter only the information that needs to appear in the template.

6 When you finish entering the information, select one of the following options:

- **Resolve**
  
  Lets you enter a resolution to the incident.

  See “Resolving an incident from the advanced incident form” on page 169.

- **Create Ticket**
  
  Submits the ticket without a resolution.

  In the Thank You dialog box, you can start another incident or close the page.

- **Save As Template**
  
  Lets you save the incident information as a template for future use.

  See “Incident Template page” on page 160.

  When you finish creating the template and click Save Template, you return to the Create Incident page. You can continue to enter information for the incident or close the page.

---

### Creating an incident from a template

When you create an incident with the advanced form, you can use a template to fill in some of the incident information.

See “About incident templates” on page 152.

**To create an incident from a template**

1. In the Process Manager portal, click Submit Request.
2. On the Submit Requests page, under Service Catalog, click IT Services.
3. On the right side of the page, click Submit Incident (Advanced).
4. On the left side of the Create Incident page, under Select Template, select a template in the drop-down list and then click Use Template.
On the Create Incident page, enter any information that was not filled in by the template. You can also edit any of the pre-filled information. See “Create Incident page: advanced form” on page 155.

When you finish entering the information, select one of the following options:

**Resolve**  
Lets you enter a resolution to the incident.  
See “Resolving an incident from the advanced incident form” on page 169.

**Create Ticket**  
Submits the ticket without a resolution.  
In the Thank You dialog box, you can start another incident or close the page.

### Create Incident page: advanced form

This page lets you create an incident with the advanced incident form.

See “Creating an incident for a user with the advanced incident form” on page 153.  
See “Incident Template page” on page 160.

<table>
<thead>
<tr>
<th>Table 12-1</th>
<th>Options on the Create Incident advanced form</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
<td><strong>Option</strong></td>
</tr>
</tbody>
</table>
| User Information | Select User | Lets you specify the primary contact for the incident. Typically, the primary contact is the person who encounters or reports the issue. You can specify the primary contact in any of the following ways:  
- You can type the user’s email address. Then click the Check if User Exists Using Email Address symbol to the right of the Select User field to verify the user in the database.  
- You can type part or all of the following information: Email address, first name, last name, nickname, phone number, manager, or employee ID, and then click the Search symbol (magnifying glass). |
<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Information</td>
<td>Location</td>
<td>Displays the information that is associated with the primary contact in the CMDB (Configuration Management Database).</td>
</tr>
<tr>
<td></td>
<td>Department</td>
<td>This display is for informational purposes only; it is not saved with the incident. However, you can click the &gt;&gt; option that appears next to any of these items to add the item to the incident.</td>
</tr>
<tr>
<td></td>
<td>Phone No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Associated Equipment</td>
<td></td>
</tr>
<tr>
<td>User Information</td>
<td>Tickets</td>
<td>Lists the incidents that have been submitted for this user. List all incidents in their various states except closed incidents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To include the closed incidents in the list, click <strong>Show Closed Tickets</strong>.</td>
</tr>
<tr>
<td>User Information</td>
<td>Show Closed Tickets</td>
<td>Lets you include closed tickets in the list of tickets that have been submitted for the user.</td>
</tr>
<tr>
<td>Select Template</td>
<td>Drop-down list</td>
<td>Lets you select a template from existing incident templates to create a new incident.</td>
</tr>
<tr>
<td>Select Template</td>
<td>Save as Template</td>
<td>Saves the information in the current incident as an incident template.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can create a template so that only you can use it, or you can make it available to others.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating an incident template” on page 159.</td>
</tr>
<tr>
<td>Select Template</td>
<td>Use Template</td>
<td>Opens the template that you select from the Select Template drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating an incident from a template” on page 154.</td>
</tr>
<tr>
<td>Ticket Information</td>
<td>Primary Contact</td>
<td>Displays the user name (email address) of the person who is specified as the primary contact.</td>
</tr>
<tr>
<td>Ticket Information</td>
<td>Title</td>
<td>Identifies this incident in any incident lists in the ServiceDesk portal.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When titling the incident, make it as specific as possible. For example, instead of “email problem,” you might type “Cannot receive external email”.</td>
</tr>
<tr>
<td>Section</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ticket Information</td>
<td>Description</td>
<td>Lets you type additional information to describe the issue. For example, you might describe the steps to reproduce the issue or provide more information about what happened. The toolbar that appears in this section provides common text formatting tools.</td>
</tr>
<tr>
<td>Ticket Information</td>
<td>Classification</td>
<td>Lets you select a classification for the incident. Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification. See “About Incident Management classifications and the data hierarchy” on page 499.</td>
</tr>
<tr>
<td>Ticket Information</td>
<td>Incident Management</td>
<td></td>
</tr>
</tbody>
</table>
Table 12-1  Options on the **Create Incident** advanced form *(continued)*

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ticket Information</strong></td>
<td>Postpone Date</td>
<td>Lets you specify the date on which the incident is assigned. The incident is created immediately but is not assigned until that date.</td>
</tr>
<tr>
<td><strong>KB Articles</strong></td>
<td>Search External KB</td>
<td>Displays any entries that are found by using the incident title as the search text. The entries that appear here are shown as a potential resolution to the incident. Lets you search Google, Technet, or another external database to which your organization might provide access.</td>
</tr>
<tr>
<td><strong>Additional Contacts</strong></td>
<td>None</td>
<td>Lets you add contacts to the incident. For example, if a user needs new equipment, you might add the user’s manager to obtain approval for the purchase.</td>
</tr>
<tr>
<td><strong>Related Processes</strong></td>
<td>None</td>
<td>Lets you search for other incidents, changes, and problems to attach to this incident.</td>
</tr>
<tr>
<td><strong>Location, Department, Equipment, Services</strong></td>
<td>Location</td>
<td>Lets you specify the location that the incident affects.</td>
</tr>
<tr>
<td><strong>Location, Department, Equipment, Services</strong></td>
<td>Department</td>
<td>Lets you specify the department that the incident affects.</td>
</tr>
<tr>
<td><strong>Location, Department, Equipment, Services</strong></td>
<td>Equipment</td>
<td>Lets you select any equipment that is related to the incident. For example, if the incident involves a printer jam, you can specify the printer that is jammed.</td>
</tr>
<tr>
<td><strong>Location, Department, Equipment, Services</strong></td>
<td>Services</td>
<td>Lets you select the business services that the incident affects. The <strong>Multiple</strong> check box opens the <strong>BusinessServices</strong> dialog box. This dialog box lets you select multiple businesses, if multiple business services are affected.</td>
</tr>
</tbody>
</table>

**Resolution page**

This page lets you resolve an incident from the advanced incident form that is available to support technicians.
### Table 12-2 Options on the Create Incident Resolution page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Close Code drop-down list</strong></td>
<td>Lets you select a code that indicates the nature of the resolution. ServiceDesk contains a set of predefined close codes. Other codes might appear if your organization has customized them. See “About incident close codes” on page 528.</td>
</tr>
<tr>
<td><strong>Resolution Notes</strong></td>
<td>Lets you type information in the text box about how the incident was resolved.</td>
</tr>
<tr>
<td><strong>Relevant Articles</strong></td>
<td>Displays any articles that are found automatically by using the incident title as the search text. The articles that appear here are shown to the user as a potential resolution to the incident.</td>
</tr>
<tr>
<td><strong>Create a KB Article checkbox</strong></td>
<td>Lets you request an entry, such as a knowledge base article, that can provide help for the same kind of issue in the future. For example, if the issue was resolved by training the user, the technician can request a knowledge base article that contains the same information. Users who encounter that issue in the future can find and read the knowledge base article instead of creating an incident. When you select this option and resolve the incident, the request becomes a task for the knowledge base (KB) editor.</td>
</tr>
</tbody>
</table>

## Creating an incident template

You can use the advanced form to create an incident template. You can create an incident template while creating an incident. The next time you create an incident for a similar issue, you can use this template to fill in some of the information automatically. You can also open the advanced form and create an incident template whenever one is needed.

See “About incident templates” on page 152.

### To create an incident template

1. In the Process Manager portal, click Submit Request.
2. On the Submit Requests page, under Service Catalog, click IT Services.
3. On the right side of the page, click Submit Incident (Advanced).
4 On the Create Incident page, enter only the information that needs to appear in the template.

See “Create Incident page: advanced form” on page 155.

5 Click Save As Template.

6 On the Incident Template page, provide information to identify and describe this template.

7 Check User Only Template if the template is only for your use. Uncheck User Only Template if the template is for all users to use.

See “Incident Template page” on page 160.

8 (Optional) Click View Attachments Details to view lists of all the items that are attached to the template. Click View Basic Details to view the general information and additional classifications information.

9 Click Save Template

10 On the Create Incident page, you can continue to create an incident or cancel it.

Note that canceling the incident does not affect the template that you created.

Incident Template page

This page lets you create a template that you and others can use to quickly create advanced incidents.

See “Creating an incident for a user with the advanced incident form” on page 153.

See “About incident templates” on page 152.

Table 12-3 Options on the Incident Template page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Identifies this template in any list of templates. When naming the template, make the name descriptive enough for you and others to easily understand the purpose of the template.</td>
</tr>
<tr>
<td>Template Description</td>
<td>Lets you type a description to further identify this template and make it more recognizable. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Only Template checkbox</td>
<td>Lets you make this template available to you only or you also can make it available to others.</td>
</tr>
</tbody>
</table>
Submitting incidents (technician method)

Incident Template page
Creating incidents from user emails

This chapter includes the following topics:

■ About the creation of incidents from emails
■ Classifying incident email submissions
■ Email Classification page
■ Set Incident Priority page
■ Search for Related Processes page

About the creation of incidents from emails

ServiceDesk can accept new incidents or updates to current incidents through inbound email. ServiceDesk monitors the appropriate inbox for all new, unread emails and processes them by creating incidents or routing them to the support team for classification. After an incident is created from an email, it can be worked the same way as any other incident.

The email monitoring process is defined in the SD.Email.Monitor and SD.Email.InboundManagement projects. You can use the monitoring process as it is defined or you can customize it. For example, you can monitor multiple mailboxes, define the email contents to be processed, and change the assignee for the new incidents.

See “About configuring the email monitoring” on page 513.
Table 13-1  How the email contents populate the incident’s values

<table>
<thead>
<tr>
<th>Email values</th>
<th>Resulting incident values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Primary contact</td>
</tr>
<tr>
<td></td>
<td>When the sender is not a ServiceDesk user, the incident’s contact is set to <a href="mailto:guest@logicbase.com">guest@logicbase.com</a>. However, because this guest user is not added as the primary contact, the support technician must add a primary contact to the incident.</td>
</tr>
<tr>
<td>Subject line</td>
<td>Incident title</td>
</tr>
<tr>
<td>Message body</td>
<td>Incident description</td>
</tr>
<tr>
<td></td>
<td>The email monitoring process can be customized to parse the message for specific words or phrases and then populate the appropriate values in the incident. For example, the process might look for the words Windows, Word, Excel, or printer.</td>
</tr>
</tbody>
</table>

The default values for normal ServiceDesk incidents are used to populate additional information in the incident. For example, the status and urgency are assigned the default values.

Table 13-2  How emails are processed for incident creation

<table>
<thead>
<tr>
<th>Criteria</th>
<th>How the email is processed</th>
</tr>
</thead>
</table>
| The subject line contains any of the phrase: New Incident. | The email monitoring process performs the following actions:  
  ■ Creates a new incident that contains data from the email message.  
  ■ Assigns the task according to the organization’s usual routing process.  
  ■ Sends a return email that contains the incident ID and the standard links for monitoring the incident. |

The email monitoring process creates a task for the Service Managers group to review and classify the email. The manager can process the email as follows:  
  ■ Create an incident or an advanced incident.  
  ■ Add the email’s contents to an existing incident.  
  ■ Create a problem ticket.  
  ■ Create a change request.  
  ■ Create a request for a knowledge base item.  
  ■ Suggest a self-service item from the Service Catalog.  
See “Email Classification page” on page 166.

The email monitoring process performs the following actions:
Classifying incident email submissions

ServiceDesk can accept new incidents or updates to current incidents through inbound email. ServiceDesk monitors the appropriate inbox for all new, unread emails and processes them by creating incidents or routing them to the support team for classification.

See “About the creation of incidents from emails” on page 163.

When ServiceDesk cannot process an email automatically, it creates a task for the Service Managers group to evaluate the email. When you work the task, you can review it, request additional information, create an incident, change request, or problem ticket, or perform other actions.

To classify an incident email submission

1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Tasks Viewer, under Project Name, expand SD.IncidentManagementSimple.
3. In the list of tasks, find and open the task that requires email classification.
4. On the incident’s Process View page, expand the Tasks and Actions section, and then click Classify Email Message.
5. On the Email Classification page, select an option to process the email.
   For example, you can create an incident, a change request, or a problem ticket based on the information in the email.
   See “Email Classification page” on page 166.
6. Depending on the option that you choose on the Email Classification page, take one of the following actions:
   ■ If another page appears, complete the page.
   ■ If you are returned to the evaluation task’s Process View page, you can close it.
Email Classification page

This page lets you review the content of an issue that was submitted in an email and decide how to process that issue in ServiceDesk.

When ServiceDesk cannot process an email automatically, it creates a task for the Service Managers group to evaluate the email. This page appears when the service manager works the evaluation task.

See “Classifying incident email submissions” on page 165.

See “About the creation of incidents from emails” on page 163.

Whenever a process ticket is created as a result of the service manager’s action, the process sends a return email. The email contains the process ID and the standard links for monitoring the ticket.

Table 13-3 Options on the Email Classification page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Service</td>
<td>Presents a list of all the available Service Catalog items. When you select an item, a return email with a link to that self-service item is sent.</td>
</tr>
<tr>
<td>Suggestions</td>
<td></td>
</tr>
<tr>
<td>Attachments</td>
<td>Displays any attachments that were included with the email.</td>
</tr>
<tr>
<td>Create Incident</td>
<td>Presents a series of options when you hover the mouse pointer over this option, as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Create an Incident Quickly</td>
</tr>
<tr>
<td></td>
<td>Creates an incident and sends a return email.</td>
</tr>
<tr>
<td></td>
<td>■ Create Incident by Setting Priority</td>
</tr>
<tr>
<td></td>
<td>Opens the Set Incident Priority page, which lets you specify the priority, impact, urgency, and business service for the new incident. A return email is sent.</td>
</tr>
<tr>
<td></td>
<td>See “Set Incident Priority page” on page 167.</td>
</tr>
<tr>
<td></td>
<td>■ Search Incidents</td>
</tr>
<tr>
<td></td>
<td>Performs an automatic search of all the other incidents that are associated with the sender and displays them on the Search for Related Processes page. You can also search for other incidents. When you select one of the displayed incidents, the email contents are added to the history section of that incident.</td>
</tr>
<tr>
<td></td>
<td>See “Search for Related Processes page” on page 168.</td>
</tr>
<tr>
<td>Create Problem</td>
<td>Creates a problem ticket and sends a return email.</td>
</tr>
<tr>
<td>Create Change Request</td>
<td>Creates a change request ticket and sends a return email.</td>
</tr>
<tr>
<td>Create KB Article</td>
<td>Creates a knowledge base article request and sends a return email.</td>
</tr>
<tr>
<td>Junk</td>
<td>Moves the email to the junk folder and ends the process.</td>
</tr>
</tbody>
</table>
Table 13-3  Options on the Email Classification page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Blacklist | When you blacklist a sender, the email monitoring process deletes all future emails from the sender. The Blacklist option adds the sender to the blacklist, marks the email as read, deletes the email, and ends the email monitoring process. The email monitoring process saves the information about the sender in the ServiceDeskBlackList table in the Process Manager database. All incoming emails are compared to the list of email addresses (senders) in the ServiceDeskBlackList table. If the email address matches an email address in the table, the email monitoring process deletes the email.  
**Note:** To remove a sender from the blacklist, you must manually remove the sender from the ServiceDeskBlackList table in the ProcessManager database. The next time the sender sends an email, the email monitoring system processes the email accordingly. |

---

Set Incident Priority page

This page lets you specify the priority, impact, urgency, and business service for a new incident that you create from an email. This page appears when you click Create Incident by Setting Priority on the Email Classification page.

See “Email Classification page” on page 166.

Table 13-4  Options on the Set Incident Priority page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Urgency**           | Lets you specify how much the issue affects the submitter or the primary contact.  
See “Default priority, urgency, and impact values” on page 433. |
| **Business Impact**   | Lets you define the extent of the issue by specifying how many people are affected.  
See “Default priority, urgency, and impact values” on page 433. |
| **Priority**          | Lets you select the priority for resolving this incident. The priority determines how the incident is routed and when it is escalated.  
See “About the incident priority” on page 432.  
See “Default priority, urgency, and impact values” on page 433. |
| **Business Services Affected** | Lets you select the business services that the incident affects. |
Table 13-4  Options on the **Set Incident Priority** page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachments</td>
<td>Displays any attachments that were included with the email.</td>
</tr>
<tr>
<td>Submit</td>
<td>Creates an incident that contains the information that you entered. The contact information, subject, and description are obtained from the email. A task is sent to the incident’s current assignee to notify them of the update.</td>
</tr>
</tbody>
</table>

**Search for Related Processes page**

This page lets you add the contents of an email submission to an existing incident. It performs an automatic search of all the other incidents that are associated with the sender. You can select from those incidents or search for additional ones.

When you select one of the displayed incidents, the email contents are added to the history section of that incident. A task is sent to the incident’s current assignee to notify them of the update.

This page appears when you click **Search Incidents** on the **Email Classification** page.

See “**Email Classification page**” on page 166.

Table 13-5  Options on the **Search for Related Processes** page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for</td>
<td>Lets you type the search text and find an incident to attach the email information to.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Lets you specify additional search criteria to help find the incident.</td>
</tr>
<tr>
<td><strong>Click here for process view</strong></td>
<td></td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays the incidents that result from your search and lets you select one to attach the email information to.</td>
</tr>
<tr>
<td>Processes Associated With This User</td>
<td>Displays the sender’s past incidents.</td>
</tr>
<tr>
<td>Email Information</td>
<td>Displays the email information that is added to the incident.</td>
</tr>
</tbody>
</table>
Resolving incidents

This chapter includes the following topics:

■ Resolving an incident from the advanced incident form
■ Resolving an incident from a task
■ Incident Response page
■ Scheduling an incident for later (postponing)
■ Reopening a postponed incident
■ Creating a problem ticket from an incident
■ Submit Problem page
■ Creating a change request from an incident
■ Closing multiple incidents

Resolving an incident from the advanced incident form

In response to a telephone call or email from a user, a support technician can record the incident on the advanced incident form. If the incident is resolved immediately, the support technician can resolve the incident at the same time as the incident entry.

For example, a user calls the Support Desk because of a printer jam. During the call, the support technician talks the user through the process of clearing the printer jam. When the call is over, the support technician creates and resolves the incident on the advanced incident form.

If you cannot resolve the incident, you might need to escalate it to another worker.
Resolving an incident from a task

The most common method for resolving an incident is to open its task from the Task List and work the incident from the incident’s Process View page.

Note that if you cannot resolve the incident, you might need to escalate it to another worker.

To resolve an incident from a task

1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Tasks Viewer, under Project Name, expand SD.IncidentManagementSimple.
3. In the list of tasks, find and open a task that requires resolution.
4. On the incident’s Process View page, expand the Task and Actions section, and then click Work Incident.
5 On the **Incident Response** page, enter information about the resolution and use any actions that are necessary.

See “**Incident Response page**” on page 171.

6 When you finish entering information about the resolution, select one of the following options:

- **Save** Saves the changes without resolving the incident. You or another worker can re-open the incident and resolve it later.
- **Resolve** Resolves the incident.

7 When the resolved incident is closed and you are returned to the incident’s **Process View** page, you can close it.

### Incident Response page

This page lets you resolve an incident from a task. It appears when you work an incident task and select the **Work Incident** option.

See “**Resolving an incident from the advanced incident form**” on page 169.

See “**Resolving an incident from a task**” on page 170.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Click Here to Classify</strong></td>
<td>Lets you select a classification for the incident.</td>
</tr>
<tr>
<td></td>
<td>Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>About Incident Management classifications and the data hierarchy</strong>” on page 499.</td>
</tr>
<tr>
<td><strong>Extend Classification</strong></td>
<td>Populates the page with the configuration items from the CMDB (Configuration Management Database).</td>
</tr>
<tr>
<td></td>
<td>You can select one or more classifications as appropriate to put the incident in the correct classification.</td>
</tr>
<tr>
<td><strong>Incident Type</strong></td>
<td>Lets you select an incident type to describe the general nature of the incident.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>About incident types</strong>” on page 440.</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>Lets you define the extent of the issue by specifying how many people the issue affects.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Default priority, urgency, and impact values</strong>” on page 433.</td>
</tr>
</tbody>
</table>
Table 14-1  Options on the Incident Response page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Urgency</strong></td>
<td>Lets you specify the urgency of the issue by specifying which service the issue affects. See “Default priority, urgency, and impact values” on page 433.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Lets you select the priority for resolving this incident. The priority determines how the incident is routed and when it is escalated. See “About the incident priority” on page 432. See “Default priority, urgency, and impact values” on page 433.</td>
</tr>
<tr>
<td><strong>Location Affected</strong></td>
<td>Lets you specify or change the location that the incident affects. When you click the Change Location symbol (magnifying glass), the Affected Location page appears. This page lets you change the affected location. You can select the contact's location or equipment's location, or you can search for a specific location.</td>
</tr>
<tr>
<td><strong>Department Affected</strong></td>
<td>Lets you specify or change the department that the incident affects. When you click the Change Department symbol (magnifying glass), the Search for Affected Department page appears. This page lets you change the affected department. You can select the contact's department or equipment's department, or you can search for a specific department.</td>
</tr>
<tr>
<td><strong>Close Code</strong></td>
<td>Lets you select a code that indicates the nature of the resolution.</td>
</tr>
<tr>
<td><strong>Specify Time Worked</strong></td>
<td>Lets you enter the amount of time that you spent on the incident offline. See “Posting process time to a ticket” on page 285.</td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td>Lets you type information in the text box about how the incident was resolved.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Saves the changes without resolving the incident. You or another worker can re-open the incident and resolve it later.</td>
</tr>
<tr>
<td><strong>Resolve</strong></td>
<td>Resolves the incident.</td>
</tr>
</tbody>
</table>

**Scheduling an incident for later (postponing)**

You can postpone the assignment and resolution of an incident by changing the task’s due date.

When you postpone an incident, the following things happen:

- The status is changed to Hold.
- The task is removed from the Tasks Viewer section on the My Task List page.
Any workers who are assigned to the task are unassigned.

A comment is added to the task's Process History section.

These actions are reversed when the postponement date arrives or when someone reopens the incident.

See “Reopening a postponed incident” on page 173.

To schedule an incident for later

1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Tasks Viewer, under Project Name, expand SD.IncidentManagementSimple.
3. In the list of tasks, find and open the task to postpone.
4. On the incident’s Process View page, under Tasks and Actions, expand the Smart Tasks section, and then click Hold Management.
5. In the Place Ticket on Hold dialog box, you must provide the following information:

<table>
<thead>
<tr>
<th>Reason for postponing the ticket</th>
<th>Provide a reason for the postponement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide date and time at which the incident should resume</td>
<td>Specify the date on which the incident should resume. Use the drop-down list calendar to specify the date. Specify the time on your selected date that the incident should resume.</td>
</tr>
</tbody>
</table>

6. Then, click Schedule for Later.
7. Close the incident’s Process View page.

Reopening a postponed incident

You can postpone the assignment and resolution of an incident by changing its due date. When you postpone an incident, it is put on hold and cannot be worked until the postponement date arrives.

See “Scheduling an incident for later (postponing)” on page 172.

If you are ready to work the incident before the postponement date, you can reopen the incident.

When you reopen an incident that was postponed, the following things happen:

- The status is changed to Open.
Creating a problem ticket from an incident

When the cause of an incident is a systemic problem rather than an isolated issue, you can associate the incident with a problem ticket. The problem analyst and problem reviewer can analyze the root cause of the problem and suggest a workaround or fix that can resolve the incident.

You can create a new problem ticket or associate the incident with an existing problem ticket. For example, a new incident might report an issue that is already associated with a problem ticket. Problem tickets can be associated with multiple incidents.

See “About cascading relationships among process tickets” on page 38.
To create a problem ticket from an incident

1. In the Process Manager portal, find and open the incident.

2. On the incident’s Process View page, under Tasks and Actions, expand Change and Problem Management Tools, and then click Create or Relate to Problem.

3. On the Submit Problem page, take one of the following actions:

   To attach the incident to an existing problem
   Under Associate with existing problems, find and select the problem as follows:
   - In Search for, type the search text and search for a problem ticket.
   - Under Search Results, click the Select link to the right of the problem to which you want to add the incident.

   Note: A problem is created as soon as you click the Select link. If you click the Select link by mistake, you can remove the relationship between the incident and the problem. You can also delete the problem ticket.

   To create a new problem ticket
   Under Create a new problem, define the new ticket as follows:
   - Review the suggested title and description and edit them if necessary.
     The title and description that default from the incident might be too specific or user-oriented to be appropriate for a problem ticket.
   - Click Create New Problem.

See “Submit Problem page” on page 175.

Submit Problem page

This page lets you associate an incident with an existing problem ticket or a create new problem ticket. It appears when you click Create Problem Ticket on the incident’s Process View page.

See “Creating a problem ticket from an incident” on page 174.

Table 14-2 Options on the Submit Problem page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for</td>
<td>Lets you type the search text for finding a problem ticket.</td>
</tr>
</tbody>
</table>
Table 14-2 Options on the Submit Problem page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Results</td>
<td>Displays the problem tickets that result from the search and lets you select the problem to which you want to add the incident.</td>
</tr>
<tr>
<td>Title</td>
<td>Lets you edit the problem title and description if necessary.</td>
</tr>
<tr>
<td>Problem Description</td>
<td>The title and description that default from the incident might be too specific or user-oriented to be appropriate for a problem ticket.</td>
</tr>
<tr>
<td>Create New Problem</td>
<td>Creates a problem that is based on the incident.</td>
</tr>
</tbody>
</table>

Creating a change request from an incident

A support technician or other worker who works an incident can create a change request.

Creating a change request is a step in the Change Management process.

See “About the Change Management process” on page 221.

To create a change request from an incident

1. In the Process Manager portal, find and open the incident.
2. On the incident's Process View page, under Tasks and Actions, expand Change and Problem Management Tools and then click Request Change.

   Note that if this action is not available, the task is probably not assigned to you. To enable this action and work the task anyway, under Others Actions, click Work Tasks Assigned To Others if that option is available.
3. In the Request a Change dialog box, on the Enter Change Request Details page, enter information about the change.

   See “Requesting a change” on page 242.

Closing multiple incidents

When multiple incidents are ready to be closed, you can close them all at the same time.

See “Performing actions on multiple tickets” on page 286.
To close multiple incidents

1. In the Process Manager portal, click Submit Request.

2. On the Submit Request page, under Service Catalog, click Administrative Services.

3. On the right side of the page, click the Resolve/Close Multiple Incidents link.

4. On the Search for Incidents to Close page, select the incidents to close as follows:
   - Search for the incidents that you want to close.
   - In the Search for Tickets search field, type the search text, and then click Search.
   - You can search for an incident by title or description.
   - Select the incidents that you want to close.
   - Under Search for Tickets, select each incident in the list that you want to close.
   - This action moves the incident to the Selected Tickets field.
   - (Optional) Select all the incidents.
   - Click Add All to select all the incidents in the list to close.
   - This action moves all the incidents to the Selected Tickets field.

5. (Optional) If you need to remove an incident from the Selected Tickets list, to the right of the incident click Remove.

6. (Optional) To skip the resolve step, check Skip the “resolved” step for these tickets (They will be completely closed).

7. In the Closure Comments field, type why the incidents can be closed.

8. When you are finished, click Commit.

9. In the Message from the webpage dialog box, click OK.
Resolving incidents

Closing multiple incidents
Creating incident subtasks

This chapter includes the following topics:

■ About subtasks
■ About subtask templates
■ Creating a subtask for an incident
■ Creating a subtask from a template
■ Create Subtasks page
■ Create Subtask page
■ Creating subtask templates from the incident Process View page
■ Creating subtask templates
■ Editing subtask templates
■ Deleting subtask templates

About subtasks

Before you resolve an incident, several additional actions might need to be taken. You can create subtasks to record, assign, and track the additional actions for an incident. For example, you might create a subtask to review a server’s specifications to determine whether that server can accommodate a software upgrade.

See “Creating a subtask for an incident” on page 180.

During the subtask creation, you can create a subtask template and you can create a subtask from a template.

See “About subtask templates” on page 180.
The subtask workers can view the subtasks in their Task Lists and work the subtasks the same as any other incident tasks. The support technician who created the subtasks can view the parent incident’s status changes and its history.

See “Create Subtasks page” on page 181.

About subtask templates

Subtask templates increase the speed of the subtask assignment process. They standardize subtask information and increase the accuracy. When you create a subtask, you can use a template to quickly fill in some of the subtask information.

For example, a common subtask in your environment requires a specific worker or group to check a user’s Active Directory permissions. You can create a template that contains the title, description, and priority. The next time that subtask is required for a specific incident, you can use the relevant template to help create the subtask.

See “Creating subtask templates” on page 184.

See “Creating subtask templates from the incident Process View page” on page 183.

See “Creating a subtask from a template” on page 181.

Creating a subtask for an incident

When the resolution of an incident requires that additional actions are taken, you can create subtasks to record, assign, and track the additional actions.

See “About subtasks” on page 179.

To speed the creation of a subtask, you can create a subtask from a template.

See “Creating a subtask from a template” on page 181.

To create a subtask for an incident

1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Tasks Viewer, under Project Name, expand SD.IncidentManagementSimple.
3. In the list of tasks, find and open the task that requires a subtask.
4. On the incident’s Process View page, expand the Smart Tasks section, and then click Manage Subtasks.
5. On the Create Subtasks page, click Add Subtask.

See “Create Subtasks page” on page 181.
6 On the **Create Subtask** page, provide the necessary information in all the required **Subtask Details** fields.

See “Create Subtask page” on page 182.

7 Click **Add Subtask**.

8 (Optional) Create additional subtasks as needed.

On the **Create Subtasks** page, click **Add Subtask** and repeat Steps 6 - 7.

9 On the Create Subtasks page, click **Finished Managing Subtasks**.

**Creating a subtask from a template**

When you create a subtask, you can use a template to quickly fill in some of the subtask information.

See “About subtask templates” on page 180.

See “Creating a subtask for an incident” on page 180.

**To create a subtask from a template**

1 In the Process Manager portal, click **My Task List**.

2 On the **MyTaskList** page, under **Tasks Viewer**, under **Project Name**, expand SD.IncidentManagementSimple.

3 In the list of tasks, find and open a task that requires a subtask.

4 On the incident’s **Process View** page, expand the **Smart Tasks** section, and then click **Manage Subtasks**.

5 On the **Create Subtasks** page, in the **Use Subtask Template** drop-down list, select a template to use to create the subtask.

6 Click the **Use Template** symbol (green go arrow).

7 (Optional) Create additional subtasks, as needed.

On the **Create Subtasks** page, click **Add Subtask**.

See “Creating a subtask for an incident” on page 180.

8 When you are finished editing information and adding additional subtasks, on the **Create Subtasks** page, click **Finished Managing Subtasks**.

**Create Subtasks page**

This page lets you create subtasks for an incident. Subtasks represent the additional actions that need to be taken to resolve the incident. This page appears
when you click **Manage Subtasks** under **Smart Tasks**, on an incident’s **Process View** page.

See “Creating a subtask for an incident” on page 180.

**Table 15-1** Options on the **Create Subtasks** page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove</td>
<td>Lets you delete the subtask to the left of this link.</td>
</tr>
<tr>
<td>Edit</td>
<td>Lets you edit the subtask to the left of this link.</td>
</tr>
<tr>
<td>Use Subtask Template drop-down list</td>
<td>Lets you select an existing subtask template to use to create a new subtask.</td>
</tr>
<tr>
<td>Use Template symbol</td>
<td>Lets you use the template that you selected from the <strong>Select Template</strong> drop-down list to create a subtask.</td>
</tr>
<tr>
<td>Add Subtask</td>
<td>Let you open the <strong>Create Subtask</strong> page, where you can enter the subtask details and make assignments.</td>
</tr>
<tr>
<td>Manage Templates</td>
<td>Lets you open the <strong>Manage Subtask Templates</strong> page, where you can add, remove, or edit subtask templates.</td>
</tr>
<tr>
<td>Finished Managing Subtasks</td>
<td>Lets you save the subtasks that are listed and close the <strong>Create Subtasks</strong> page.</td>
</tr>
</tbody>
</table>

**Create Subtask page**

This page lets you add one or more subtasks to an incident and assign the subtasks to other workers. It appears when you click **Add Subtask** on the **Create Subtasks** page.

See “Creating a subtask for an incident” on page 180.

**Table 15-2** Options on the **Create Subtask** page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to user field</td>
<td>Lets you assign the subtask to a user.</td>
</tr>
<tr>
<td>Search symbol</td>
<td>Lets you search for and select a user to whom you want to assign the subtask.</td>
</tr>
<tr>
<td>Enter task title field</td>
<td>Identifies this subtask in any task lists or ticket lists in the Process Manager portal. When you type the title, make it as specific as possible.</td>
</tr>
</tbody>
</table>
You can use subtask to break up the items that you need to accomplish to resolve an incident. Then, you can assign those subtasks to other personnel. For the subtasks that are repeatable, you can create subtask templates. After you create a subtask template, you can use the template to create identical or similar subtasks. The template fills in the information automatically for the new subtask. You can create a subtask template while you create a subtask.

To create a subtask template from an incident’s Process View page

1. In the Process Manager portal, click My Task List.
3. In the list of tasks, find and open the task that requires subtasks.
4. On the incident’s Process View page, under Tasks and Actions, expand the Smart Tasks section, and then click Manage Subtasks.
5. On the Create Subtask page, click Manage Templates.
6. On the Manage Subtask Templates page, click Add Template.
7. Under Subtask Template’s Details, in the Template Name field, type the name of the subtask template and then click Add Task to Template.
Creating incident subtasks

Creating subtask templates

You can use subtask to break up the actions that are needed to resolve an incident. Then, you can assign those subtasks to other personnel. For the subtasks that are repeatable, you can create subtask templates. After you create a subtask template, you can use the template to create identical subtasks. The template fills in the information automatically for the new subtask.

To create a subtask template

1. In the Process Manager portal, click Submit Request.
2. On the Submit Request page, in the Service Catalog section, click Administrative Services.
3. On the right side of the page, click Manage Incident Subtask Templates.
4. On the Manage Subtask Templates page, click Add Template.
5 Under Subtask Template’s Details, in the Template Name field, type a descriptive name for the email template. Type a name that makes the subtask easy to identify a list of subtask templates.

6 Click Add Task.

7 On the Create Subtask page, in the Task Title field, type the title of the subtask.

8 In the Task Priority drop-down list, select the priority for the subtask.

9 Assign the incident to a user as follows:
   ■ To the right of the Assign to user field click the Search symbol (magnifying glass).
   ■ In the User Selection dialog box, in the Search Text field, type the first name, last name, or part of an email address. Then, click the Search symbol (magnifying glass).
   ■ Select the user and then click Select User.

10 In the Task Details field, type instructions for completing the subtask.

11 When you are finished, click Save Subtask.

12 Click Save Template.

   The subtask template is displayed in the Manage Subtask Templates dialog box, in the Subtask Template’s Details section.

13 On the Manage Subtask Templates page, click Finished Managing Templates.

See “About subtask templates” on page 180.

See “Deleting subtask templates” on page 186.

See “Editing subtask templates” on page 185.

See “Creating subtask templates from the incident Process View page” on page 183.

On the Submit Request page, in the Service Catalog section, click Administrative Services

---

**Editing subtask templates**

After you create your subtask template, you may need to edit it. For example, you may need to assign the subtask to a different user or add additional information to the task details.
To edit a subtask template

1. In the Process Manager portal, click Submit Request.
2. On the Submit Request page, in the Service Catalog section, click Administrative Services.
3. On the right side of the page, click Manage Incident Subtask Templates.
4. On the Manage Subtask Templates page, locate the subtask template that you want to edit.
5. To the right of the subtask template, click the Edit link.
6. Under Subtask Template's Details, perform any of the following actions:
   - Change the descriptive name for the email template.
   - Remove a task from the subtask template.
   - Edit a task in the subtask template.
   - Add a task to the subtask template.

   - In the Template Name field, type a name that makes the subtask easy to identify a list of subtask templates.
   - To the right of the task that you want to remove, click the Remove link.
   - To the right of the task that you want to edit, click the Edit link.
   - On the Create Subtask page, modify the Subtask Details information as needed.
   - Click Save Subtask.
   - Click the Add Task.
   - On the Create Subtask page, provide the required Subtask Details information.
   - Click Save Subtask.

7. Click Save Template.
8. Click Finished Managing Templates.

See “Creating subtask templates” on page 184.

See “Deleting subtask templates” on page 186.

Deleting subtask templates

After you create your subtask templates, you may need to delete an obsolete subtask template.
To delete a subtask template

1  In the Process Manager portal, click Submit Request.

2  On the Submit Request page, under Service Catalog, click Administrative Services.

3  On the right side of the page, click Manage Incident Subtask Templates.

4  On the Manage Subtask Templates page, locate the subtask that you want to delete.

5  To the right of the subtask template, click the Remove link.

6  On the Manage Subtask Templates page, click Finished Managing Templates.

See “Creating subtask templates” on page 184.

See “Editing subtask templates” on page 185.
Creating incident subtasks

Deleting subtask templates
Managing incident service queues

This chapter includes the following topics:

- Creating incident service queues
- Editing incident service queues
- Deleting incident service queues

Creating incident service queues

The Incident Management process lets you route incidents to service queues. By default, ServiceDesk provides the Default Incident Queue service queue, and associates the Support group to it. Before you can configure your automation rules, Symantec recommends that you first create your incident service queues and associate your groups to the queues.

Video: For more information about creating and managing incident service queues, see ServiceDesk Configuration: Create and Manage Service Queues on Symantec Connect.

Service queues consist of a group or multiple groups that you associate with it. You can change users and group without reconfiguring your routing rules. You can add or remove the users that are in the group that you associate with the service queue. You can add or remove the groups that are associated with the service queue.

Note: Adding and removing groups from queues only affects future assignments and does not affect currently assigned incidents.
To create an incident service queue

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Request** page, in the **Service Catalog** section, click **Administrative Services**.
3. On the right side of the page, click **Manage Incident Service Queues**.
4. On the **Active Service Queues** page, click **New Queue**.
5. On the **Create/Edit Service Queue** page, in the **Service Queue Name** field, type the name of the service queue.
   Type a descriptive name of the service queue to make it easy to identify. The name is displayed in the list of service queues on the **Active Service Queues** page.
6. (Optional) Add the service queue location as follows:
   - To the right of the **Queue Location (Optional)** field, click the **Search** symbol (magnifying glass).
   - In the **Location Selection** dialog box, in the **Search Text** field, type your search criteria and click the **Search** symbol (magnifying glass).
   - Select the location and then click **Select Location**.
   - The location appears in the **Queue Location (Optional)** field.
7. In the **Queue Description** field, type a description of the service queue.
8. Add groups to the service queue as follows:
   - Under **Security Group Membership**, in the **Search** field, type your group search criteria and click the **Search** symbol (magnifying glass).
   - Select the group that you want to add and click **Add Selected**.
   - To add additional groups to the service queue, repeat this step.
   - The group appears in the **Groups Currently in Queue** field.
   - To remove a group from this field, click the group.
9. When you are finished, click **Save Queue**.
10. On the **Active Service Queues** page, click **Close**.

See “**Editing incident service queues**” on page 191.

See “**Deleting incident service queues**” on page 192.
Editing incident service queues

You can edit your incident service queues. For example, you need to add another group to a service queue. Edit the service queue and add an additional group to the service queue.

Note: The group-to-service queue relationship is only used during ticket assignment. Adding and removing groups from queues only affects future assignments and does not affect currently assigned incidents. Individual ticket assignments can be reset when you reassign them to queue to which they are currently assigned. For example, you remove a group from a queue. To restrict the group's access to the existing tickets, reassign those tickets back to the queue.

Adding and removing groups from queues only affects future assignments and does not affect currently assigned incidents.

To edit an incident service queue

1. In the Process Manager portal, click Submit Request.
2. On the Submit Request page, in the Service Catalog section, click Administrative Services.
3. On the right side of the page, click Manage Incident Service Queues.
4. On the Active Service Queues page, locate the service queue that you want to edit.
5. To the right of the service queue, click the Edit link.
6. (Optional) In the Service Queue Name field, edit the name of the service queue.
7. (Optional) Change the service queue location as follows:
   - To the right of the Queue Location (Optional) field, click the Search symbol (magnifying glass).
   - In the Location Selection dialog box, in the Search Text field, type your search criteria and click the Search symbol (magnifying glass).
   - Select the location and then click Select Location.
   - The location appears in the Queue Location (Optional) field.
8. (Optional) In the Queue Description field, edit the description of the service queue.
9. (Optional) Remove groups from the service queue.
   - Under Groups Currently in Queue click the group that you want to remove.
10 (Optional) Add groups to the service queue as follows:

- Under **Security Group Membership**, in the **Search** field, type your group search criteria and click the **Search** symbol (magnifying glass).

- Select the group that you want to add and click **Add Selected**.
  
  To add additional groups to the service queue, repeat this step.

- In the **Service Queue Management** dialog box, under **Service Queue Group Association**, click the **Add** symbol (green plus sign).

- The group appears in the **Groups Currently in Queue** field.

11 When you are finished, click **Save Queue**.

12 On the **Active Service Queues** page, click **Close**.

See “Creating incident service queues” on page 189.

See “Deleting incident service queues” on page 192.

### Deleting incident service queues

You can delete incident service queues. Symantec recommends that you delete a service queue before you create your routing rules. Symantec also recommends that after you start routing incidents to a service queue, that you do not delete that service queue.

If you must delete a service queue after incidents are routed to it, make sure that the following conditions are met:

- Modify all the rules that route incidents to the queue and route them to another queue.

  **Warning:** If you delete a service queue before you modify the routing rules that route incidents to that queue, the routing rules error out.

- Remove the groups from the queue.

  **Note:** Deleting a service queue does not affect the incidents that are currently assigned to the groups that are associated to the queue. Incidents previously routed to a queue remain assigned to that queue’s groups, even if you delete the queue.
To delete an incident service queue

1. In the Process Manager portal, click Submit Request.
2. On the Submit Request page, in the Service Catalog section, click Administrative Services.
3. On the right side of the page, click Manage Incident Service Queues.
4. On the Active Service Queues page locate the service queue that you want to delete.
5. Note that you should not complete the next step unless you are sure that you want to delete the routing rule.
6. To the right of the service queue, click the Remove link.
7. Click Close.

See “Editing incident service queues” on page 191.
See “Creating incident service queues” on page 189.
Managing email templates

This chapter includes the following topics:

■ Creating email templates for Incident Management
■ Editing email templates for Incident Management
■ Deleting email templates for Incident Management

Creating email templates for Incident Management

Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. You can create email templates and associate them with actions. For example, a VIP submits an incident. A preconfigured email can be sent to a specific user or group notifying them of a VIP incident submittal. The email template can be preconfigured with subject line and message information.

Note: The Send Email process type action, on the Incident Management Process View page uses the Incident Management email templates. You may want to create email templates specifically for your technicians to use when working an incident ticket.

Video: For more information about creating email templates and creating rules to send emails, see ServiceDesk Configuration: Manage Email Templates in ServiceDesk on Symantec Connect.

To create an email template

1 In the Process Manager portal, click Admin > Process Automation.
2 On the Available Services page, expand Incident Management and then click Service Dashboard.
3 On the Automation Rules page, in the Actions: INCIDENT-MGMT section, click Manage Email Templates.

4 On the Notification Templates page, in the Email Templates section, click Add Email Template.

5 In the Add Email Template dialog box, in the Template Type area, select one of the following template types:

- **Process Event**
  - Lets you create an email template for process event rulesets.
  - The list of available fields in the Available Fields section corresponds specifically to process events.
  - These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset.
  - For example, a process event email template can be delivered from the OnIncidentReceived ruleset.

- **Data Event**
  - Lets you create an email template for a specific data event ruleset.
  - Lets you use the Event field to assign a data event category to the email template.
  - The list of available fields in the Available Fields section corresponds specifically to the type of data events that you select.
  - These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event.
  - Note that the email template is only available for its corresponding data event ruleset.
  - For example, you create a ruleset for <OnDocumentAdded> data event. You create a rule to deliver an email anytime a document is added to the incident ticket. When you create the email template for this rule, you must select DocumentAdded in the Event drop-down list.

6 (Optional) If you selected Data Event, in the Event drop-down list, select a data event.

   For example, you want to create an email template so you can send an email out when a comment is added to an incident ticket. In the Event drop-down list, click CommentAdded.
7 In the **Name** field, type the name for the email template.

This name displays on the **Notification Templates** page, in the **Email Templates** section.

8 In the **From** field, type the name of the user or group sending the message.

9 (Optional) In the **Description** field, type the description of the email template.

This description displays on the **Notification Templates** page in the **Email Templates** section.

10 (Optional) In the **Subject** field, type the subject of the email.

11 (Optional) In the **Body** field, type the message.

   If you want to let the end user's reply to the emails and have ServiceDesk capture those emails, you must add a reply code.

   Use the following format:

   \[ \text{IID} = \{\text{WorkflowTrackingId}\} \]

   \{WorkflowTrackingId\} is the variable that is added to the body of the email when you select **Workflow Tracking ID** in the **Available Fields** section.

12 (Optional) Add additional information to a specific area of the email.

   ■ In the **Add To** area, select the field (**From**, **Subject**, or **Body**) to which you want to add the additional information.

   ■ Then, in the **Available Fields** section, select the fields that you want to add.

   ■ Repeat this step until you are finished adding additional information.

13 When you are finished, click **Save**.

See “**Editing email templates for Incident Management**” on page 197.

See “**Deleting email templates for Incident Management**” on page 200.

---

**Editing email templates for Incident Management**

You can edit email templates if necessary. If you edit an email template before you use it in the **Send Email** action of a rule, you can edit all parts of the template. If you edit an email template after you use it in the **Send Email** action of a routing rule, do not edit the **Template Type**. **Template Type** makes the email template available only to rulesets that correspond to the event type that you select.

For example, process event email templates are only available to process event type rulesets. If you want to use that same email template for a different template
type, you need to create a new email template. Then, you need to create a new rule to deliver it.

---

**Note:** Do not change the **Template Type** in an email template after you use it in a rule. Changing the **Template Type** appears to remove the selected email template from the **Send Email** action of the rule. Because the rule uses the ID number of the email template, the email is still sent, but it may not display the information as expected.

---

**To edit an email template**

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Incident Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: INCIDENT-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section locate the email template that you want to edit. To the right of the email template, click the **Action** symbol (orange lightning) and then click **Edit Email Template**.
5. (Optional) In the **Edit Email Template** dialog box, in the **Template Type** area, change the **Template Type** only if you have not created a rule that delivers the email template.

**Process Event**

- Lets you create an email template for process event rule sets.
- The list of available fields in the **Available Fields** section corresponds specifically to process events.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset. For example, a process event email template can be delivered from the **OnIncidentReceived** ruleset.
**Data Event**  
- Lets you create an email template for a specific data event ruleset.
- Lets you use the **Event** field to assign a data event category to the email template.
- The list of available fields in the **Available Fields** section corresponds specifically to the type of data events that you select.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event. Note that the email template is only available for its corresponding data event ruleset. For example, you create a ruleset for `<OnDocumentAdded>` data event. You create a rule to deliver an email anytime a document is added to the incident ticket. When you create the email template for this rule, you must select **DocumentAdded** in the **Event** drop-down list.

6  (Optional) If you changed the template type to **Data Event**, in the **Event** drop-down list, select a data event.

For example, you want to edit the email template so you can send an email out when a comment is added to an incident ticket. In the **Event** drop-down list, click **CommentAdded**.

7  (Optional) In the **Name** field, edit the name for the email template.

This name displays on the **Notification Templates** page, in the **Email Templates** section.

8  (Optional) In the **From** field, edit the name of the user or group sending the message.

9  (Optional) In the **Description** field, edit the description of the email template.

This description displays on the **Notification Templates** page in the **Email Templates** section.

10  (Optional) In the **Subject** field, edit the subject of the email.

11  (Optional) In the **Body** field, edit the message.

12  (Optional) Add additional information to a specific area of the email.

- In the **Add To** area, select the field (**From**, **Subject**, or **Body**) to which you want to add the additional information.
- Then, in the **Available Fields** section, select the fields that you want to add.
Repeat this step until you are finished adding additional information.

13  (Optional) Remove additional information from a specific area of the email.

14  When you are finished, click Save.

See “Creating email templates for Incident Management” on page 195.

See “Deleting email templates for Incident Management” on page 200.

Deleting email templates for Incident Management

You can delete email templates if necessary. If you want to delete an email template before creating a rule that delivers it, you can delete it without taking any other actions. To delete an email template after creating a rule that delivers it, you must first edit the rule to use a different email template. You can also delete the rule and then delete the email template.

To delete an email template

1  In the Process Manager portal, click Admin > Process Automation.

2  On the Available Services page, expand Incident Management and then click Service Dashboard.

3  On the Automation Rules page, in the Actions: INCIDENT-MGMT section, click Manage Email Templates.

4  On the Notification Templates page, in the Email Templates section locate the email template that you want to delete.

5  To the right of the email template, click the Action symbol (orange lightning) and then click Delete Email Template.

6  In the Message from webpage dialog box, click OK

See “Creating email templates for Incident Management” on page 195.

See “Editing email templates for Incident Management” on page 197.
Routing and escalating incidents

This chapter includes the following topics:

- About incident routing and escalation
- About the Incident Management Automation rules
- Incident Management Process Automation rules components
- Configuring new automation rules for Incident Management

About incident routing and escalation

A key feature of ServiceDesk is its ability to route (assign) and escalate incident tickets to provide efficient and timely incident handling.

Routing rules determine the users or groups that new ServiceDesk incidents are assigned to. The rules also determine how incidents are escalated. ServiceDesk contains predefined routing rules and other settings that are ready to use, but you can customize them to meet your organization’s requirements. Most organizations perform some level of customization.

The default routing rules in ServiceDesk assign new incidents based on each incident’s priority setting as follows:

- All incidents are assigned to the Default Incident Queue.
- As part of your ServiceDesk setup, you should configure routing rules.

The additional ServiceDesk settings that can affect the incident routing are as follows:
The Service Level Agreement (SLA) time frames should be configured in the Process Automation Rules.

The SLA time frame determines when you should escalate an incident. You should configure your SLA time frames. Then you should configure routing rules to determine what the process should do when an incident's SLA status changes.

For example, when an incident's SLA status changes to Warn, you want to send an email to the worker assigned to work the incident. You can set up a routing rule to send out an email notification when an incident's SLA status changes.

See “Creating and Editing Service Level Agreements (SLAs)” on page 435.

Customized rules should be created on the Process Automation Rules Service Dashboard.

Automation rules allow the ServiceDesk administrator to create custom rulesets. Every incident is evaluated against existing rulesets and if conditions are met, the incident is routed accordingly.

See “About the Incident Management Automation rules” on page 202.


Process workers can override the default routing and escalation by reassigning and escalating the tickets manually.

See “Reassigning incidents, problems, or change tickets” on page 289.

You can customize the routing rules to define more specific criteria for routing and escalating incidents. For example, you can customize the routing rules to assign incidents to a specific group based on the group's location. Another way to customize your incident routing is to combine rules. For example, you can route incidents to a specific group if their priority is High, their category is Server, and their location is Corporate Headquarters.

---

**About the Incident Management Automation rules**

The Automation rules let you use the Incident Management automation library to configure your Incident Management process. The rulesets for a process are referred to as the automation library.

Out-of-the-box, the Incident Management automation library contains 13 rulesets, two of which have predefined rules:

- **OnIncidentReceived**
  
  This ruleset contains one default rule and is launched when an incident is created.
The default rule routes all new incidents to the default service queue. You can create additional rules for the ruleset.

- **OnResolutionVerified**
  This ruleset contains one default rule and is launched when an incident is resolved.
  The default rule sends the customer survey when an incident is verified as resolved.
  You can create additional rules for the ruleset.

- You can create rules for all other rulesets.

The Administrator can configure routing and notification rules for specific events within the incident management process. A rule is comprised of two variables: composite condition and an action to take. One rule can have multiple conditions.

After you select a condition and a corresponding action, additional options are displayed. These additional options let you narrow the parameters of the condition and action. Also, when you create a ruleset, you can sequence multiple rules to fine-tune the parameters of the ruleset.

See “Configuring new automation rules for Incident Management” on page 214.


### Incident Management Process Automation rules components

The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process. You control the events that trigger a rule to run, the conditions for rule evaluation, and the action that occurs once the conditions are met.

The Process Automation rules contain three main components:

- **Rulesets**
  Rulesets function as triggers that initiate a rule to run. Rulesets can contain multiple rules. Rulesets are classified either process event types or data event types.
  **Process Events** let you determine what happens at specific points in the lifecycle of an incident.
  For example, **OnIncidentReceived** is a process event ruleset that lets you determine what happens at the incident creation point of the process.
  **Data Events** let you determine what happens if data changes at any point during the lifecycle of an incident.
For example, **CommentAdded** is a data event ruleset that lets you take an action whenever a comment is added to an incident. By default, the **OnAnySlaMissed** and **OnAnySlaCompletedLate** rulesets are enabled. Only enable the data event type rulesets that you plan to use. See “Incident Management automation rules rulesets” on page 204.

### Conditions
Conditions determine when an action should occur. You can add multiple conditions to a rule. You can configure them to meet all of the conditions or only some of the conditions. Conditions support the “Not” statement, with a **Not** checkbox.
For example, you can add the **Affected User** condition to the rule that you create for the **OnIncidentReceived** ruleset. This condition lets you evaluate the new incident by who was affected. See “Incident Management automation rules conditions” on page 206.

### Actions
Actions are the result of a rule when the conditions are met.
For example, you can add the **Route Incoming Incident** action to the rule that you create for the **OnIncidentReceived** ruleset. This action lets you control which service queues receive which tickets when the conditions are met. See “Incident Management automation rules actions” on page 211.

See “Configuring new automation rules for Incident Management” on page 214.

### Incident Management automation rules rulesets
The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process.

See “Configuring new automation rules for Incident Management” on page 214.

Rulesets function as triggers that initiate a rule to run. Rulesets are classified as either process event or data event types.

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Description</th>
<th>Event type</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnIncidentReceived</td>
<td>Runs when an incident is created.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnOwnershipChanged</td>
<td>Runs when the ownership of a ticket is assigned or changed to a specific person.</td>
<td>Process Event</td>
</tr>
<tr>
<td>Ruleset</td>
<td>Description</td>
<td>Event type</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>OnResolutionVerified</td>
<td>Runs when the affected contact verifies the resolution of an incident.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnTicketAssigned</td>
<td>Runs when an incident is assigned to a Service Queue.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnTicketClosed</td>
<td>Runs when an incident is finally closed.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnIncidentEdited</td>
<td>Runs when a technician edits the details of a ticket.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnTicketPlacedOnHold</td>
<td>Runs when an incident is put on hold.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnTicketRemovedFromHold</td>
<td>Runs when an incident is removed from hold.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnTicketReopened</td>
<td>Runs when a closed incident is reopened.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnTicketResolved</td>
<td>Runs when an incident is resolved.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnVerificationTimeout</td>
<td>Runs if the primary contact does not verify the incident within the verification window.</td>
<td>Process Event</td>
</tr>
<tr>
<td>OnAnySlaCompletedLate</td>
<td>Runs when an SLA is complete late: Initial Response or Resolution.</td>
<td>Data Event</td>
</tr>
<tr>
<td>OnAnySlaMissed</td>
<td>Runs if an SLA is reached before action is completed: Initial Response or Resolution.</td>
<td>Data Event</td>
</tr>
<tr>
<td>ContactAdded</td>
<td>Runs if a contact is added to an incident. The ruleset is not enabled by default.</td>
<td>Data Event</td>
</tr>
<tr>
<td>DocumentAdded</td>
<td>Runs if a document is added to an incident. For example, you add an asset to an incident. The ruleset is not enabled by default.</td>
<td>Data Event</td>
</tr>
<tr>
<td>ProcessReferenceCreated</td>
<td>Runs when a process reference is added to an incident. The ruleset is not enabled by default.</td>
<td>Data Event</td>
</tr>
</tbody>
</table>
### Incident Management rulesets (continued)

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Description</th>
<th>Event type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TaskAssignmentCreated</td>
<td>Runs when a subtask is assigned on an incident.</td>
<td>Data Event</td>
</tr>
<tr>
<td></td>
<td>The ruleset is not enabled by default.</td>
<td></td>
</tr>
<tr>
<td>TaskCompleted</td>
<td>Runs when a subtask on a ticket is completed.</td>
<td>Data Event</td>
</tr>
<tr>
<td></td>
<td>The ruleset is not enabled by default.</td>
<td></td>
</tr>
</tbody>
</table>

### Incident Management automation rules conditions

The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process.


See “Configuring new automation rules for Incident Management” on page 214.

Conditions determine when an action should occur. You can add multiple conditions to a rule.

### Table 18-2 Ruleset conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Condition availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected Assets</td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If any assets are attached to an incident</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If specific assets are attached to an incident</td>
<td></td>
</tr>
<tr>
<td>Affected Business Service</td>
<td>If a specific service is attached to an incident</td>
<td>All rulesets</td>
</tr>
<tr>
<td>Affected Departments</td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If an affected department is set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If a specific department is set</td>
<td></td>
</tr>
<tr>
<td>Affected Location</td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If an affected location is set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If a specific location is set</td>
<td></td>
</tr>
</tbody>
</table>
## Table 18-2

Ruleset conditions (continued)

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Condition availability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Affected User</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If the affected user is also the submitter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If the affected user is in a specific group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If the affected user is a VIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If the affected user is a specific user</td>
<td></td>
</tr>
<tr>
<td><strong>Any</strong></td>
<td>Runs the rule on all incidents</td>
<td>All rulesets</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ Runs the rule on all incidents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If an Incident has been classified If a specific classification is set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If a specific subclassification is set</td>
<td></td>
</tr>
<tr>
<td><strong>Contacts</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If a contact exists</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If a contact on the incident is part of a specific group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If a contact on the incident is a specific contact</td>
<td></td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If an impact is set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If a specific impact is set</td>
<td></td>
</tr>
<tr>
<td><strong>Incident Description</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If the descriptions contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If the description starts with text</td>
<td></td>
</tr>
<tr>
<td><strong>Incident Title</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If the title contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If the title starts with text</td>
<td></td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If a priority is set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If a specific priority is set</td>
<td></td>
</tr>
</tbody>
</table>
### Table 18-2  
**Ruleset conditions (continued)**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Condition availability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Name</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If the process name contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If the process name starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If the process name is a specific text</td>
<td></td>
</tr>
<tr>
<td><strong>Random</strong></td>
<td>Random pass based on a target % between 0 and 100</td>
<td>All rulesets</td>
</tr>
<tr>
<td><strong>Request Channel</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ Incident is created from the service catalog</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Incident is created from the Technician Page</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Incident is created from an Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Incident is created from a Custom entry point</td>
<td></td>
</tr>
<tr>
<td><strong>SLA Exists</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ SLA Exist for Milestone: Initial Response or Resolution.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A specific SLA exist</td>
<td></td>
</tr>
<tr>
<td><strong>SLA Status (by Escalation)</strong></td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ If it is completed late for a specific milestone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If late for a specific milestone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If it is satisfied for a specific milestone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If working for a specific milestone</td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
<td>Condition availability</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>SLA Status (by Level)</td>
<td>Options:&lt;br&gt; ■ If it is completed late for a specific SLA level&lt;br&gt; ■ If late for a specific SLA level&lt;br&gt; ■ If it is paused for a specific SLA level&lt;br&gt; ■ If it is satisfied for a specific SLA level&lt;br&gt; ■ If working for a specific SLA level</td>
<td>All rule sets</td>
</tr>
<tr>
<td>Urgency</td>
<td>Options:&lt;br&gt; ■ If an urgency is set&lt;br&gt; ■ If a specific urgency is set</td>
<td>All rule sets</td>
</tr>
<tr>
<td>SLA Type</td>
<td>Is set to a specific type</td>
<td>OnAnySlaCompletedLate&lt;br&gt;OnAnySlaMissed</td>
</tr>
<tr>
<td>Comment</td>
<td>Options:&lt;br&gt; ■ Added comment contains text&lt;br&gt; ■ Added comment starts with text&lt;br&gt; ■ Added comment is specific text</td>
<td>CommentAdded</td>
</tr>
<tr>
<td>Commenter</td>
<td>Is a specific user</td>
<td>CommentAdded</td>
</tr>
<tr>
<td>Contact</td>
<td>Options:&lt;br&gt; ■ Added contact is primary contact&lt;br&gt; ■ Added contact is VIP&lt;br&gt; ■ Added contact is specific user</td>
<td>ContactAdded</td>
</tr>
<tr>
<td>Contact Location</td>
<td>Options:&lt;br&gt; ■ Added contact location contains text&lt;br&gt; ■ Added contact location starts with text&lt;br&gt; ■ Added contact location is specific text</td>
<td>ContactAdded</td>
</tr>
</tbody>
</table>
### Ruleset conditions (continued)

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Condition availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment Name</td>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added document name contains text</td>
<td>DocumentAdded</td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added document name starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added document name is specific text</td>
<td></td>
</tr>
<tr>
<td>Attachment Size</td>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added document is larger than KB</td>
<td>DocumentAdded</td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added document is smaller than KB</td>
<td></td>
</tr>
<tr>
<td>Process Reference Type</td>
<td>Added process reference is a specific type</td>
<td>ProcessReferenceCreated</td>
</tr>
<tr>
<td>Process Reference URL</td>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added process reference URL contains text</td>
<td>ProcessReferenceCreated</td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added process reference URL starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added process reference URL is specific text</td>
<td></td>
</tr>
<tr>
<td>Child Process Name</td>
<td>Options:</td>
<td>ProcessRelationshipCreated</td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added child process name contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added child process name starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added child process name is specific text</td>
<td></td>
</tr>
<tr>
<td>Child Process ServiceID</td>
<td>Options:</td>
<td>ProcessRelationshipCreated</td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added child process Service ID contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added child process Service ID starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ 🎯 Added child process Service ID is specific text</td>
<td></td>
</tr>
</tbody>
</table>
**Incident Management automation rules actions**

The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process.

See “**Incident Management Process Automation rules components**” on page 203.

See “**Configuring new automation rules for Incident Management**” on page 214.

Actions are the result of a rule when the conditions are met. You can add multiple actions to a rule.

---

**Table 18-2 Ruleset conditions (continued)**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Condition availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Relationship Name</td>
<td>Options:</td>
<td>ProcessRelationshipCreated</td>
</tr>
<tr>
<td></td>
<td>- Added process relationship name contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Added process relationship name starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Added process relationship name is specific text</td>
<td></td>
</tr>
<tr>
<td>Task Assignee</td>
<td>Options:</td>
<td>TaskAssignmentChanged</td>
</tr>
<tr>
<td></td>
<td>- New task assignee contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- New task assignee starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- New task assignee is specific text</td>
<td></td>
</tr>
<tr>
<td>Task Name</td>
<td>Options:</td>
<td>TaskAssignmentChanged TaskCreated TaskCompleted</td>
</tr>
<tr>
<td></td>
<td>- New task name contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- New task name starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- New task name is specific text</td>
<td></td>
</tr>
<tr>
<td>Task Priority</td>
<td>Options:</td>
<td>TaskAssignmentChanged TaskCreated TaskCompleted</td>
</tr>
<tr>
<td></td>
<td>- New task priority contains text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- New task priority starts with text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- New task priority is specific text</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Action availability</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Add Contact</td>
<td>Adds a contact to the incident and defines contact information.</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Define Contact Type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Define Is Primary.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Define User.</td>
<td></td>
</tr>
<tr>
<td>Do Nothing</td>
<td>Take no action</td>
<td>All rulesets</td>
</tr>
<tr>
<td>Grant Ticket Access</td>
<td>Sets the permissions for the ticket</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Set Can Administrate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Set Can Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Set Can View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Grants access to ticket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ To User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ To Group</td>
<td></td>
</tr>
<tr>
<td>Modify SLA</td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ Complete for Milestone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Delete for Milestone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Reset for Milestone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Resume for Milestone</td>
<td></td>
</tr>
<tr>
<td>Pause SLA</td>
<td>By Milestone</td>
<td>All rulesets</td>
</tr>
<tr>
<td>Remove Ticket Access</td>
<td>Options:</td>
<td>All rulesets</td>
</tr>
<tr>
<td></td>
<td>■ From Everyone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ From Specific User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ From Specific Group</td>
<td></td>
</tr>
</tbody>
</table>
### Table 18-3 (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Action availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Email</td>
<td>Send Email Options:</td>
<td>All rule sets</td>
</tr>
<tr>
<td></td>
<td>■ To Affected User</td>
<td>Data event email templates are only</td>
</tr>
<tr>
<td></td>
<td>■ To Submitter</td>
<td>available to the specific events</td>
</tr>
<tr>
<td></td>
<td>■ To all Assignees</td>
<td>to which they are tied.</td>
</tr>
<tr>
<td></td>
<td>■ To Owner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ To Resolver</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ To Specific Group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ To Specific User</td>
<td></td>
</tr>
<tr>
<td>Send Incident To Workflow</td>
<td>Defines URL of Workflow, evokes workflow, and passes session ID for incident</td>
<td>All rule sets</td>
</tr>
<tr>
<td>Set SLA</td>
<td>Sets SLA for an incident and define Options:</td>
<td>All rule sets</td>
</tr>
<tr>
<td></td>
<td>■ Replace existing SLA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SLA calculation start time (Submit Date / Now)</td>
<td></td>
</tr>
<tr>
<td>Route Incoming Ticket</td>
<td>Assign ticket to Service Queue Options:</td>
<td>Process event type rulesets</td>
</tr>
<tr>
<td></td>
<td>■ To Specific Service Queue</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Based on Category Table</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Based on Location Table</td>
<td></td>
</tr>
<tr>
<td>Set Impact</td>
<td>Set Impact for Incident</td>
<td>Process event type rulesets</td>
</tr>
<tr>
<td>Set Location</td>
<td>Set incident location Options:</td>
<td>Process event type rulesets</td>
</tr>
<tr>
<td></td>
<td>■ To Affected User’s Location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ To Specific Location</td>
<td></td>
</tr>
<tr>
<td>Set Owner</td>
<td>Assign Owner for an incident to a specific user</td>
<td>Process event type rulesets</td>
</tr>
<tr>
<td>Set Priority</td>
<td>Set Priority for Incident</td>
<td>Process event type rulesets</td>
</tr>
<tr>
<td>Reassign Current Incident Task</td>
<td>Reassign incident to a specific queue</td>
<td>Data event type rulesets</td>
</tr>
</tbody>
</table>
Configuring new automation rules for Incident Management

You can configure rulesets for the Incident Management process. The set of rulesets is known as the automation library.

Video: For more information about configuring new automation rules for Incident Management, see the following on videos Symantec Connect:

- ServiceDesk: Rulesets Overview
- ServiceDesk Configuration: Data Mapping and Routing Rules
- ServiceDesk: SLA Framework Overview
- ServiceDesk Configuration: Manage Email Templates


See “About Incident Management” on page 127.

To configure a new automation rule for Incident Management

1. In the Process Manager portal, click Admin > Process Automation.
2. On the Available Services page, expand Incident Management and then click Service Dashboard.
3. On the Automation Rules page, in the Service Dashboard: INCIDENT-MGMT section, locate the ruleset to which you want to add a rule.
4. To the right of the ruleset, click the Actions symbol (orange lightning) and then click Add Rule.

See “Incident Management automation rules rulesets” on page 204.

5. In the Add Rule dialog box, in the How groups are evaluated area, select one of the following options:
   - All groups must be met to satisfy
   - Any group satisfies

6. Click Add Group.
7. Click Add Condition.
8. In the How conditions in this group are evaluated area, select one of the following options:
   - All conditions must be met to satisfy
   - Any condition satisfies
9 In the **Add Condition** drop-down list, select a condition for the rule.

   See **“Incident Management automation rules conditions”** on page 206.

10 Select an option from each drop-down list that appears or type the information in the specified field to narrow the parameters of the condition.

11 (Optional) Check **Not** to set a condition that inverts the selected condition so that the rule only executes if the condition is false.

   The **Not** operator applies only to the condition, not to the entire rule.

12 Click the **Plus** symbol (blue plus sign) to add the condition.

13 (Optional) Click the **Plus** symbol (blue plus sign) to add another condition.


14 Click **Add Action**.

15 In the **Actions** drop-down list, select an action to execute if the condition is met.

   See **“Incident Management automation rules actions”** on page 211.

16 Select an option from each drop-down list that appears or type the information in the specified field to narrow the parameters of the action.

17 Click the **Plus** symbol (blue plus sign) to add the action.

18 (Optional) Click the **Plus** symbol (blue plus sign) to add another action. Repeat Steps 15 - 18.

19 In the Disposition (on successful actions) area, select one of the following options:

   ■ **Continue**

   ■ **Stop**
20 (Optional) Click **Advanced** and select which of the following actions you want to include in the ruleset:

**Run next rule if condition fails to evaluate**  
If an error occurs during the evaluation of an incident's conditions, the ruleset continues to execute (if not checked, the ruleset does not execute).

**Run next rule if action fails to execute**  
If an error occurs while the condition executes, the ruleset attempts to continue executing.

21 Click **Save**.
Managing changes

- Chapter 19. Introducing Change Management
- Chapter 20. Submitting change requests
- Chapter 21. Scheduling and planning changes
- Chapter 22. Approving and implementing changes
Introducing Change Management

This chapter includes the following topics:

- About Change Management
- About the Change Management process
- Change Management process: Planned state
- Change Management process: Received State
- Change Management process: Reviewed state
- Change Management process: Closed state
- Actions in the Change Management process states
- Configuring Change Management
- Change request rulesets
- Configuring change request rulesets
- Creating email templates for Change Management
- Editing email templates for Change Management
- Deleting email templates for Change Management
- About the roles in Change Management
About Change Management

The goal of Change Management is to standardize methods and procedures to ensure the most efficient handling of the changes that an organization requires. An effective Change Management process minimizes how changes affect service and improves the reliability and responsiveness of IT services and processes. This improvement leads to a quicker turnaround on changes and reduces unplanned work, rework, and duplicated efforts.

Change Management includes the following key features:

■ Problems can be escalated to a change request or change requests can be initiated independently.

■ The Automation rules designer lets you execute actions based on eight potential decision points.

■ The eight decision points, or rulesets, let you create rules for routing, email, and other actions. When the ruleset is initiated, the rules execute automatically.

■ In addition to the eight default rulesets, you can create your own rulesets based on your organization's requirements.

■ The change approval board analyzes the risk that is associated with the change as part of the process.

■ Supports multiple change managers, each with their own customized rights to tickets and actions.

■ All participants review the proposed schedule.

■ All the plans that are created as part of the Change Management process are stored with the change request and easily accessible to all participants.

■ Users can consult the Forward Schedule of Change calendar to avoid scheduling conflicts when they plan changes. The Forward Schedule of Change calendar provides visibility into other planned changes, outages, change freeze periods, and holidays.

■ When the plans are finalized, the change approval board provides final approval, and the implementation task is assigned based on the scheduled date and time.

■ When a change request is completed, the problems and incidents that are associated with that change request are automatically updated with a resolution and closed.

The Change Management process interacts with the other ServiceDesk processes as follows:

■ Obtains incident information from the Incident Management process.
About the Change Management process

The Change Management process ensures that standardized methods and procedures are used to handle all changes efficiently and promptly. The process minimizes the effect of any related incidents upon service. Using Change Management improves the reliability and responsiveness of IT services and processes, leading to a higher turnaround of changes. It also reduces rework and the duplication of effort. Standard or common change requests can be expedited. The use of automation rules enables customization without having to edit the workflow directly. The process includes the ability to define and use templates for quickly completing a change plan.

The Change Management process is initiated when someone requests a change. The change manager who provides the initial approval of a change request also selects the change type. The change type determines the number of steps that the change implementation requires. It also determines the number of workers who must be involved in each step.

When a task is assigned to multiple workers, all the assignees must complete the task for the change request to advance to the next stage. The change manager can complete tasks on behalf of the task assignees by checking the Work Tasks Assigned To Others check box on the change request’s Process View page. This option helps move the process forward if a task assignee is unavailable, on vacation, or otherwise unable to work the task.

The Change management process consists of the following states:

- Received
  
  See “Change Management process: Received State” on page 223.

- Planned
  
  See “Change Management process: Planned state” on page 222.

- Reviewed
  
  See “Change Management process: Reviewed state” on page 224.
During the planning phase, the change manager can select one of two variations to tailor the process to the request: Standard or Emergency.

A standard plan change is commonly requested and performed, meaning that procedures, risk and cost are well-understood and CAB approval is not necessary. Essentially, the Planned state is skipped. For example, once a computer has become obsolete, it experiences a standard change of repurposing or disposal. A standard change is usually scheduled for a later time to coincide with maintenance windows or a release. Typically, an organization has a one-to-one mapping between standard plans and plan templates. This one-to-one mapping is so that if the Standard type is selected, the change manager can find the matching template, and load the plan details.

An emergency change cannot be scheduled for later. If it is designated as an emergency, then it should be implemented immediately following approval by the E-CAB. Like the Standard plan type, the plan details are not required before submission to the CAB.

Change Management process: Planned state

The Planned state is a state in the Change Management process.

The Change Manager has submitted the change plan to the CAB for approval. The change manager selects the CAB during the Received state. The CAB can either approve or reject the plan. The CAB can opt to schedule it for a later time. This state is skipped if the Change Manager chooses the Standard plan type.

The table describes the details of the Planned state in the Change Management process.

<table>
<thead>
<tr>
<th>State name:</th>
<th>Planned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief description:</td>
<td>Change Manager submits the change plan to the CAB for approval.</td>
</tr>
<tr>
<td>Initiated by:</td>
<td>Change Manager completes and submits change plan</td>
</tr>
<tr>
<td>Outcome/Next status:</td>
<td>- Change scheduled for implementation (Reviewed)</td>
</tr>
<tr>
<td></td>
<td>- Change plan denied (Closed: DeniedByCab)</td>
</tr>
<tr>
<td>Players:</td>
<td>Change Approval Board (CAB/ECAB)</td>
</tr>
</tbody>
</table>
Change Management process: Received State

The Received state is a state in the Change Management process.

See “About the Change Management process” on page 221.

In this state, the Change Manager receives the change request and is ready for planning. During this state, the Change Manager can delegate portions of the planning to others.

The table describes the details of the Received state in the Change Management process.

<table>
<thead>
<tr>
<th>State name:</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief description:</td>
<td>The request has been received and the Change Manager reviews it.</td>
</tr>
<tr>
<td>Initiated by:</td>
<td>Change request submitted</td>
</tr>
<tr>
<td>Outcome/Next status:</td>
<td>Plan completed and submitted to CAB for review (Planned)</td>
</tr>
<tr>
<td></td>
<td>CAB approval is bypassed and change is scheduled (Reviewed)</td>
</tr>
<tr>
<td></td>
<td>Request denied (Closed: DeniedByCm)</td>
</tr>
</tbody>
</table>

| Players: | Change manager, selected delegates |
Change Management process: Reviewed state

The Reviewed state is a state in the Change Management process. See “About the Change Management process” on page 221.

In this state, CAB approval was either provided or was not needed. During this phase the change is implemented, either immediately or at the scheduled time.

The table describes the details of the Reviewed state in the Change Management process.

| State name: | Reviewed |
| Brief description: | The change plan has been approved and is scheduled for implementation |
| Initiated by: | CAB approves Change plan or the Change Manager initiates change directly (for Standard plan) |
| Outcome/Next status: | ▪ Change successfully implemented (Closed: Success)  
▪ Change cannot be implemented (Closed: Failure) |
| Players: | Implementer is selected during the planning phase |
Available actions:

■ Task: Cancel Change
■ Task: Implement Right Away
■ Task: Complete Task
■ Implementation Options: Delegate Implementation Task
■ Implementation Options: Manage Implementation Tasks
■ Process Action: Edit Change Plan
■ Process Action: Manage CABs
■ Process Action: Manage Templates
■ Process Action: Manage Related Configuration Items
■ Process Action: Manage Related Processes
■ Process Action: Add Bulletin Board Entry
■ Process Action: Search Knowledge Base

Change Management process: Closed state

The Closed state is a state in the Change Management process.

See “About the Change Management process” on page 221.

To reach this state, a close code must be provided. It can be one of the following:

■ Success – The change was implemented.
■ Failure – The change cannot be implemented for some reason.
■ DeniedByCm – Change manager denies Request.
■ DeniedByCab – CAB denies the plan.

The table describes the details of the Closed state in the Change Management process.

State name: Closed
Brief description: No further action is taken on the ticket
Initiated by: Change Manager denies change request, CAB denies change plan, or Implementer marked change as Completed
Outcome/Next status: N/A
Players: N/A
Available actions:  
Process Action: **Edit Change Plan**  
Process Action: **Manage CABs**  
Process Action: **Manage Templates**  
Process Action: **Manage Related Configuration Items**  
Process Action: **Manage Related Processes**  
Process Action: **Add Bulletin Board Entry**  
Process Action: **Search Knowledge Base**

### Actions in the Change Management process states

In each state in the Change Management process, specific types of actions are available. Each action is associated with a specific user role.

See “About the Change Management process” on page 221.

The following types of actions are available in the Change Management process:

- **Task**
  
  A **Task** is an actual workflow step. The completion of a task moves the process along.

- **Planning Tasks, Implementation Options, and CAB Options**
  
  **Planning Tasks, Implementation Options, and CAB Options** are additional actions, which are specific to a user or a group at a specific moment in the process. After the user or group completes the main task that is assigned to them, the additional actions are no longer available.

- **Process Action**
  
  A **Process Action** is an action that anyone with the appropriate access level to the process can perform, regardless of process state. This action can be used to edit ticket data directly, and so forth. It may or may not provide an alternative to completing the main task or advancing the process along.
Table 19-1 Change Management process actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Initiator of Action</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Approve/Deny Change Plan| Change Manager      | Task            | ■ Provide state-sensitive elements of the change plan, such as the designated CAB, the change type, and the implementer.  
■ Submit the change plan to the CAB, moving the process to the Planned state. |
| Delegate Implementation Plan | Change Manager | Planning Tasks | ■ Create tasks for selected delegates to complete portions of the change plan, like the implementation plan or the testing plan. Sets the status for the affected plan elements to Assigned.  
■ Remove delegated tasks or change their assignments. |
| Delegate Test Plan       | Change Manager      | Planning Tasks  |                                                                              |
| Delegate Backout Plan    | Change Manager      | Planning Tasks  |                                                                              |
| Delegate Other Task      | Change Manager      | Planning Tasks  | ■ Provide a generic tasking ability for the Change Manager to use to assign tasks like testing a change ahead of implementing it. These tasks are not bound to the process state, so they do not delay the main process. |
Table 19-1  Change Management process actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Initiator of Action</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Change Plan</td>
<td>Change Manager, selected delegates, CAB</td>
<td>Process Action</td>
<td>■ Provide non-state-sensitive elements of the change plan, such as the risk, cost, and plan elements (implementation, testing, and backout).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Implemented as a Process Action to allow editing of a change plan at any process state. Also, anyone with administrative or edit rights to the process can edit the plan.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Used by the plan element delegates to provide details for their plan element.</td>
</tr>
<tr>
<td>Manage CABs</td>
<td>Change Manager</td>
<td>Process Action, Service Catalog Item</td>
<td>■ Add, remove, and edit CABs (available only to those with administrative rights to the process).</td>
</tr>
<tr>
<td>Manage Related</td>
<td>Change Manager</td>
<td>Process Action</td>
<td>■ Associate configuration items from the CMDB with the change request.</td>
</tr>
<tr>
<td>Configuration Items</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 19-1  
Change Management process actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Initiator of Action</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Manage Related Processes              | Change Manager      | Process Action | • Lets you add or remove the incidents that are associated with the change request. Adding incidents to a change request creates a cascading relationship, whereby the successful completion of the change triggers the closure of any associated incidents.  
• Lets you add or remove the problems that are associated with the change request. Adding problems to a change request creates a cascading relationship, whereby the successful completion of the change triggers the closure of any associated incidents. |
| Approve Change Plan                   | CAB/ECAB            | Task     | • Used by the CAB to move the process to the next state.  
• Can approve or deny change plan.  
• Can add process documents           |
| Complete Task (Fulfill Request)       | Implementer         | Task     | • Used by the implementer to indicate that the task is complete.  
• Can choose close code of Success or Failure.  
• Must enter comments if close code is Failure. |

### Configuring Change Management

To configure change management you define the change manager group. Next you configure access to the Service Catalog items and to the change request process view. Then you set up email templates. Finally, you configure automation rules.
**Table 19-2**  Process for configuring Change Management

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Define your Change manager group or groups</td>
<td>Your organization may have several different groups responsible for managing incoming change requests. Which group manages the incoming change may depend on the category, location, or other attributes of the request. You must create these groups in the portal and add people to them as needed. See “About the roles in Change Management” on page 239.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure Access to the Service Catalog Items</td>
<td>ServiceDesk Installation adds three service catalog items: Request Change, Manage CABs, and Manage Change Templates. By default, the Request Change item is accessible to anyone in the All Users group. However, this form is contained in the ServiceDesk category, which is not accessible to all users. If this access level is not desirable, you should change it in Admin &gt; Service Catalog Settings. Select to edit categories or forms and then add permissions as desired. Manage CABs and Manage Change Templates are only accessible to Administrators by default. You may want to grant access to these items to your change manager group or groups. See “Requesting a change” on page 242.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Access to the Change Request Process View</td>
<td>The process view page for Change Management is very robust. The page contains a full description of the request. It also contains the current implementation plan, history of the ticket, current assignments, etc. You can grant access to other users or groups to the full view in the Admin &gt; Portal &gt; Manage Pages screen. The page is located under the Process View Pages category and is called SD Change View. Select Edit Page, and then open the Permissions tab.</td>
</tr>
</tbody>
</table>
Table 19-2  Process for configuring Change Management (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Set up Email Templates</td>
<td>In Change Management, you have complete control over who receives notifications and what those notifications look like. You have control over when the notifications are sent, without ever needing to open the process in the Workflow Designer. You can customize the templates by determining what your notification rules should be and what the notifications should contain. For example, you may want to notify the requestor as soon as the system receives the ticket. You may want to notify the requestor after the ticket has been approved at each level. Email templates for this process can be configured in Admin &gt; Automation Rules. See “Creating email templates for Change Management” on page 234.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure Automation Rules</td>
<td>This step requires time for testing and configuration. To set up automation rules properly, it’s important to understand the underlying process. The actions available in the rule builder give you the ability to change information about the ticket while the ticket executes. For example, when a ticket is received, you might check if the requestor is a VIP and automatically set the ticket owner and send email. Typically, the first ruleset you want to configure is the OnChangeReceived ruleset. This ruleset is enacted upon the receipt of a change request. See “Configuring change request rulesets” on page 232.</td>
</tr>
</tbody>
</table>

Change request rulesets

Rulesets allow the administrator to configure the Change Management process. Configurations based on ticket routing, prioritization, and urgency can play a role in change requests. You can configure change request rulesets.

See “Configuring change request rulesets” on page 232.
The following table describes the change request rulesets that allow for routing, and prioritization.

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnCabApproval</td>
<td>Executed when the CAB approves a change plan and submits it for implementation.</td>
</tr>
<tr>
<td>OnChangeReceived</td>
<td>Executed when the system receives a change request. Use for routing, prioritization, auto-planning, and notification.</td>
</tr>
<tr>
<td>OnImplementationCompleted</td>
<td>Executed when a change has been successfully completed.</td>
</tr>
<tr>
<td>OnImplementationDateReached</td>
<td>Executed when the Planned Start Date for a change has been reached.</td>
</tr>
<tr>
<td>OnImplementationPlanFailed</td>
<td>Executed when implementer indicates that they were unable to implement the change.</td>
</tr>
<tr>
<td>OnPlanningCompleted</td>
<td>Executed when the change manager (Gatekeeper) approves and submits a change request.</td>
</tr>
<tr>
<td>OnPlanRejectedByCab</td>
<td>Executed when the CAB rejects a change plan.</td>
</tr>
<tr>
<td>OnRequestRejectedByCm</td>
<td>Executed when the CM (Gatekeeper) has denied a change request.</td>
</tr>
</tbody>
</table>

**Configuring change request rulesets**

You can configure change request rulesets. The set of rulesets is known as the automation library.

**To configure change request rulesets**

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Change Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Service Dashboard: CHANGE-MGMT** section, locate the ruleset to which you want to add a rule.

The rulesets are defined in the Change request rulesets section.

See “**Change request rulesets**” on page 231.
4 To the right of the ruleset, click the Actions symbol (orange lightning) and then click Add Rule.

5 In Add Rule dialog box, in the How groups are evaluated area, select one of the following options:
   - All groups must be met to satisfy
   - Any group satisfies

6 Click Add Group.

7 Click Add Condition.

8 In the How conditions in this group are evaluated area, select one of the following options:
   - All conditions must be met to satisfy
   - Any condition satisfies

9 In the Add Condition drop-down list, select a condition for the rule.

10 Select an option from each drop-down list that appears or type the information in the specified field to narrow the parameters of the condition.

11 (Optional) Check Not to set a condition that inverts the selected condition so that the rule only executes if the condition is false.
   The Not operator applies only to the condition, not to the entire rule.

12 Click the Plus symbol (blue plus sign) to add the condition.

13 (Optional) Click the Plus symbol (blue plus sign) to add another condition. Repeat Steps 9 - 13.

14 Click Add Action.

15 In the Actions drop-down list, select an action to execute if the condition is met.

16 Select an option from each drop-down list that appears or type the information in the specified field to narrow the parameters of the action.

17 Click the Plus symbol (blue plus sign) to add the action.

18 (Optional) Click the Plus symbol (blue plus sign) to add another action. Repeat Steps 15 - 18.

19 In the Disposition (on successful actions) area, select one of the following options:
   - Continue
   - Stop
(Optional) Click Advanced and select which of the following actions you want to include in the ruleset:

- **Run next rule if condition fails to evaluate**: If an error occurs during the evaluation of an incident’s conditions, the ruleset continues to execute (if not checked, the ruleset does not execute).
- **Run next rule if action fails to execute**: If an error occurs while the condition executes, the ruleset attempts to continue executing.

Click **Save**.

**Creating email templates for Change Management**

Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. You can create email templates and associate them with actions. For example, if a change management request requires the approval of a director-level individual, a preconfigured email can be sent to that individual. The email template can be preconfigured with subject line and message information.

**Note**: The Send Email process type action, on the Change Management Process View page uses the Change Management email templates. You may want to create email templates specifically for your change analyst, approvers, and others to use when working a change request ticket.

See “Change request rulesets” on page 231.

**To create an email template**

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the Available Service page, expand **Change Management** and then click **Service Dashboard**.
3. On the Automation Rules page, in the Actions: CHANGE-MGMT section, click **Manage Email Templates**.
4 On the Notification Templates page, in the Email Templates section, click Add Email Template.

5 In the Add Email Template dialog box, in the Template Type area, select one of the following template types:

**Process Event**
- Lets you create an email template for process event rulesets.
- The list of available fields in the Available Fields section corresponds specifically to process events.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset.
- For example, a process event email template can be delivered from the OnChangeReceived ruleset.

**Data Event**
- Lets you create an email template for a specific data event ruleset.
- Lets you use the Event field to assign a data event category to the email template.
- The list of available fields in the Available Fields section corresponds specifically to the type of data events that you select.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event.
- Note that the email template is only available for its corresponding data event ruleset.
- For example, you create a ruleset for `<OnDocumentAdded>` data event. You create a rule to deliver an email anytime a document is added to the change request ticket. When you create the email template for this rule, you must select DocumentAdded in the Event drop-down list.

6 (Optional) If you selected **Data Event**, in the Event drop-down list, select a data event.

   For example, you want to create an email template so you can send an email out when a comment is added to a change ticket. In the Event drop-down list, click **CommentAdded**.

7 In the Name field, type the name for the email template.

   This name displays on the Notification Templates page, in the Email Templates section.
8 (Optional) In the **Description** field, type the description of the email template.

This description displays on the **Notification Templates** page in the **Email Templates** section.

9 In the **From** field, type the name of the user or group sending the message.

10 (Optional) In the **Subject** field, type the subject of the email.

11 (Optional) In the **Body** field, type the message.

If you want to let the end user's reply to the emails and have ServiceDesk capture those emails, you must add a reply code.

Use the following format:

```
{IID= ${WorkflowTrackingId}}
```

`${WorkflowTrackingId}` is the variable that is added to the body of the email when you select **Workflow Tracking ID** in the **Available Fields** section.

12 (Optional) Add additional information to a specific area of the email.

- In the **Add To** area, select the field (**From**, **Subject**, or **Body**) to which you want to add the additional information.
- Then, in the **Available Fields** section, select the fields that you want to add.
- Repeat this step until you are finished adding additional information.

13 When you are finished, click **Save**.

See “**Editing email templates for Change Management**” on page 236.

See “**Deleting email templates for Change Management**” on page 239.

## Editing email templates for Change Management

You can edit email templates if necessary. If you edit an email template before you use it in the **Send Email** action of a rule, you can edit all parts of the template. If you edit an email template after you use it in the **Send Email** action of a rule, do not edit the **Template Type**. **Template Type** makes the email template available only to rulesets that correspond to the event type that you select.

For example, process event email templates are only available to process event type rulesets. If you want to use that same email template for a different template type, you need to create a new email template. Then, you need to create a new rule to deliver it.
**Note:** Do not change the **Template Type** in an email template after you use it in a rule. Changing the **Template Type** appears to remove the selected email template from the **Send Email** action of the rule. Because the rule uses the ID number of the email template, the email is still sent, but it may not display the information as expected.

**To edit an email template**

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Change Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: CHANGE-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section locate the email template that you want to edit. To the right of the email template, click the **Action** symbol (orange lightning) and then click **Edit Email Template**.
5. (Optional) In the **Edit Email Template** dialog box, **Template Type** area change the **Template Type** only if you have not created a rule that delivers the email template.

**Process Event**

- Lets you create an email template for process event rulesets.
- The list of available fields in the **Available Fields** section corresponds specifically to process events.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset. For example, a process event email template can be delivered from the **OnChangeReceived** ruleset.
Data Event

- Lets you create an email template for a specific data event ruleset.
- Lets you use the Event field to assign a data event category to the email template.
- The list of available fields in the Available Fields section corresponds specifically to the type of data events that you select.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event.

Note that the email template is only available for its corresponding data event ruleset.

For example, you create a ruleset for `<OnDocumentAdded>` data event. You create a rule to deliver an email anytime a document is added to the change request ticket. When you create the email template for this rule, you must select DocumentAdded in the Event drop-down list.

6 (Optional) If you changed the template type to Data Event, in the Event drop-down list, select a data event.

For example, you want to edit the email template so you can send an email out when a comment is added to a change ticket. In the Event drop-down list, click CommentAdded.

7 (Optional) In the Name field, edit the name for the email template.

This name displays on the Notification Templates page, in the Email Templates section.

8 (Optional) In the Description field, edit the description of the email template.

This description displays on the Notification Templates page in the Email Templates section.

9 (Optional) In the From field, edit the name of the user or group sending the message.

10 (Optional) In the Subject field, edit the subject of the email.

11 (Optional) In the Body field, edit the message.

12 (Optional) Add additional information to a specific area of the email.

- In the Add To area, select the field (From, Subject, or Body) to which you want to add the additional information.
- Then, in the Available Fields section, select the fields that you want to add.
Repeat this step until you are finished adding additional information.

13 (Optional) Remove additional information from a specific area of the email.
14 Click Save.

See “Creating email templates for Change Management” on page 234.

See “Deleting email templates for Change Management” on page 239.

Deleting email templates for Change Management

You can delete email templates if necessary. If you need to delete an email template before creating a rule that delivers it, you can delete it without taking any other actions. To delete an email template after you create a rule that delivers it, you need to edit the rule and select a different email template. You can also delete the rule and then delete the email template.

To delete an email template

1 In the Process Manager portal, click Admin > Process Automation.

2 On the Available Services page, expand Incident Management and then click Service Dashboard.

3 On the Automation Rules page, in the Actions: CHANGE-MGMT section, click Manage Email Templates.

4 On the Notification Templates page, in the Email Templates section locate the email template that you want to delete.

5 To the right of the email template, click the Action symbol (orange lightning) and then click Delete Email Template

6 In the Message from webpage dialog box, click OK.

See “Creating email templates for Change Management” on page 234.

See “Editing email templates for Change Management” on page 236.

About the roles in Change Management

ServiceDesk employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes. The roles in the Change Management process are tasked with efficiently managing all changes to minimize the effect of any related incidents on service quality.

See “About the Change Management process” on page 221.
### Table 19-4  Roles in Change Management

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Submitter                   | The submitter is any worker who can request a change. Typically, the submitter is a support technician or manager, a change worker, or a problem manager.  
                               | See “Sources of change requests” on page 241.                                                                                               |
| Change manager (CM)         | The change manager can be anyone who is assigned to the Change Manager group. The change manager is responsible for the daily activities of the Change Management process.  
                               | The change manager authorizes and documents all changes in the IT infrastructure and its components (configuration items) to reduce the amount of unplanned down time. |
| Change Approval Board (CAB) | The change advisory board (CAB) is a group of people who can advise the change manager in the assessment, prioritization, and scheduling of changes. |
Submitting change requests

This chapter includes the following topics:

- Sources of change requests
- Requesting a change
- About change templates
- Creating a new change template
- Editing a change template
- Deleting a change template
- Using a change template

Sources of change requests

The creation of a change request triggers the Change Management process. A change request can originate from several sources.

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Management</td>
<td>A support technician or manager can create a change request as follows:</td>
</tr>
<tr>
<td></td>
<td>- From an incident ticket's Process View page</td>
</tr>
<tr>
<td></td>
<td>See “Creating a change request from an incident” on page 176.</td>
</tr>
<tr>
<td></td>
<td>- From the Submit Request portal page</td>
</tr>
<tr>
<td></td>
<td>See “Requesting a change” on page 242.</td>
</tr>
<tr>
<td></td>
<td>Typically, support technicians create change requests when they see a pattern of similar incidents.</td>
</tr>
</tbody>
</table>
Table 20-1  Sources of change requests (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Management</td>
<td>If the resolution of a problem requires a fix or change, the problem manager can create a change request from a problem ticket. See “Reviewing a proposed fix or workaround” on page 277.</td>
</tr>
<tr>
<td>Change Management</td>
<td>A change worker can create a new change request but in most cases, the change worker works on the change requests that other workers submit. A change worker can also clone an existing, completed change request. For example, if a change was made at one location, and you need to make the same change elsewhere, you can clone the original change.</td>
</tr>
</tbody>
</table>

### Requesting a change

A change worker or incident technician can create a change request that is not associated with other process tickets.

Creating a change request is a step in the Change Management process.

See “About the Change Management process” on page 221.

Change requests can also be created from incidents and from problem tickets.

See “Sources of change requests” on page 241.

#### To request a change

1. In the Process Manager portal, click Submit Request.
2. On the Submit Request page, under Service Catalog, click IT Services.
3. On the right side of the page, click Request Change.
4. In the Request a Change dialog box, on the Enter Change Request Details page, enter information about the change.

**Warning:** The Change Request form's Location field Search functionality does not discover locations. In the Location field, type in the location and use the auto-complete functionality of this field to select the location. Do not use the Search function to search for a location.

For more information, see the Symantec™ ServiceDesk 7.5 Release Notes.
5 (Optional) To attach a file to the change request, under Attach Supporting Documents, next to the Upload a File field, click Browse. Next, select the file(s) to upload. Then, click Attach.

You can also attach a file to the change request after it has been created. See “Attaching a file to an existing process ticket” on page 287.

6 On the Enter Change Request Details page, click Finish if you are finished or click Next to enter more information.

7 (Optional) On the Provide Risk Assessment page, in the Risk Score drop-down list, select a risk score. Next, in the Explanation field, type a justification for the score. Then, click Finish if you are finished or click Next to enter more information.

8 (Optional) On the Provide Cost Information page, type in a cost to implement and a cost not to implement. Then, click Finish if you are finished or click Next to enter more information.

9 (Optional) On the Provide Implementation Details page, type details about the Implementation Plan, Testing Plan, and Backout Plan. Then, click Finish if you are finished or click Next to enter more information.

10 (Optional) On the What equipment and services are affected by this change? page, in the Search the CMDB field, type the name of the equipment or service that you want to add and click Search. Select the item and click Add Selected. When you are finished, click Finish.

About change templates

After you create a change request, you can use a template to fill in the following change request information:

- Risk Assessment Score
- Cost of Implementing
- Cost of Not Implementing
- Implementation Plan
- Testing Plan
- Backout Plan

Using change templates speeds up the entry of change request information and helps to standardize and increase the accuracy of the change request information. For example, a template can help you create a change request for the occasional
change of a user's security configuration. By using a template, you can be sure that the correct steps are followed.

Change templates are useful when you have standardized plans for rolling out periodic maintenance changes. For example, you can use a template to provide the change request information for deploying hot fixes from Microsoft every two months. Once you create a change template, it is available from within a change request ticket's Process View page.

You can create a change template as follows:

- On the Submit Request portal page
  Click Administrative Services and then click Manage Change Templates.
- On a change request ticket's Process View page
  Under Process Actions, click Manage Templates.

See “Creating a new change template” on page 244.

See “Using a change template” on page 247.

Creating a new change template

You can create your own change templates. Using change templates speeds up the entry of change request information and helps to standardize and increase the accuracy of the change request information. For example, a template can help you create a change request for the occasional change of a user's security configuration. By using a template, you can be sure that the correct steps are followed.

To create a new change template

1. To open the Manage Change Plan Templates dialog box use one of the following options:

   **Option 1:**
   - In the Process Manager portal, click Submit Request.
   - On the Submit Request page, under Service Catalog, click Administrative Services.
   - On the right side of the page, click Manage Change Templates.
Option 2:  
- In the Process Manager portal, click My Task List.
- Under Task Viewer, under Project Name, expand SD.ChangeManagement.
- In the list of tasks, find and open the change request ticket.
- On the change request ticket’s Process View page under Process Actions, click Manage Templates.

3. In the Template Name field, type the name of the template.
4. (Optional) Provide the following information:
   - Template Description
   - Risk Assessment Score
   - Cost of Implementing
   - Cost of Not Implementing
   - Implementation Plan
   - Testing Plan
   - Backout Plan
5. Click Save Template.

See “About change templates” on page 243.
See “Using a change template” on page 247.
See “Editing a change template” on page 245.

Editing a change template

You can edit your change templates. For example, you may need to add additional steps to the testing plan section or increase the cost of implementing the change.

To edit a change template

1. To open the Manage Change Plan Templates dialog box use one of the following options:

   Option 1:
   - In the Process Manager portal, click Submit Request.
   - On the Submit Request page, under Service Catalog, click Administrative Services.
   - On the right side of the page, click Manage Change Templates.
Option 2:  
- In the Process Manager portal, click My Task List.
- Under Task Viewer, under Project Name, expand SD.ChangeManagement.
- In the list of tasks, find and open the change request ticket.
- On the change request ticket's Process View page under Process Actions, click Manage Templates.

2 On the Manage Change Plan Templates page to the right of the template that you want to edit, click Edit.

3 (Optional) In the Template Name field, edit the name of the template.

4 (Optional) Edit the following information:
   - Template Description
   - Risk Assessment Score
   - Cost of Implementing
   - Cost of Not Implementing
   - Implementation Plan
   - Testing Plan
   - Backout Plan

5 Click Save Template.

See “Creating a new change template” on page 244.
See “Deleting a change template” on page 246.

Deleting a change template

You can delete your change templates. For example, you may want to delete an obsolete change template.

To edit a change template

1 To open the Manage Change Plan Templates dialog box use one of the following options:

Option 1:  
- In the Process Manager portal, click Submit Request.
- On the Submit Request page, under Service Catalog, click Administrative Services.
- On the right side of the page, click Manage Change Templates.
Option 2:  
- In the Process Manager portal, click My Task List.
- Under Task Viewer, under Project Name, expand SD.ChangeManagement.
- In the list of tasks, find and open the change request ticket.
- On the change request ticket's Process View page under Process Actions, click Manage Templates.

2 On the Manage Change Plan Templates page to the right of the template that you want to delete, click Delete.

Warning: When you click Delete, your change template is permanently deleted.

See “Creating a new change template” on page 244.
See “Editing a change template” on page 245.

Using a change template

After an end user request a change, you can open the change request ticket and use a change template to fill in change plan information. Using change templates speeds up the entry of change request information and helps to standardize and increase the accuracy of the change request information.

To use a change template

1 In the Process Manager portal, click My Task List.
2 Under Task Viewer, under Project Name, expand SD.ChangeManagement.
3 In the list of tasks, find and open the change request ticket.
4 On the change request ticket's Process View page, under Process Actions, click Edit Change Plan.
5 In the Edit Change Plan dialog box, in the Load Template drop-down list, select the template that you want to use and click Load.
6 In the confirmation dialog box, click OK.
7 (Optional) In the Edit Change Plan dialog box, change the data or provide additional data.
8 Click Save Change Plan.
9 On the change request ticket's Process View page, under Tasks and Actions, click Approve/Deny Change Plan.
10 In the Complete Planning Phase dialog box, in the Set Change Plan Type drop-down list, click Standard.

11 In the Applied Template field, you should see the name of the template that you selected in the Edit Change Plan dialog box.

12 To the right of the Choose Implementer field, click the Search symbol (magnifying glass) to open the User Selection dialog box.

13 In the SearchText field, type your search criteria and click the Search symbol (magnifying glass).

14 Select the user and click Select User.

15 (Optional) To the right of the Choose Start Date drop-down list, click View Change Schedule to review other changes that are scheduled.

16 In the Choose Start Date drop-down list, select a start date.

17 In the Estimate End Date drop-down list, select an approximate end date.

18 (Optional) In the Add Comments (Optional) field, type your comments.

19 Select one of the following options:

- **Save** Saves the information and closes the page. Use this option if you plan to make changes to the change plan later.

- **Submit Change Plan** Submits the change plan so that the implementor can implement the change.

See “Creating a new change template” on page 244.

See “About change templates” on page 243.
Scheduling and planning changes

This chapter includes the following topics:

- Scheduling the implementation of a change plan

Scheduling the implementation of a change plan

You can schedule the implementation of a change plan. You can schedule the change from the change request ticket’s Process View page.

The change requestor provides a required by date for the change request. You can use the needed by date to schedule when the change request should be implemented. Typically, you schedule the implementation of a change plan after the planning tasks are completed.

Scheduling a change request is a step in the Change Management process.

See “About the Change Management process” on page 221.

See “About scheduling in ServiceDesk” on page 299.

To schedule the implementation of a change plan

1. In the Process Manager portal, click My Task List.

2. On the My Task List page, under Task Viewer, under Project Name, expand SD.ChangeManagement.

3. In the list of task, find and open the change request ticket that has the Change Manager Review and Approval status
4 On the change request’s Process View page, under Tasks and Actions, click Approve/Deny Change Plan.

If this action is not available, the task is probably not assigned to you. To enable this action and work the task anyway, under Tasks and Actions, click Work Tasks Assigned To Others if that option is available.

5 In the Complete Planning Phase dialog box, select a start date and an estimated end date for the change.

6 Click View Change Schedule.

7 On the Calendar page, check the schedules on the calendar to verify that your change dates do not interfere with any other scheduled events.

8 In the upper right corner of the page, click the Add Entry symbol (white paper with green plus sign).

9 In the Add Entry dialog box, select a schedule, type a name, and select start date and time and an event end date and time.

See “Add Entry dialog box” on page 304.

10 (Optional) In the Add Entry dialog box, type a popup description, select an item color, type a URL, and type a description.

11 Click Save.

12 Close the Calendar page.

13 In the Complete Planning Phase dialog box, provide the following information:

- Select a change plan type. In the Set Change Plan Type drop-down list, select a change plan type.
- Select a CAB. In the Select CAB drop-down list select a CAB.
- This information is not required for a Standard change plan type.
- Verify that the correct template is applied. A template is only required for a Standard change type plan.
- Select a change implementer. Click the Search symbol (magnifying glass). In the User Select dialog box search for and select a change implementer.
- (Optional) Add comments. In the Add Comments (Optional) field, type additional information that might be relevant to the change request or change plan.
14 Select one of the following options:

**Save**
Select this option if you are not ready to submit the change plan for approval.
This option saves the changes that you made. You can click Approve/Deny Change Plan to open the Complete Planning Phase dialog box and make additional changes later.

**Submit Change Plan**
Select this option if you are ready to submit the change plan for approval.

15 (Optional) On the Process View page, perform any of the other actions that are available as needed.

16 Close the change request’s Process View page.
Scheduling and planning changes

Scheduling the implementation of a change plan
Approving and implementing changes

This chapter includes the following topics:

- Initiating a vote on a change
- Voting on a change (CAB)
- Approving a change (change manager)
- Closing a change request ticket

Initiating a vote on a change

You can initiate a vote so that the Change Approval Board (CAB) can vote on the change plan. After you initiate the voting, the members of the CAB receive a task that lets them vote to approve or deny the change plan. After the CAB votes on the change plan, the change manager can then approve or deny the change.

The voting process is skipped when the Emergency or the Standard change type is used. Instead, the plan is assigned directly to the change manager for final approval.

To initiate a vote on a change

1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Task Viewer, under Project Name, expand SD.ChangeManagement.
3. In the list of task, find and open the change request ticket that has the status CAB Review and Approval.
4 On the change request's Process View page, under Task and Actions, expand CAB Options: 3 Action(s).
5 Click Initiate Voting.
6 In the CAB Voting dialog box, in the Set Title for Voting Task field, type a title for the voting task.
7 In the Set Description for Voting Task field, type a description for the voting task.
8 In the Set Priority for Voting Task drop-down list, select a priority for the voting task, and click Continue
9 Click Continue.

See “About the Change Management process” on page 221.
See “Approving a change (change manager)” on page 256.
See “Monitoring a vote on a change” on page 254.
See “Canceling the vote on a change” on page 255.

Monitoring a vote on a change

You can monitor the voting on a change plan. You can see who has voted. You can also see the votes to approve or deny the change plan.

To monitor a vote on a change
1 In the Process Manager portal, click My Task List.
2 On the My Task List page, under Task Viewer, under Project Name, expand SD.ChangeManagement.
3 In the list of task, find and open the change request ticket that has the status CAB Review and Approval.
4 On the change request's Process View page, under Task and Actions, expand CAB Options: 3 Action(s).
5 Click Monitor Voting.
6 In the CAB Voting dialog box, review the voting records.
7 Click Close.

See “Initiating a vote on a change” on page 253.
Canceling the vote on a change

You can cancel a vote on a change plan, while the change plan is in the voting process. After you cancel the voting process, votes are ignored. The change manager can still approve the change request plan.

To cancel a vote on a change
1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Task Viewer, under Project Name, expand SD.ChangeManagement.
3. In the list of task, find and open the change request ticket that has the status CAB Review and Approval.
4. On the change request's Process View page, under Task and Actions, expand CAB Options: 3 Action(s).
5. Click Cancel Voting.
6. In the CAB Voting dialog box, click Continue.

See “Initiating a vote on a change” on page 253.

Voting on a change (CAB)

The change advisory board’s (CAB’s) authorization of a change request is part of the Change Management process. After the CAB members review the plans for a change request, each member can approve or deny the plan through the voting process. Each CAB member can review the plans for a change request and then vote to approve or deny the plan through the voting process.

The voting process is skipped when the Emergency or the Standard change type is used. Instead, the plan is assigned directly to the change manager for final approval.

After the voting on the change is complete, the change manager provides the final approval or denial for implementing the change.

See “Approving a change (change manager)” on page 256.

To vote on a change
1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Task Viewer, under Project Name, expand SD.ChangeManagement.
3. In the list of task, find and open the change request ticket that has the status Vote on Change Plan.
4 On the change request ticket’s Process View page, under Tasks and Actions, click Complete Task.

5 In the CAB Voting dialog box, to the right of Your Vote, select one of the following options:
   ■ Approve
   ■ Reject

6 In the Comments field, type your reasons for accepting or rejecting the change.
   When you select Reject, you must provide comments.
   When you select Approve, no additional actions are required.

7 Click Cast Vote.

Approving a change (change manager)

The change manager can approve or deny a change plan after the CAB votes to approve or deny the change plan. The change manager can approve or deny a change plan before all the CAB members have voted. The change manager can approve or deny a change plan, after a vote is canceled.

Approving a change is part of the Change Management process.

To approve a change

1 In the Process Manager portal, click My Task List.

2 On the My Task List page, under Task Viewer, expand SD.ChangeManagement.

3 In the list of tasks, find and open the change request ticket that has the status CAB Review and Approval.

4 On the change request’s Process View page, under Tasks and Actions, click Approve Change Plan.

5 In the CAB Approval dialog box, review the voting record.

6 Confirm the start and the end dates, review the change schedule, and confirm the implementer.

7 (Optional) Search for and select a different implementer.

8 (Optional) Select a different start date.

9 (Optional) Select a different end date.

10 (Optional) Edit the change schedule.
11  In the CAB Approval dialog box, next to CAB Decisions select Reject or Approve.

12  Click Submit.

13  Close the change request’s Process View page.

See “About the Change Management process” on page 221.

See “Voting on a change (CAB)” on page 255.

See “Initiating a vote on a change” on page 253.

Closing a change request ticket

After you implement the change request, you must close the change request ticket. Closing the ticket lets you fulfill the request. Fulfilling the change request is part of the Change Management process.

See “About the Change Management process” on page 221.

To close a change request ticket

1  In the Process Manager portal, click My Task List.

2  On the My Task List page, under Task Viewer, under Project Name, expand SD.ChangeManagement.

3  In the list of task, find and open the change request ticket that has the status Implement Change Plan.

4  On the change request’s Process View page, under Task and Actions, click Complete Task.

5  In the Fulfill Change Ticket dialog box, take one of the following actions:

Check This change request was fulfilled according to the change plan provided. This action applies the Succeeded close code to the closed ticket.

Do not check This change request was fulfilled according to the change plan provided. This action applies the Failed close code to the closed ticket.

6  In the Provide Comments field, type your comments.

7  Click Close Ticket.
Approving and implementing changes
Closing a change request ticket
Managing problems

- Chapter 23. Managing problems
Managing problems

This chapter includes the following topics:

■ About Problem Management
■ About the Problem Management process
■ Problem statuses
■ Roles in Problem Management
■ Sources of problem tickets
■ Email notifications from Problem Management
■ Process View page for problem tickets
■ About discussions in the Problem Management process
■ Reporting a problem
■ Create Problem page
■ Submit a New Problem page
■ Adding incidents to a problem ticket
■ Working a problem ticket
■ Examination and Analysis page
■ Propose Workaround page, Propose a Fix page
■ Reviewing a proposed fix or workaround
■ Submit Change Request page
■ Reworking a problem ticket
About Problem Management

The Problem Management process looks at the root causes of the problems that cause multiple incidents. Problem Management then seeks to take actions to fix the situation and prevent it from recurring. The goal of the process is to minimize the effect of incidents and problems on the business.

To manage problems successfully, you need the ability to perform the following actions:

- Track problems.
- Diagnose the problems.
- Fix the problems through change requests.
- Publish known errors to help with future resolutions.

Part of the Problem Management process is to group related incidents for additional analysis and discovery of root causes. This analysis and discovery lets Problem Management take Incident Management a step further. Incident Management seeks to resolve the single issue at hand, so that a user can get up and running again. Problem Management goes deeper and seeks to take the actions that prevent that issue from happening again. When the problem is identified, a change request can be created or a knowledge base article can be requested.

In general, Problem Management deals with the issues that multiple users have encountered. For example, multiple users may experience an issue with a certain software program. Each of these issues can be resolved individually through the Incident Management process. However, the Problem Management process might suggest a Service Pack update for all users of that software. This solution would solve the individual incidents and prevent other users from encountering the issue and creating new incidents.

Problem Management includes the following key features:

- The ability to group incidents so that the root cause that is common to all the incidents can be analyzed.
  - The information in the problem request can be forwarded for use in a change request, or sent back to support technicians as a resolution.
- One notification can be sent for all the incidents that are associated with the problem.
- The knowledge base can be used as part of a resolution for a problem, and problems can provide information for the knowledge base.

See “About the Problem Management process” on page 263.
The Problem Management process provides information to the other ServiceDesk processes as follows:

- Obtains the initial context of a problem from the Incident Management process.
- Provides the context that is related to the problem to assist in the decision making during the Change Management process.
- Provides the documentation from problems to the knowledge base.

See “About cascading relationships among process tickets” on page 38.

See “What you can do with ServiceDesk” on page 24.

About the Problem Management process

The goal of Problem Management is to minimize the effect of problems and known errors that result from systemic issues within the IT infrastructure. The Problem Management process lets you track and diagnose problems, propose actions to resolve the problems, and take action on the problem resolutions.

The Problem Management process is initiated when someone creates a problem ticket.

To identify problems, ServiceDesk workers can take the following approaches:

- **Proactive**: A problem analyst or manager identifies problems and known issues before they occur.
- **Reactive**: Another ServiceDesk worker reports a problem in response to one or more incidents. For example, the support manager notices a significant increase in requests to unlock user accounts.

See “About cascading relationships among process tickets” on page 38.

Table 23-1 The Problem Management process

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Someone creates a problem ticket.</td>
<td>A problem ticket can be created in the following ways:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A problem analyst reviews incidents to find the errors that reoccur frequently and creates a problem ticket for those errors. See “Reporting a problem” on page 270.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A support worker creates a problem ticket from within an incident.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating a problem ticket from an incident” on page 174.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The creation of a problem ticket creates a task for the problem analyst.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Step 2 | The problem analyst works the problem ticket. | The problem analyst views the ticket and researches the problem. After the analysis is finished, the analyst updates the problem ticket with additional details, proposes a fix or workaround, and submits the problem for review.  
See “Working a problem ticket” on page 274.  
When the problem is submitted, a task is created for the problem reviewer. |
| Step 3 | (Optional) A problem worker can add incidents to the problem ticket. | If the problem is related to one or more incidents, they can be associated with the problem ticket. The incidents can help to uncover root causes.  
Incidents can be added to a problem ticket at any time before the problem reviewer approves the fix or workaround.  
See “Adding incidents to a problem ticket” on page 273. |
| Step 4 | The problem reviewer reviews the proposal. | The problem reviewer reviews the proposed fix or workaround and decides how to handle it.  
See “Reviewing a proposed fix or workaround” on page 277.  
When the proposal is accepted, the problem reviewer decides whether to create a change request, request the creation of a knowledge base article, or both. If a change request is not created, the problem is closed and the process skips to the final step.  
When the proposal is rejected, the problem reviewer provides a reason for the rejection. A task is created for the problem analyst, who can decide to remove the problem or rework the problem by repeating Step 2.  
See “Reworking a problem ticket” on page 279. |
| Step 5 | If the problem reviewer requests a change, the problem process waits for the change process. | The change manager reviews the change request and approves or rejects it.  
When the change request is accepted, the Problem Management process pauses until the change is completed.  
If the change is rejected, a task is created for the problem reviewer. The problem reviewer decides to either remove the problem or rework the problem by repeating Step 2. |
Table 23-1  The Problem Management process (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>The problem is closed.</td>
<td>The problem ticket can be closed in the following ways:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The problem reviewer accepts the problem proposal, chooses to request a knowledge base article, and closes the problem ticket.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- All changes that are associated with the problem are completed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The closure of the problem triggers a cascading closure, in which the changes and the incidents that are associated with the problem are closed. Any incidents that are associated with those changes are also closed.</td>
</tr>
</tbody>
</table>

Problem statuses

The problem status accurately reports the progression and outcome of the stages of the Problem Management process. The percentage represents the level of completion that the process has reached. For example, if the status percentage is 60, it means that the process is 60 percent complete.

The status and percentage appear in several places in the Process Manager portal. For example, they appear at the top of the ticket’s Process View page.

Table 23-2  Problem statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Completion percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze New Problem</td>
<td>The problem ticket is in a waiting state for the problem analyst to review the ticket and propose a resolution.</td>
<td>5%</td>
</tr>
<tr>
<td>Awaiting proposal review.</td>
<td>The problem analyst proposed a resolution and submitted the problem ticket, which is in a waiting state for the problem reviewer to review the ticket.</td>
<td>50%</td>
</tr>
<tr>
<td>Waiting on Change Management</td>
<td>A change was requested to resolve the problem, which is in a waiting state for the completion of the change process.</td>
<td>75%</td>
</tr>
<tr>
<td>Closed</td>
<td>The problem process is complete. The closure occurs when the problem analyst or reviewer closes the problem ticket or all the changes that are associated with the release are closed.</td>
<td>100%</td>
</tr>
<tr>
<td>Schedule Change has been submitted</td>
<td>A change request is submitted to resolve the problem.</td>
<td>85%</td>
</tr>
</tbody>
</table>
Table 23-2  Problem statuses (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Completion percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Document</td>
<td>A fix or workaround for the problem is submitted as a new knowledge base article request</td>
<td>80%</td>
</tr>
<tr>
<td>Solution was rejected</td>
<td>The problem reviewer rejected the problem and returned it to the problem analyst. The problem ticket is in a waiting state for the problem analyst to rework or remove the problem.</td>
<td>5%</td>
</tr>
<tr>
<td>Exception</td>
<td>The SLA time was surpassed.</td>
<td>85%</td>
</tr>
</tbody>
</table>

Roles in Problem Management

Depending on their structure, some organizations might have different hierarchy levels and multiple roles for Problem Management. ServiceDesk contains two default groups for Problem Management: Problem Analyst and Problem Reviewer.

Table 23-3  Roles in Problem Management

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem analyst</td>
<td>Analyzes the root cause of the problem, proposes a solution, and submits the proposal. The proposal can be in the form of a fix or a workaround. Analysts can also remove the problem. In many organizations, the same person fills both the problem analyst and the problem reviewer roles. However, in larger organizations the problem analyst role is assigned to one or more people other than the problem reviewer.</td>
</tr>
<tr>
<td>Problem reviewer</td>
<td>Approves the proposed fix or workaround and decides how to handle the problem, or returns the problem to the problem analyst for rework.</td>
</tr>
</tbody>
</table>

ITIL recommends that the same person should not be involved in both Problem Management and Incident Management. The priorities of those processes are not always consistent with each other.

Sources of problem tickets

The creation of a problem ticket triggers the Problem Management process. A problem ticket can originate from several sources.
**Table 23-4** Sources of problem tickets

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Manager portal</td>
<td>A problem analyst or other ServiceDesk worker creates a problem ticket from the Report a Problem link in the Service Catalog.</td>
</tr>
<tr>
<td>Incident Management</td>
<td>A support worker creates a problem from the Create or Relate to a Problem Ticket action in an incident’s Process View page.</td>
</tr>
</tbody>
</table>

**Email notifications from Problem Management**

ServiceDesk sends email notifications at various stages of the Problem Management process. In this context, a problem event is any action that is taken to create or work a problem ticket. The type of event and the ServiceDesk configurations determine the recipients of the email notifications.

The email notifications from incidents, discussions, and problems can process replies to the notifications and add them to the history of the related ticket.

Replies are processed in the following situations:

- The email notification is sent from a process. Such emails contain an identifier to trigger the response.
- The email notification is sent from a template and the ServiceDesk worker selected the option to include a reply code.

**Table 23-5** Default problem events that trigger email notifications

<table>
<thead>
<tr>
<th>Event</th>
<th>Email recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>A problem ticket is created.</td>
<td>The submitter and the primary contact, if they are not the same person</td>
</tr>
<tr>
<td>A problem worker decides to handle the problem by creating a knowledge base article.</td>
<td>The knowledge base editor&lt;br&gt;The email message requests an article that describes how to handle the problem.</td>
</tr>
</tbody>
</table>

**Process View page for problem tickets**

The Process View page is the primary interface for working a task. The Process View page appears when you select a task from your Task List or from another list in the Process Manager portal.
The default sections on the Process View page are similar for all types of tasks. If your organization uses customized Process View pages, your views might look different.

See “Process View page (Problem Management)” on page 98.

In addition to the common actions that you can perform for all tasks, the problem Process View page contains additional, problem-specific actions. The actions that are available depend on your permissions and the state of the problem ticket. For example, the Review Fix or Workaround action appears only after the problem ticket is reviewed and analyzed.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Incident</td>
<td>Lets you add one or more incidents that are related to the problem. See “Adding incidents to a problem ticket” on page 273.</td>
</tr>
<tr>
<td>Add/Manage Bulletin Boards</td>
<td>Lets you manage bulletin boards, if you have permission to do so. It also lets you create a bulletin board entry.</td>
</tr>
<tr>
<td>Assignments</td>
<td>Lets you assign the ticket to another user, group, or organization. This action appears under Actions on the task pop-up that appears when you click the task in the History section.</td>
</tr>
<tr>
<td>Change Priority</td>
<td>Lets you change the problem ticket’s priority. For example, after a problem is created, many incidents that are related to the problem are submitted. In this situation, you might change the problem’s priority to a higher level.</td>
</tr>
<tr>
<td>Edit Description</td>
<td>Lets you describe the problem accurately. For example, when you create a problem from an incident, the problem inherits the incident’s description. However, the incident’s description is likely to be user-specific while the problem typically represents a more general issue.</td>
</tr>
<tr>
<td>Go To Discussion</td>
<td>Lets you view and add to the posts in a discussion about the problem. A discussion is formed when a problem is created. See “About discussions in the Problem Management process” on page 269.</td>
</tr>
<tr>
<td>Invite Participant</td>
<td>Lets you invite another user to become a contact on the problem. You can also choose whether to send an email to notify the user of the addition.</td>
</tr>
<tr>
<td>Manage Equipment</td>
<td>Opens the Add Equipment dialog box, which lets you add or delete the equipment that is related to the process. You can also access the quick tools for a piece of equipment.</td>
</tr>
</tbody>
</table>
Table 23-6  
Actions on the problem ticket’s Process View page (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Remove Problem      | Displays the **Remove Problem** page, where you must provide a detailed reason for the deletion. Examples of why you might remove a problem are as follows:  
- You determine that the issue is not a problem and does not require further processing.  
- You determine that this issue is related to or is a duplicate of another problem. In this situation, you can choose to move any attached incidents to another problem ticket. |
| Review Fix Or Workaround | Lets you review the proposed fix or workaround, determine how to handle the problem, and approve the problem or return it to the analyst. See “Reviewing a proposed fix or workaround” on page 277. |
| Search KB          | Lets you search the knowledge base for an article that is related to the ticket and then attach the article. See “Searching the knowledge base” on page 339. |
| Send Email         | Lets you send an email message regarding the ticket. See “Sending an email from a ticket’s Process View page” on page 375. |
| View Problem       | Lets you view the details of the problem ticket and select the options that appear under Other Actions. For example, you can send emails or participate in a discussion. |
| Work Problem       | Lets you perform the following actions:  
- Resume work on a ticket that you started and then saved without completing. The ticket is saved as a draft and a task is created to complete the ticket.  
- Update a problem ticket to provide the cause and a detailed description of the problem. You can also categorize the problem and propose a workaround or a fix.  
See “Working a problem ticket” on page 274. |

**About discussions in the Problem Management process**

You can use discussions to help you research or resolve a problem. Discussions are started automatically from within the Problem Management process.

When a problem ticket is created, the problem’s name and ID become the title of the new discussion. The problem’s description becomes the discussion’s description. Anyone who works the problem can use the **Go to Discussion** smart task to create posts and view any posts that have been made for the problem.

See “About discussions in the Process Manager portal” on page 381.
See “Reporting a problem” on page 270.

Reporting a problem

Report a problem to create a problem ticket to initiate the process of taking measures to prevent an issue that can lead to incidents. Reporting a problem to create a problem ticket is the first step in the Problem Management process.

See “About the Problem Management process” on page 263.

A problem ticket can also be created from an incident, which creates an association between the incident and the problem.

See “Creating a problem ticket from an incident” on page 174.

When the problem ticket is created, a new discussion is created and associated with the problem.

See “About discussions in the Problem Management process” on page 269.

After the problem ticket is created, the problem analyst works the ticket by entering the results of the analysis and proposing a fix or workaround.

See “Working a problem ticket” on page 274.

To report a problem

1. In the Process Manager portal, click Submit Request.
2. Under Service Catalog, click IT Services.
3. On the right side of the page, click Report a Problem.
4. (Optional) On the Create Problem page, to attach one or more incidents to the problem ticket, take the following steps:
   - In the Search for field, type the search text to evaluate against incident descriptions, and then click the Search symbol (magnifying glass). Incidents that are already attached to a problem do not appear in the search results.
   - Under Incidents with Possible Relation to Current Problem, click the Add link to the right of each incident to attach, or click Add All Listed to add all the incidents that you found.

See “Create Problem page” on page 271.

5. (Optional) On the Create Problem page, if you choose not to attach any incidents, click Verify you are not attaching incidents.
6. On the Create Problem page, click Create a New Problem.
On the **Submit a New Problem** page, define the problem, and then click **Continue**.

See “**Submit a New Problem page**” on page 272.

On the **Review New Problem** page, verify that the information is correct, remove incidents if necessary, and then select one of the following options:

**Close Without Saving**  Cancels your entry without creating a problem ticket.

**Back to Incident Search**  Returns to the **Create Problem** page, where you can add or remove incidents.

Repeat from step 4.

**Create Problem**  Creates the problem ticket.

On the **Submission Complete** page, click **Close**.

---

**Create Problem page**

This page lets you define the incidents to attach to a new problem ticket. You can also choose not to attach incidents.

See “**Reporting a problem**” on page 270.

See “**Adding incidents to a problem ticket**” on page 273.

**Table 23-7** Options on the **Create Problem** page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for</td>
<td>Lets you find one or more related incidents to attach to the problem ticket. The search text that you enter is evaluated against the text in the incident’s description or title.</td>
</tr>
<tr>
<td></td>
<td>For example, if several users could not access a network printer, you might search for all incidents that are related to the network printer.</td>
</tr>
<tr>
<td>Incidents with Possible Relation to Current Problem</td>
<td>Displays the search results and lets you review each incident or add it to the problem ticket. Incidents that are already attached to a problem do not appear in the search results.</td>
</tr>
<tr>
<td>Currently Added Incidents</td>
<td>Lists the incidents that you add to the problem ticket.</td>
</tr>
</tbody>
</table>
Table 23-7  Options on the Create Problem page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add All Listed</td>
<td>Adds all the incidents that are listed under Incidents with Possible Relation to Current Problem to the problem ticket.</td>
</tr>
<tr>
<td>Remove all listed</td>
<td>Removes all the incidents that are listed under Currently Added Incidents from the list.</td>
</tr>
<tr>
<td>Add to Existing Problem</td>
<td>Lets you select an existing problem to attach the incidents to.</td>
</tr>
<tr>
<td>Create New Problem</td>
<td>Creates a problem ticket.</td>
</tr>
<tr>
<td>Verify you are not attaching incidents.</td>
<td>Lets you choose not to attach incidents to the problem ticket. However, because it is more typical to attach tickets, you must verify your choice not to do so.</td>
</tr>
</tbody>
</table>

Submit a New Problem page

This page lets you define the details of a problem. It appears during the creation of a new problem ticket.

See “Reporting a problem” on page 270.

Table 23-8  Options on the Submit a New Problem page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Contact</td>
<td>Lets you specify the primary contact for the problem ticket. Typically, the primary contact is the person who encounters or reports the problem.</td>
</tr>
<tr>
<td>Search for User</td>
<td>Opens the Select User page, where you can specify the person who this problem affects. This link appears only when you specify that this problem affects someone else.</td>
</tr>
<tr>
<td>Title</td>
<td>Becomes the title that identifies the problem in the Process Manager portal. Make the name descriptive enough for you and others to easily understand the nature of the problem.</td>
</tr>
<tr>
<td>Detailed Description of the Problem</td>
<td>Lets you type additional information to describe the problem. For example, you might describe the steps to reproduce the problem or provide information about what happens as a result of the problem.</td>
</tr>
</tbody>
</table>
Table 23-8  Options on the Submit a New Problem page (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause of the Problem</td>
<td>Lets you describe what causes the problem.</td>
</tr>
<tr>
<td>Business Impact</td>
<td>Lets you define the extent of the problem by specifying how many people are affected. See “Default priority, urgency, and impact values” on page 433.</td>
</tr>
<tr>
<td>Urgency</td>
<td>Lets you specify how much the problem affects the submitter or the primary contact. See “Default priority, urgency, and impact values” on page 433.</td>
</tr>
</tbody>
</table>

Adding incidents to a problem ticket

Adding incidents to a problem ticket is an optional step in the Problem Management process. You can add incidents to a problem ticket at any time before the proposed fix or workaround is approved. See “About the Problem Management process” on page 263.

To add incidents to an existing problem ticket

1. In the Process Manager portal, click My Task List.
2. Under Task Viewer, under Project Name, expand SD.Problem Management.
3. In the list of tasks, find and open the task to work on.
4. On the ticket’s Process View page, expand Assignments, expand Smart Tasks, and then click Add Incident.
5. In the Associate Incidents page, in the Search for field, type the search text, and then click the Search symbol (magnifying glass).
6. Under Incidents with Possible Relation to Current Problem, in the list of search results, click the Add to Problem link to the right of each incident to attach.
7. When you finish adding incidents, click Close.
8. When the ticket’s Process View page reappears, you can continue to work the ticket or close it.
Working a problem ticket

After you analyze a problem, you update the problem ticket to provide the cause and a detailed description of the problem. You also categorize the problem and propose a fix or a workaround.

You can also use the actions that are available in the ticket to help with your research. For example, you can communicate with other users by opening a chat session or posting to the discussion that is associated with the problem.

Working a problem ticket is a step in the Problem Management process.

See “About the Problem Management process” on page 263.

After you propose a resolution for the problem, the problem reviewer views the proposal and then takes action.

See “Reviewing a proposed fix or workaround” on page 277.

To work a problem ticket

1. In the Process Manager portal, click My Task List.
2. Under Task Viewer, under Project Name, expand SD.Problem Management.
3. In the list of tasks, find and open the task.
4. On the ticket’s Process View page, under Assignment, click Work Problem.
5. On the Examination and Analysis page, record the results of your analysis.
   See “Examination and Analysis page” on page 275.
6. When you finish describing the analysis, select one of the following options:
   - Save and Close
     Saves the information and closes the page. Use this option when you plan to continue to work the problem later.
   - Propose a Workaround
   - Propose a Fix
     See “Propose Workaround page, Propose a Fix page” on page 276.
7. On the Propose Workaround page or the Propose Fix page, enter information about the proposal, and then click Submit Proposal.
8. When the ticket’s Process View page reappears, you can continue to work the ticket.
Examination and Analysis page

This page lets you record the results of your problem analysis. It appears when you select Work Problem on a problem ticket’s Process View page.

See “Working a problem ticket” on page 274.

Table 23-9  Options on the Examination and Analysis page

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>Lets you select a classification for the problem. Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification. You can select from several default classifications as well as any custom classifications that your organization added. See “Default categories for incidents and default classifications for problems” on page 559.</td>
</tr>
<tr>
<td>Classification Click here to classify</td>
<td></td>
</tr>
<tr>
<td>Root Cause</td>
<td>Lets you describe what you think is the cause of the problem. This option defaults to the text from the problem entry and lets you type additional text.</td>
</tr>
</tbody>
</table>
| Category                      | Lets you select the category that the problem belongs to. The default categories are as follows:   
|                               | ■ Add/Install  
|                               | ■ Break/Fix  
|                               | ■ Request |
| Business Services Affected    | Lets you select one or more business services that the problem affects. If the problem originated from an incident, any business service that is associated with the incident appears as a related item on the Process View page. |
| Problem Description           | Contains the text from the problem entry and lets you type additional text.                                                                     |
| Supporting Documents          | Lets you attach documents or other files that provide additional information about the problem. For example, you can attach error logs. |
| Attach File                   |                                                                                                                                                  |
| Remove File                   |                                                                                                                                                  |
| Add Location                  | Lets you specify the location that the problem affects. The location is for informational purposes only. When you click this link, the Location Affected page appears. It displays your default location but you can change it when you report the problem from a different location. |
| Save and Close                | Saves the information and closes the page. Use this option when you plan to continue to work the problem later.                                       |
Table 23-9 Options on the Examination and Analysis page (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propose a Workaround</td>
<td>Lets you document a workaround or a fix to a problem.</td>
</tr>
<tr>
<td>Propose a Fix</td>
<td>See “Propose Workaround page, Propose a Fix page” on page 276.</td>
</tr>
</tbody>
</table>

Propose Workaround page, Propose a Fix page

These pages let you document a workaround or a fix to a problem. They appear when you work a problem ticket.

See “Working a problem ticket” on page 274.

Table 23-10 Options on the Propose a Workaround and Propose a Fix pages

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>Lets you change the problem’s classification. Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification. Your classification can be a default classification or a custom classification that was added by your organization. See “Default categories for incidents and default classifications for problems” on page 559.</td>
</tr>
<tr>
<td>Category</td>
<td>Read-only.</td>
</tr>
<tr>
<td>Workaround Instructions</td>
<td>Lets you type instructions for performing the workaround or fix.</td>
</tr>
<tr>
<td>Detailed Fix Instructions</td>
<td></td>
</tr>
<tr>
<td>Details</td>
<td>(Read only) Contains the text from the problem entry.</td>
</tr>
<tr>
<td>Business Impact</td>
<td>Lets you define the extent of the problem by specifying how many people are affected.</td>
</tr>
<tr>
<td>Urgency</td>
<td>Lets you specify how much the problem affects the submitter or the primary contact.</td>
</tr>
<tr>
<td>Priority</td>
<td>Lets you select the priority for resolving this problem.</td>
</tr>
</tbody>
</table>
Reviewing a proposed fix or workaround

After a problem analyst proposes a solution to a problem, you can review the proposal and accept or reject it. When you accept a proposal, you can decide whether to create a change request, request the creation of a knowledge base article, or both. When you reject a proposal, you return the problem to the problem analyst, who can remove the problem or provide additional information and resubmit it.

Reviewing a fix or workaround is a step in the Problem Management process. If you submit a change request after your review, a problem task with the status Waiting for Change Request to Complete appears in the task list. This task cannot be worked; it is a reminder that the problem is on hold pending the completion of the change request.

See “About the Problem Management process” on page 263.

To review a fix or workaround

1 In the Process Manager portal, click My Task List.
2 Under Task Viewer, under Project Name, expand SD.Problem Management.
3 In the list of tasks, find and open the task.
4 On the ticket’s Process View page, under Assignment, click Review Fix Or Workaround.
5 On the Review Proposal page, review the information about the proposed workaround or fix.
6 In How this Problem will be Handled, select one of the following options:
   ■ Create KB Article
     Creates a new request for a knowledge base article and sends a notification email to the knowledge base editor.
   ■ Create Change Ticket
     Lets you create a change request from this problem ticket.
   ■ Create Change and Article
Create Known Issue

Select one of the following options:

- **Close**
  
  Saves the information and closes the page.

- **Return Problem to Analyst**
  
  Go to step 8.

- **Approve proposal**
  
  Go to step 9.

If you chose to return the problem to the analyst, on the Return to Analyst page, provide the reason for returning the problem, and then click Submit. See “Reworking a problem ticket” on page 279.

If you chose to create a change request, on the Submit Change Request page, provide the information for the change ticket, and then click Submit Change Request. See “Submit Change Request page” on page 278.

When the ticket’s Process View page reappears, you can close it.

Submit Change Request page

This page lets you provide the information for a change ticket that you create from a problem ticket. It appears when you choose to create a change ticket during the problem review task.

See “Reviewing a proposed fix or workaround” on page 277.

Table 23-11 Options on the Submit Change Request page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Description</td>
<td>Lets you describe in detail the change that needs to be made.</td>
</tr>
<tr>
<td>Change Needed By</td>
<td>Lets you specify when the change must be made.</td>
</tr>
<tr>
<td>Priority</td>
<td>Lets you specify the priority for the change request.</td>
</tr>
<tr>
<td>Submit Change Request</td>
<td>Creates a change request ticket and assigns it to the change queue.</td>
</tr>
</tbody>
</table>
Reworking a problem ticket

During the review of a problem ticket, the problem reviewer can choose to return the problem to the analyst. The reviewer provides guidance to the analyst by including a reason for the rejection. For example, the reviewer might request a more detailed workaround description, or decide that a change is required instead of a workaround.

See “Reviewing a proposed fix or workaround” on page 277.

The problem analyst can rework the problem ticket to provide the information that the reviewer requested. The analyst can also remove the problem ticket at the reviewer’s recommendation or as a result of additional research.

If the analyst removes the problem, the process ends and triggers a cascading closure of any changes and incidents that are associated with the problem.

To rework a problem ticket

1. In the Process Manager portal, click My Task List.
2. Under Task Viewer, under Project Name, expand SD.Problem Management.
3. In the list of tasks, find and open the task.
4. On the ticket’s Process View page, under Assignments, click Work Problem.
5. On the Rejection Reason page, review the problem reviewer’s comments, and then select one of the following options:

   - **Close**: Saves the problem and closes the page. Select this option if you plan to take either of the following actions:
     - Resume work on the problem later.
     - Remove the problem ticket. This option itself does not remove the problem ticket. However, it lets you return to the problem’s Process View page, from which you can access the Remove Problem smart task.

   - **Rework Proposal**: Opens the Examination and Analysis page, where you can continue to work the problem as usual.

See “Working a problem ticket” on page 274.
Managing problems

Reworking a problem ticket
Working with process tickets

- Chapter 24. Performing common ticket actions
- Chapter 25. Assigning and delegating process tickets
- Chapter 26. Managing the ServiceDesk schedule
Performing common ticket actions

This chapter includes the following topics:

- About restricting access to open tasks (leasing)
- Breaking the lease on a task
- About the process time for tickets
- Posting process time to a ticket
- Performing actions on multiple tickets
- Attaching a file to an existing process ticket

About restricting access to open tasks (leasing)

To prevent multiple workers from changing a task at the same time, ServiceDesk can restrict access to the task while someone works on it. This process is referred to as leasing.

The administrator can enable and configure settings for leasing in the Portal Master Settings.

If leasing is enabled, when a worker opens a task and takes a specific action, the task is immediately leased to that worker. For example, an incident task is leased as soon as the worker begins to escalate it. No other worker can work on that task until the lease is released or broken. The option to work on the incidents that are assigned to others does not override a lease.

A lease is released or broken in the following situations:

- The leasing worker closes the task.
The maximum allowable lease time passes. The administrator configures the setting that determines the amount of time that a task can be leased from the time that the lease begins. After a task has been leased for that amount of time, the lease is released automatically, even if the worker has not completed the task.

The administrator breaks the lease. The administrator can open a leased task and break its lease. For example, a worker begins work on an emergency task and then leaves their desk before the task is completed. Another worker sees the task on the Process View page and notices that it is leased. The second worker notifies the administrator to break the lease. After the lease is broken, the second worker or the administrator can finish the task.

See “Breaking the lease on a task” on page 284.

Other workers can see leased tasks on the Process View page. They can also see leased tasks in their task lists if the administrator enabled the setting to allow leased items to appear there. When a leased task is opened, a message on the task page identifies it as leased. Other workers can view the task’s details but cannot make any changes.

**Breaking the lease on a task**

If leasing is enabled, when a worker opens a task and takes a specific action, the task is immediately leased to that worker. No other worker can work on that task until the lease is released or broken.

See “About restricting access to open tasks (leasing)” on page 283.

The administrator can open a leased task and break its lease.

**To break the lease on a task**

1. In the Process Manager portal, open the task.
2. Under History, at the right of the current task line, click the Green Down Arrow symbol.
3. In the dialog box, under Actions, click Break Lease, and then close the dialog box.
4. (Optional) Work the task yourself or let someone else work it.
5. Close the task window.
About the process time for tickets

Process time represents the amount of time that it takes to work on and resolve a process ticket. The process time is used for reporting purposes. For example, you might need to report the time that was spent on a specific customer’s incidents. You might also track how much time certain kinds of incidents take to resolve, to help you analyze whether to create a problem ticket.

ServiceDesk can track either the entire time that a process ticket is open or only the time that someone actively works on it. A setting in the ServiceDesk installation determines how the time is tracked.

ServiceDesk process workers can also record the time that they spend on a ticket offline, which ServiceDesk cannot record automatically. Process time is not recorded during the ticket creation.

See “Posting process time to a ticket” on page 285.

ServiceDesk tracks the following times:

- **Current User Process Time**
  The amount of time that accumulates for the worker who has the Process View page open.

- **User Process Time**
  The total amount of offline time that workers have posted to the ticket to date.

- **Total Process Time**
  The amount of time that was spent on the ticket to date, including the time that was recorded automatically and the time that workers posted.

A ticket’s process time appears on the Process View page, under the top section that contains the ticket’s statistics and under the Process Time section.

Posting process time to a ticket

ServiceDesk tracks the amount of time that a process ticket is open or worked on and adds it to the ticket’s total process time. However, ServiceDesk cannot automatically record the time that process workers spend on a ticket offline. For example, a support technician might spend time researching an issue or trying to reproduce the issue. You can add the time that you spend offline to a ticket’s total process time.

See “About the process time for tickets” on page 285.

You can post time on the process ticket’s Process View page. For incidents, you can also post time on a page that appears during the incident resolution.

See “Resolving an incident from a task” on page 170.
To post process time to a process ticket

1  In the Process Manager portal, find and open the task on which you spent time.

2  On the process ticket’s Process View page, expand the Process Time or the Start/Stop Process Timing section, and then click Post Process Time.

3  In the Post User Time dialog box, enter the amount of time that you spent on the process ticket offline.

4  (Optional) In the Description field, add a description.

5  Click Save.

6  When you are returned to the process ticket’s Process View page, you can continue to work the ticket or close it.

Performing actions on multiple tickets

In the Process Manager portal, you can perform certain actions on a group of process tickets at one time. For example, you can add a comment to multiple process tickets or reassign a group of tickets.

The option to perform group actions can appear on any portal page that contains a list of process tickets. By default, the option appears on the Home page, My Task List page, and Tickets page.

You can also choose to close a group of incidents. This option is available on the Service Catalog.

See “Closing multiple incidents” on page 176.

To perform an action on multiple tickets

1  In the Process Manager portal, go to any page that contains a list of tickets.

   For example, a task list appears on the following portal pages: Home, My Task List, and Tickets.

2  On the portal page, click in the Select a group action drop-down list, and then select the action to take.

3  After the screen refreshes, click the check box to the left of each ticket to act on.
4 To the right of the Select a group action drop-down list, click Do action.

5 The action that you select determines what happens next. If a dialog box appears, complete the dialog box.
   For example, if the Add Comment dialog box opens, add a comment title and comment and then click Add Comment.

Attaching a file to an existing process ticket

You can attach one or more files to a process ticket to provide additional information to support the ticket. For example, you can attach an error log file or a screen image that you captured.

Files larger than 4 MB are not supported.

The files that you attach to a process ticket are added to the Document Management system. In the Process Manager portal, on the Documents page, the files appear in a folder whose name is the process ID.

See “Documents page” on page 59.

To attach a file to an existing process ticket

1 In the Process Manager portal, find and open the ticket to which you want to attach a file.

2 On the process ticket’s Process View page, expand the Documents, the Change Request Attachments, or the Incident Request Attachments section, and then click Add Attachments.

3 In the Add Documents dialog box, on the Documents Information tab, in File, type or browse to the file to attach.
4 (Optional) Click the **Optional** tab and enter additional information about the file as follows:

**Document Type** Lets you identify the document format or type. The ServiceDesk administrator creates the types that appear in the list. However, you can attach any type of file even if it is not listed.

**Override Name** Identifies this file in any list of documents in the Process Manager portal. Make the name descriptive enough for you and others to easily understand the purpose of the file.

If you do not provide a name, the file name is used.

**Description** Provide additional information to describe the file and its contents.

5 When you finish entering the document information, click **Save**.
Assigning and delegating process tickets

This chapter includes the following topics:

■ Reassigning incidents, problems, or change tickets
■ Edit Assignments dialog box
■ Delegating a user’s tickets to another user
■ Deleting a ticket delegation
■ Delegating your tickets to another user
■ Add Delegation dialog box
■ Reassigning incident tickets to a service queue

Reassigning incidents, problems, or change tickets

ServiceDesk incidents, problems, and change tickets can be assigned to another entity such as a user, group, permission, or organizational unit. For example, if an employee is out of the office unexpectedly, you can reassign that employee’s tickets to someone else.

You can assign a ticket to multiple users, groups, permissions, and organizational units.

If you need to reassign the incoming tickets for an employee, you can use the delegation function.

You can reassign an employee's incident ticket to a service queue.

See “Delegating your tickets to another user” on page 295.
To reassign an incident, problem, or change ticket

1. In the Process Manager portal, open the ticket to reassign.

2. On the ticket’s Process View page, in the History section, click the task’s name.
   
   You can also click the Green Down Arrow symbol to the far right of the task’s name.

3. On the ticket’s Workflow Task Details page, under Actions, click Assignments.

4. In the Edit Assignments dialog box, in the Assign Type drop-down list, select one of the following options:
   - Group
   - Organization
   - Permission
   - User

5. In the User, Group, Permission, or Organization field type the name of the entity to which you want to assign the ticket.

   Note that the name of this field is the same as your selection in the Assign Type drop-down list. For example, if you select Group in the Assign Type drop-down list, the name of this field is Group.

6. (Optional) Click Pick and in the User Picker, Group Picker, Permission Picker, or Organization Picker dialog box, select a specific entity as follows:
Assigning and delegating process tickets

Reassigning incidents, problems, or change tickets

User Picker dialog box  Type your search parameters into one or more of following fields as needed to find the user and then click Search:

- Email
- First Name
- Last Name
- City
- State
- ZIP Code
- Country
- Group
- Organization
- Max Results

For example, if you only know the user's first name, type the name in the First Name field and click Search.

Click the Select link to the right of the appropriate user.

See “Picking a user” on page 114.

Group Picker dialog box  In the Group Name field, type the group name and then click Search:

- Group Name
- Max Results

Click the Select link to the right of the appropriate group.

Permission Picker dialog box  Under Permission Name, click the Select link to the right of the appropriate permission.

Organization Picker dialog box  If necessary, expand the organizations, and then click the appropriate organization.

7  (Optional) In the Assign From and Assign To fields, specify a start date and end date for the assignment.

When the end date passes, if the incident is still not resolved, it is escalated automatically.

8  (Optional) To remove any assignees, click the Delete symbol (red X) next to the assignment record, and then click OK in the confirmation dialog box.

9  When you are finished, click Add.

Note that if you click Close, your new assignee is not saved.

10  (Optional) Repeat step 3 through step 9 to add additional assignments if necessary.
Edit Assignments dialog box

This dialog box lets you reassign a process ticket to another entity such as a user, group, permission, or organizational unit.

You can assign a ticket to multiple users, groups, permissions, and organizational units.

See “Reassigning incidents, problems, or change tickets” on page 289.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete symbol</td>
<td>Lets you delete any of the current assignees that appear at the top of the dialog box.</td>
</tr>
<tr>
<td>Assign To (Drop-down list)</td>
<td>Lets you select the entity to assign the task to. You can assign a task to a user, group, permission, or organizational unit.</td>
</tr>
<tr>
<td>User</td>
<td>Lets you type or select the name of a specific assignee.</td>
</tr>
<tr>
<td>Group</td>
<td></td>
</tr>
<tr>
<td>Permission</td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td></td>
</tr>
</tbody>
</table>
Delegating a user’s tickets to another user

The delegation function lets you route all the incoming tickets for one user to another user for a specified period. For example, you might delegate incoming tickets when a user is on leave or vacation, or is otherwise unable to work their tickets.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pick</td>
<td>Opens a Picker dialog box, which lets you search for a specific assignee.</td>
</tr>
<tr>
<td>Assign From</td>
<td>(Optional) specify a start date and end date for the assignment. When the end date passes, if the incident is still not resolved, it is escalated automatically.</td>
</tr>
<tr>
<td>Assign To</td>
<td>Adds the selected assignee without closing the dialog box.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds the selected assignee without closing the dialog box.</td>
</tr>
</tbody>
</table>

Table 25-1 Options in the **Edit Assignments** dialog box *(continued)*
The administrator or another user with the appropriate permissions typically performs this task.

If you need to reassign existing tickets to someone else, you can use the reassignment function.

See “Reassigning incidents, problems, or change tickets” on page 289.

See “Deleting a ticket delegation” on page 294.

**To delegate a user’s tickets to another user**

1. In the Process Manager portal, select **Admin > Users > Manage Delegations**.
2. In the **Delegations** section, click the **Add Delegation** symbol (green plus sign).
3. In the **Add Delegation** dialog box, specify the following information:
   - The user whose tickets you plan to delegate.
   - The user to whom you plan to delegate the tickets.
   - The starting date and ending date of the delegation period.
   See “**Add Delegation dialog box**” on page 295.
4. Click **Save**.

**Deleting a ticket delegation**

Delegations route all the incoming tickets for one user to another user for a specified period.

See “**Delegating a user’s tickets to another user**” on page 293.

A delegation expires on its specified end date, and the tickets resume being routed to the original user’s queue. If you need to end a delegation early, you can delete the delegation.

The administrator or another user with the appropriate permissions typically performs this task.

**To delete a ticket delegation**

1. In the Process Manager portal, click **Admin > Users > Manage Delegations**.
2. In the **Delegations** section, click the **Delete** symbol (red X) that appears next to the delegation to delete.
3. In the confirmation message, click **OK**.
Delegating your tickets to another user

Delegations route all the incoming tickets for one user to another user for a specified period. You can use delegation to ensure that someone else handles the incoming tickets that are assigned to you while you cannot work on them. When the end date for the delegation passes, the tickets resume being routed to your queue.

For example, you might set up a delegation during your vacation time and set the end date for when you plan to return to work.

If you need to reassign existing tickets to someone else, you can use the reassignment function.

See “Reassigning incidents, problems, or change tickets” on page 289.

To delegate your tickets to another user

1. In the upper right of the Process Manager portal, click Account.
2. Scroll to the Manage Delegations section, and then click the Add Delegations symbol (green plus sign).
3. In the Add Delegation dialog box, specify the following information:
   - The user whose tickets you plan to delegate.
   - The user to whom you plan to delegate the tickets.
   - The starting date and ending date of the delegation period.

   See “Add Delegation dialog box” on page 295.
4. Click Save.

Add Delegation dialog box

This dialog box lets you route all the incoming tickets for one user to another user for a specified period.

See “Delegating a user’s tickets to another user” on page 293.

See “Delegating your tickets to another user” on page 295.
Reassigning incident tickets to a service queue

ServiceDesk incidents can be reassigned to a service queue.

For example, an employee is out of the office unexpectedly. You can reassign that employee’s tickets to a service queue. Any of the users that are assigned to the queue can work the incident during that employee’s absence.

See “Reassigning incidents, problems, or change tickets” on page 289.

To reassign an incident ticket to a service queue

1. In the Process Manager portal, open the ticket that you want to reassign.
2. On the ticket’s Process View page, in the History section, at the right of the current task line, click the Green Down Arrow symbol.
3. On the ticket's Workflow Task Details page, in the Page Actions section, click Reassign Ticket.
4. In the Reassign Incident dialog box, in the Assign to Queue field, type the name of the service queue to which you want to reassign the incident.
5 (Optional) To search for and select a service queue, perform the following actions:

Open the Service Queue Selection dialog box.

To the right of the Assign to Queue field, click the Search symbol (magnifying glass).

Type your search parameters and search for the queue.

In the Service Queue Selection dialog box, in the Search Text field, type the name or part of the name of the queue. Then click the Search symbol (magnifying glass).

Select the service queue.

Select the queue to which you want to reassign the incident and click Select Queue.

6 In the Remove Existing Assignments checkbox, perform one of the following actions:

Check Remove Existing Assignments.

This action removes the ticket's existing assignments.

Uncheck Remove Existing Assignments.

This action retains the ticket's existing assignments.

7 Click Reassign.
Assigning and delegating process tickets

Reassigning incident tickets to a service queue
Managing the ServiceDesk schedule

This chapter includes the following topics:

- About scheduling in ServiceDesk
- Viewing the ServiceDesk schedule
- Searching for a schedule entry
- Creating a new schedule
- Add Schedule dialog box
- Adding an entry to the schedule
- Add Entry dialog box

About scheduling in ServiceDesk

In ServiceDesk, schedules record various date-related events and functions in a calendar on the Calendar page. The Calendar is an integrated view of all the approved changes and their release dates. This schedule lets the change manager plan changes and releases that coordinate with the existing schedule. When you consider the scheduled events together instead of in isolation, you can avoid unforeseen conflicts.

The schedule also provides the information that you can use to communicate planned downtime to management and the users who the implementation affects.
Table 26-1  Elements of the Calendar

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedules</td>
<td>A group of entries that are of a specific type. Each schedule contains entries for the events of the appropriate type. For example, the <strong>Changes Waiting for Release</strong> schedule contains entries for the changes that are approved and that need to be included in a release. All the entries in the individual schedules are combined on a single calendar. ServiceDesk contains the Scheduled Changes default schedule. See “Scheduling the implementation of a change plan” on page 249. You can use the default schedules and you can add customized schedules. See “Creating a new schedule” on page 302.</td>
</tr>
<tr>
<td>Schedule entries</td>
<td>The scheduled time for a specific event. A schedule entry is associated with a schedule. The Change Management process updates the schedules directly. The process places the entry in the appropriate schedule based on the status of the process ticket. Schedule entries can also be entered manually. For example, you might add a company meeting, a training session, or other non-process event that can affect the process-related schedules. See “Adding an entry to the schedule” on page 303.</td>
</tr>
<tr>
<td>Calendar</td>
<td>A page that displays the schedule entries. You can display the entries for all the schedules or for only the schedules that you select. The format options for viewing the schedule are as follows: Printed Today, Three Days, Work Week, Week, Month, Gantt View Displays the schedule in a Gantt style so that you can see other task dependencies in one view. You can select a start date and an end date, and then click Go to display the interactions.</td>
</tr>
</tbody>
</table>

Viewing the ServiceDesk schedule

You can view the **Calendar** page to review an integrated view of all the approved changes and their release dates.

See “Calendar page” on page 57.

The schedule is also visible when you view or schedule a process ticket.
To view the ServiceDesk schedule

1. In the Process Manager portal, click Calendar.

2. On the Schedules page, under Schedules, check the check box for each schedule to display and uncheck the check box for each schedule to hide.

   You can check or uncheck the check boxes at any time and the schedule display changes immediately.

3. To change the display color for a specific schedule, select a color from the drop-down list to the right of the schedule name.

4. To change the format of the schedule display, click one of the following options:
   - Today
   - Three Days
   - Work Week
   - Week
   - Month
   - Gantt View
     Displays the schedule in a Gantt style so that you can see other task dependencies in one view. You can select a start date and an end date, and then click Go to display the interactions.

5. To move the display forward or backward in time, click the arrows that appear at the far right and far left on the schedule heading.

Searching for a schedule entry

When you need to find a specific schedule event, you can search the Calendar. The search checks both the title and description for the search text. The search results and their start dates and end dates appear in the right pane of the Calendar page.

See “Calendar page” on page 57.

To search for a schedule entry

1. In the Process Manager portal, click Calendar.

2. On the Schedules page, expand the Search Schedule Entry section. Enter .

3. In the search field, type one or more words from the entry’s title or description, and then click the Search symbol (magnifying glass).
Creating a new schedule

In ServiceDesk, a schedule represents a certain type of schedule entry. For example, the Scheduled Changes schedule contains entries for the changes that have been approved and assigned a release date.

You can create additional schedules to extend the organization of schedule entries. For example, each location or organizational unit can have its own schedule.

When you create a new schedule, it appears in the Process Manager portal on the Calendar page.

To add a schedule

1. In the Process Manager portal, click Calendar.
2. On the Schedules page, in the upper right of the Schedules section, click the Add Schedule symbol (a white page with a green plus sign).
3. In the Add Schedule dialog box, on the Schedule Information tab, define the schedule.

See “Add Schedule dialog box” on page 302.

4. To add permissions to the schedule, on the Permissions tab, click Add New Permissions, and then complete the information on the Permissions page that appears.

See “Setting permissions” on page 113.

5. When you finish defining the schedule and its permissions, click Save.

Add Schedule dialog box

This dialog box lets you create a new schedule in the Calendar. In ServiceDesk, a schedule represents a certain type of schedule entry. For example, the Scheduled Changes schedule contains entries for the changes that have been approved and assigned a release date.

See “Creating a new schedule” on page 302.

The Add Schedule dialog box contains the following tabs:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Information</td>
<td>Lets you define the schedule.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Lets you set the permissions for accessing this schedule.</td>
</tr>
</tbody>
</table>

See “Setting permissions” on page 113.
## Table 26-2  Options on the Add Schedule Information tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Identifies this schedule in any schedule list or display in the Process Manager portal. For example, if this schedule is for a specific location, you might use the location name.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Lets you provide additional information to describe the schedule.</td>
</tr>
<tr>
<td><strong>Color</strong></td>
<td>Lets you select the color in which to display the items that appear in this schedule.</td>
</tr>
<tr>
<td><strong>Process Notifications</strong></td>
<td>Sends the email notifications when events occur on this schedule. For example, notifications can be sent when a schedule entry is added, edited, or deleted. The notifications are sent to those who have notify permissions for this schedule. This option is selected by default.</td>
</tr>
</tbody>
</table>

## Adding an entry to the schedule

A schedule entry represents the scheduled time for a specific event in ServiceDesk. For example, an entry can represent a change or a release. Most event entries are created through the ServiceDesk processes. However, you can add an event to the schedule manually. For example, you might add a company meeting, a training session, or other non-process event that can affect the process-related schedules.

The entries that you create appear in the Process Manager portal on the **Calendar** page.

See “Calendar page” on page 57.

### To add an entry to the schedule

1. In the Process Manager portal, click **Calendar**.
2. On the Schedules page, in the upper right of the **Schedule Entries** section, click the **Add Entry** symbol (a white page with a green plus sign).
3. In the **Add Entry** dialog box, on the **Entry Information** tab, define the schedule entry.

   See “Add Entry dialog box” on page 304.
4. When you finish defining the schedule entry, click **Save**.
Add Entry dialog box

This dialog box lets you define an event that you add to a schedule in ServiceDesk. See “Adding an entry to the schedule” on page 303.

The Add Entry dialog box contains the following tabs:

**Entry Information**  
Lets you define the event entry.

**Profiles**  
Lets you view a profile value to the entry.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Schedules</strong></td>
<td>Lets you select the schedule to associate the entry with. The entry takes</td>
</tr>
<tr>
<td></td>
<td>the appearance and permissions that are associated with the selected</td>
</tr>
<tr>
<td></td>
<td>schedule.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Identifies the entry on the calendar display.</td>
</tr>
<tr>
<td><strong>Start Date</strong></td>
<td>Defines when the entry event begins and ends.</td>
</tr>
<tr>
<td><strong>End Date</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Popup Description</strong></td>
<td>Lets you provide a brief description that appears when someone</td>
</tr>
<tr>
<td></td>
<td>hovers over the entry on the calendar display.</td>
</tr>
<tr>
<td><strong>Item Color</strong></td>
<td>Lets you select the color in which to display the item on the schedule.</td>
</tr>
<tr>
<td></td>
<td>You can use different colors to highlight certain types of entries or</td>
</tr>
<tr>
<td></td>
<td>entries for a specific type of schedule.</td>
</tr>
<tr>
<td><strong>Url</strong></td>
<td>Lets you display the content of the schedule entry in a specific page. For</td>
</tr>
<tr>
<td></td>
<td>example, if your organization has an intranet page to announce a special</td>
</tr>
<tr>
<td></td>
<td>event, you can specify that page’s URL. When someone views the schedule</td>
</tr>
<tr>
<td></td>
<td>entry for that event, the intranet page for that event opens.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Lets you provide additional information to describe the entry event.</td>
</tr>
</tbody>
</table>
Managing your organization’s knowledge

- Chapter 27. Introducing Knowledge Management
- Chapter 28. Processing requests for knowledge base entries
- Chapter 29. Managing the knowledge base
- Chapter 30. Using the knowledge base
Introducing Knowledge Management

This chapter includes the following topics:

- About Knowledge Management
- Types of knowledge base items
- About the Bulletin Board
- Knowledge base statuses
- Email notifications from Knowledge Management
- About permissions in the knowledge base

About Knowledge Management

The Knowledge Management process gathers, analyzes, stores, and shares knowledge and information within an organization. The goal of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge. Collecting information in the knowledge base lets organizations match new incidents against previous ones and reuse established solutions and approaches.

When the knowledge base is implemented correctly, it can significantly improve incident resolution time and customer satisfaction. The knowledge base can contain information about the best practices that address the most common issues that users encounter. Instead of having to solve the same customer issues repeatedly, incident technicians can search the knowledge base for information about similar issues. Providing established methods for addressing common incidents reduces response time.
Users can access the knowledge base to obtain self-service resolution of common problems. By providing users with the knowledge resources to solve problems on their own, you can greatly reduce the number of incidents that they submit. When a user submits an incident, they can search the knowledge base to determine if there is a solution to the incident. If the user finds a solution, they might be able to implement the solution on their own. This self-service reduces the number of incidents that are submitted to the ServiceDesk.

In ServiceDesk, the Knowledge Management process provides a means to submit, review, approve, and post information to the knowledge base. The process increases the reliability of the knowledge base so that it can be used to improve the other processes in your organization.

The Knowledge Management process includes the following key features:

- The Bulletin Board, which facilitates proactive notification of important issues. For example, if the Internet access is down, you can let users know that IT is aware of the problem. As a result, you minimize further incident submissions for that issue.
  See “About the Bulletin Board” on page 309.

- The ability to set up a nested category hierarchy to organize knowledge base items and make them easier for users to find.
  See “Adding a knowledge base category or subcategory” on page 326.

- The ability to set permissions at both the category level and the individual document level.
  See “About permissions in the knowledge base” on page 312.

- A knowledge base approval process that helps to ensure that the content is relevant and accurate before publication.
  See “Processing requests for knowledge base entries” on page 313.

- The ability for users to rate knowledge base items based on their usefulness. ServiceDesk automatically gives higher ratings to the articles that are most often used to resolve issues. You can run reports on the ratings to determine which knowledge base items should be removed or modified to improve their content.

- A fully-audited content management system that stores the knowledge base content. You can run reports to analyze this content. For example, you can report the number of times a knowledge base item was viewed and how recently it was viewed.

- The accessibility of the knowledge base information from within the ServiceDesk processes. Easy access from processes lets users take full advantage of the knowledge base, as well as easily add new content to the knowledge base.
See “Processing requests for knowledge base entries” on page 313.
See “What you can do with ServiceDesk” on page 24.

Types of knowledge base items

The ServiceDesk knowledge base can contain several types of items. These items help organize the information and provide users with different levels of information to meet a variety of needs.

Table 27-1 Types of knowledge base items

<table>
<thead>
<tr>
<th>Knowledge base item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article</td>
<td>A general-purpose, informational document. The article format provides the most flexibility. In addition to text, an article can contain images, formatted HTML, and links. An article has no size limitations.</td>
</tr>
<tr>
<td>FAQ (frequently asked question)</td>
<td>Provides the information in a question-and-answer format. FAQ items typically provide self-service information but can be used for other purposes as well.</td>
</tr>
<tr>
<td>Bulletin board message</td>
<td>A message that provides users with time-sensitive, critical information. Bulletin board items have date restrictions and a priority.</td>
</tr>
<tr>
<td></td>
<td>See “About the Bulletin Board” on page 309.</td>
</tr>
<tr>
<td>Wiki article</td>
<td>A group of related articles, entries, or other documents and files about a specific topic.</td>
</tr>
</tbody>
</table>

About the Bulletin Board

The Bulletin Board is a Web part that appears on most of the main pages in the Process Manager portal. It contains any number of messages, which scroll up the Bulletin Board section. A bulletin board message provides users with time-sensitive, critical information.

The bulletin board messages are components of the ServiceDesk knowledge base. However, the Bulletin Board provides a proactive way to display the time-sensitive messages to ServiceDesk users without requiring them to access the Knowledge Base page.

Examples of how you can use the Bulletin Board are as follows:

- Inform users about critical, known issues.
For example, if email access is down, you can let users know that IT is aware of the problem. As a result, you minimize further incident submissions for that issue.

- Inform users about upcoming outages and planned disruptions in service.
- Leave public or private messages for specific users, groups, or organizational units.

Like the other items in the knowledge base, you can set permissions on bulletin board messages. Therefore, you can create messages for certain segments of your organization. You can also provide creation permissions so that others can create messages for the members of their groups or departments.

Bulletin Board messages can be created as a result of the Knowledge Management process or outside the process on the Knowledge Base page. Bulletin Board messages can also be created by using the Add Bulletin Board Entry and Create Bulletin Board Entry Process Type Actions that appear on the Process View pages of the ServiceDesk process.

See “Processing requests for knowledge base entries” on page 313.

See “Creating a knowledge base item from the Knowledge Base page” on page 328.

### Knowledge base statuses

The knowledge base request status accurately reports the progression and outcome of the stages of the knowledge base process. The percentage represents the level of completion that the process has reached. For example, if the status percentage is 60, it means that the process is 60 percent complete.

The status and percentage appear in several places in the Process Manager portal. For example, they appear at the top of the ticket’s Process View page.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Completion percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed</td>
<td>The process is complete as a result of either of the following actions:</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>- A knowledge base article was created.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The knowledge base article was removed.</td>
<td></td>
</tr>
</tbody>
</table>
Table 27-2  Knowledge base statuses (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Completion percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Article</td>
<td>The creation of the knowledge base article is underway.</td>
<td>80%</td>
</tr>
<tr>
<td></td>
<td>This status appears only if your Knowledge Management workflow is customized to skip the approval step.</td>
<td></td>
</tr>
<tr>
<td>Review Proposed KB Article</td>
<td>A request for a knowledge base article was submitted and is ready to be worked.</td>
<td>20%</td>
</tr>
<tr>
<td>Review Request to Remove the KB Submittal</td>
<td>The knowledge base request was rejected and is in a waiting state for the knowledge base approver to remove it.</td>
<td>60%</td>
</tr>
<tr>
<td>Review Request to Create KB Entry</td>
<td>The knowledge base request was accepted and edited and is ready for the final review, or the review is underway.</td>
<td>60%</td>
</tr>
</tbody>
</table>

Email notifications from Knowledge Management

ServiceDesk sends email notifications at various stages of the Knowledge Management process. In this context, a knowledge base event is any action that is taken to request or create a knowledge base article. The type of event and the ServiceDesk configurations determine the recipients of the email notifications.

When you create an item in the knowledge base, you can specify whether notifications should be sent for that item.

Table 27-3  Default knowledge base events that trigger email notifications

<table>
<thead>
<tr>
<th>Event</th>
<th>Email recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>A knowledge base request is submitted.</td>
<td>The submitter</td>
</tr>
<tr>
<td>A knowledge base request is approved or rejected.</td>
<td>The submitter or the user on whose behalf someone submitted the request</td>
</tr>
</tbody>
</table>
Table 27-3  Default knowledge base events that trigger email notifications (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Email recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>A knowledge base article is changed.</td>
<td>Any user A user can set up an automatic email notification to be informed of changes to a specific article.</td>
</tr>
<tr>
<td>The Bulletin Board is cleared.</td>
<td>Any user A user can set up an automatic email notification to be informed when the Bulletin Board is cleared.</td>
</tr>
</tbody>
</table>

About permissions in the knowledge base

Access to knowledge base items is controlled through permissions. Permissions can be set on the knowledge base categories and on the individual knowledge base items. Permissions can be granted to users, groups, and organizational units.

The knowledge base items that are created through the Knowledge Management process contain default group permissions. Those default permissions can be edited from the KnowledgeBase page. The knowledge base items that are created outside the process do not have default permissions. The permissions must be assigned during or after the item creation.

Typically, only the administrator or other user with the appropriate permissions can set permissions on knowledge base items and categories. For example, the knowledge base editors and approvers cannot set permissions for the items that are in the default categories. However, they can set permissions on the items that are in the categories that they created.

See “Creating a knowledge base item from the Knowledge Base page” on page 328.
See “Adding a knowledge base category or subcategory” on page 326.
See “Setting permissions” on page 113.
Processing requests for knowledge base entries

This chapter includes the following topics:

■ Processing requests for knowledge base entries
■ Roles in Knowledge Management
■ Sources of knowledge base requests and entries
■ Submitting a request for a knowledge base entry
■ Accepting or rejecting a knowledge base request
■ Create KB Article dialog box
■ Reviewing a knowledge base entry for final resolution

Processing requests for knowledge base entries

In ServiceDesk, the Knowledge Management process provides a means to submit, review, approve, and post information to the knowledge base. The process increases the reliability of the knowledge base so that it can be used to improve the other processes in your organization.

See “Roles in Knowledge Management” on page 314.
## Table 28-1 Process for submitting and reviewing requests for knowledge base entries

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>A request for a knowledge base entry is submitted.</td>
<td>Requests for a knowledge base entry can originate from the Service Catalog, incidents, or problems. See “Submitting a request for a knowledge base entry” on page 317. See “Sources of knowledge base requests and entries” on page 315. When the request is submitted, a task to review the knowledge base request is assigned to the knowledge base editor.</td>
</tr>
<tr>
<td>Step 2</td>
<td>The knowledge base editor reviews the request.</td>
<td>After a knowledge base request is submitted, a knowledge base editor reviews the request and accepts or rejects it. When the request is accepted, the editor can categorize the entry and edit it to improve usability. See “Accepting or rejecting a knowledge base request” on page 318. When the knowledge base editor finishes working with the request, a task is assigned to the knowledge base approver.</td>
</tr>
<tr>
<td>Step 3</td>
<td>The knowledge base approver reviews the request and determines how to handle it.</td>
<td>The knowledge base approver makes the final decision to post or remove a proposed knowledge base item. The approver can also return the request to the knowledge base editor for further editing or reconsideration.</td>
</tr>
<tr>
<td>Step 4</td>
<td>The knowledge base approver posts the entry to the knowledge base.</td>
<td>After the knowledge base entry is posted, it is available to all users.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) The knowledge base approver sets additional restrictions on the entry.</td>
<td>The knowledge base items that are created through the Knowledge Management process contain default group permissions. If access to the entry needs to be restricted further, the knowledge base approver can edit the entry and its permissions from the Knowledge Base page. See “About permissions in the knowledge base” on page 312.</td>
</tr>
</tbody>
</table>

An administrator or other user with the appropriate permissions can create knowledge base items outside the Knowledge Management process. See “Creating a knowledge base item from the Knowledge Base page” on page 328.

### Roles in Knowledge Management

ServiceDesk employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes.
The roles in the Knowledge Management process are tasked with editing, approving, and categorizing knowledge base entries.

See “Processing requests for knowledge base entries” on page 313.

Table 28-2 Roles in Knowledge Management

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB editor</td>
<td>Reviews a knowledge base request and approves or rejects it. The editor can categorize the entry and edit the title or content to improve usability.</td>
</tr>
<tr>
<td>KB approver</td>
<td>Reviews the proposed entry and provides a final approval for posting the entry to the knowledge base.</td>
</tr>
</tbody>
</table>

Sources of knowledge base requests and entries

The creation of a knowledge base request triggers the Knowledge Management process for approving and creating knowledge base items. A knowledge base request can originate from several sources.

See Table 28-3.

The administrator or other user with the appropriate permissions can also create knowledge base entries outside the approval process.

See Table 28-4.

Table 28-3 Sources of knowledge base requests for the Knowledge Management process

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Manager portal</td>
<td>A user requests the creation of a knowledge base entry by creating a knowledge base request in the Process Manager portal.</td>
</tr>
<tr>
<td></td>
<td>See “Submitting a request for a knowledge base entry” on page 317.</td>
</tr>
</tbody>
</table>
### Table 28-3  Sources of knowledge base requests for the Knowledge Management process (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident resolution</td>
<td>During the incident resolution process, on the <strong>Create Incident Details</strong> page, the support technician selects the option to create a knowledge base entry.</td>
</tr>
<tr>
<td></td>
<td>See “Resolving an incident from the advanced incident form” on page 169.</td>
</tr>
<tr>
<td></td>
<td>This option lets the support technician request an entry that can provide help for the same kind of issue in the future. For example, if the issue was resolved by training the user, the technician can request a knowledge base article that contains the same information. Users who encounter that issue in the future can find and read the knowledge base article instead of creating an incident.</td>
</tr>
<tr>
<td>Problem Management</td>
<td>During the problem review, on the <strong>Review Proposal</strong> page, the problem manager selects the option to create a knowledge base entry.</td>
</tr>
<tr>
<td></td>
<td>See “Reviewing a proposed fix or workaround” on page 277.</td>
</tr>
<tr>
<td></td>
<td>Creating a knowledge base entry is one way to resolve a problem. For example, if the problem cannot be fixed but a workaround exists, the workaround can be documented in a knowledge base article.</td>
</tr>
</tbody>
</table>

See “Processing requests for knowledge base entries” on page 313.

### Table 28-4  Sources of knowledge base items outside the process

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Base</td>
<td>On the <strong>Knowledge Base</strong> page, the administrator or other user with the appropriate permissions selects any of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Add Article</td>
</tr>
<tr>
<td></td>
<td>■ Add Bulletin Board</td>
</tr>
<tr>
<td></td>
<td>■ Add FAQ</td>
</tr>
<tr>
<td></td>
<td>■ Add Wiki</td>
</tr>
<tr>
<td></td>
<td>See “Creating a knowledge base item from the Knowledge Base page” on page 328.</td>
</tr>
</tbody>
</table>
Table 28-4  Sources of knowledge base items outside the process (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process View page of an incident, change request, or problem ticket</td>
<td>On the Process View page of an incident, change request, or problem ticket, process workers can create Bulletin Board messages. They can use the Add Bulletin Board Entry and Create Bulletin Board Entry Process Type Actions to create these messages.</td>
</tr>
</tbody>
</table>

Submitting a request for a knowledge base entry

Before it can be added to the knowledge base, most new content must go through the knowledge base approval and review process.

This task is a step in the process for creating a knowledge base entry.

See “Processing requests for knowledge base entries” on page 313.

The knowledge base article request is created, and a confirmation screen displays the process ID for the entry request. The proposed knowledge base entry now goes to a knowledge base editor, who approves or denies the request. Click Close to close the dialog.

To submit a request for a knowledge base entry

1. In the Process Manager portal, click Submit Request.
2. On the Submit Requests page, under Service Catalog, click IT Services.
3. On the right side of the page, click the Submit Knowledge Base Entry link.
4. In the Entry Request dialog box, define the entry as follows:

   **Title**      Type a title to identify this entry in any article lists or search results in the Process Manager portal. When you type the title, make it as specific as possible so that it quickly conveys the purpose of the entry. For example, instead of “printer jam,” you might type “Clearing a printer jam”.

   **Content**    Type and format the content for the proposed entry.

5. In the Entry Request dialog box, click Submit.
6. In the Thank You dialog box, click Close.
Accepting or rejecting a knowledge base request

After a knowledge base request is submitted, a knowledge base editor reviews the request and accepts or rejects it. The editor can categorize the entry and edit it to improve usability.

To prevent the addition of duplicate entries, ServiceDesk can determine if similar entries already exist and display the duplicates to the editor.

This task is a step in the process for creating a knowledge base entry.

See “Processing requests for knowledge base entries” on page 313.

Whether the request is accepted or rejected, a task is created for the knowledge base reviewer to review it and take final action.

See “Reviewing a knowledge base entry for final resolution” on page 320.

To review a knowledge base request

1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Tasks Viewer, under Project Name, expand SD.KBSubmission.
3. In the list of tasks, find and open a request that has the status Review Proposed KB Article.
4. On the ticket’s Process View page, under My Actions, click Review KB Request.
5. If the request’s title or content matches that of an existing entry, in the Possible Duplicate Entries dialog box, click the View link.

Note: If the request is a duplicate, follow the steps in To designate a duplicate knowledge base entry.

6. Close the article’s view page.
7. In the Possible Duplicate Entries dialog box, click Continue.
8. In the Create KB Article dialog box, review the entry submission, and then take one of the following actions:

   To reject the request  Follow the steps in To reject a knowledge base request.
   To accept the request  Follow the steps in To accept a knowledge base request.
To designate a duplicate knowledge base entry

1. Close the duplicate article's view page.
2. In the Possible Duplicate Entries dialog box, click Duplicate.
3. In the Reason for Closing this Request dialog box, provide a reason for rejecting the entry, and then click Submit.
4. In the Thank You dialog box, click Close.
5. When you are returned to the task’s Process View page, you can close it.

To reject a knowledge base request

1. In the Create KB Article dialog box, click Reject Submission.
2. In the Close Request dialog box, provide a reason for rejecting the entry, and then click Submit.
3. In the Thank You dialog box, click Close.
4. When you are returned to the task’s Process View page, you can close it.

To accept a knowledge base request

1. In the Create KB Article dialog box, categorize and enter additional information about the knowledge base entry.

   See “Create KB Article dialog box” on page 319.
2. When you are satisfied with the information, click Preview.
3. In the Preview Post dialog box, review the entry in its final format, and then click Submit.
4. In the Thank You dialog box, click Close.
5. When you are returned to the task’s Process View page, you can close it.

Create KB Article dialog box

This dialog box lets you review a request for a knowledge base entry, edit it, categorize it, and accept or reject it. It appears when a knowledge base editor clicks Review KB Request on the request’s Process View page.

See “Accepting or rejecting a knowledge base request” on page 318.
### Table 28-5 Options in the Create KB Article dialog box

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Knowledge Type</strong></td>
<td>Lets you select the type of knowledge base item that the submission should be created as. The knowledge base item types are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Article</td>
</tr>
<tr>
<td></td>
<td>■ Wiki</td>
</tr>
<tr>
<td></td>
<td>■ FAQ</td>
</tr>
<tr>
<td></td>
<td>■ Bulletin Board</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Lets you select the category in which to place the knowledge base entry. You can also create a new category by clicking New Category.</td>
</tr>
<tr>
<td></td>
<td>See “Adding a knowledge base category or subcategory” on page 326.</td>
</tr>
<tr>
<td><strong>Parent Entry</strong></td>
<td>(Optional) Lets you link entry articles by selecting a parent entry. You can choose from the other entries that are in the same category as the new entry.</td>
</tr>
<tr>
<td></td>
<td>When a user searches the knowledge base, child entries are also displayed as links.</td>
</tr>
<tr>
<td><strong>Description/Explanation of Question</strong></td>
<td>Lets you provide a description of the article or a more detailed explanation of the question. This description appears under the title of the knowledge base item on the Knowledge Base page.</td>
</tr>
<tr>
<td><strong>Edit Title/Question</strong></td>
<td>(Optional) Lets you edit the title of the entry question to improve its usability. Depending on the entry type and category, you might use a question format.</td>
</tr>
<tr>
<td></td>
<td>Examples of possible titles and questions are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ If the entry describes how to reset a password, you might type <em>How do I reset a password?</em>.</td>
</tr>
<tr>
<td></td>
<td>■ If the entry explains when a password must be changed, you might type <em>How often should I change my password?</em>.</td>
</tr>
<tr>
<td></td>
<td>■ If the entry is an article that lists password creation standards, you might type <em>Guidelines for strong passwords</em>.</td>
</tr>
<tr>
<td><strong>Content/Answer</strong></td>
<td>Lets you edit or add to the content of the entry.</td>
</tr>
</tbody>
</table>

### Reviewing a knowledge base entry for final resolution

After a knowledge base editor accepts or rejects a knowledge base request, the knowledge base approver receives a task to make a final decision. The knowledge base approver can take the following actions:

- Approve and submit the entry.
- Edit the entry before approving it.
Reject the entry.

Return the request to the knowledge base editor for further editing or reconsideration.

The knowledge base approver can review the tasks that have the following statuses:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Request to Create KB Entry</td>
<td>This status represents a request that the knowledge base editor accepted. You can return it for further editing, reject it, edit it, or approve it.</td>
<td>Reviewing a request to create a knowledge base entry.</td>
</tr>
<tr>
<td>Review Request to Remove the KB Submittal</td>
<td>This status represents a request that the knowledge base editor rejected. You can agree to remove the request or you can decide to return the request to the editor for further editing or consideration.</td>
<td>Reviewing a knowledge base entry rejection.</td>
</tr>
</tbody>
</table>

**Reviewing a request to create a knowledge base entry**

1. In the Process Manager portal, click My Task List.

2. On the My Task List page, under Task Viewer, under Project Name, expand SD.KBSubmission.

3. In the list of tasks, find and open a request that has the status Review Request to Create KB Entry.
On the ticket’s Process View page, under My Actions, click Approve KB Request.

In the Approve Post dialog box, select one of the following options:

Return to Editors

- Select this option if the entry needs further review or edits.
- In the Return Request dialog box, enter a reason for returning the request, and then click Return.
- When you enter the reason for the return, you might also provide suggestions for changing the entry.

Remove Submission

- Select this option to reject the entry and remove the request.
- In the Close Request dialog box, enter a reason for removing the request, and then click Submit.

Edit Request

- Select this option to edit the request before you take further action.
- In the Edit KB Details dialog box, review and edit the entry as needed, and then click Preview. Step through the remaining dialog boxes to submit the entry and close the process.
- See “Create KB Article dialog box” on page 319.

Approve

- Select this option to close the request and create the entry in the knowledge base.

Reviewing a knowledge base entry rejection

1 In the Process Manager portal, click My Task List.

2 On the My Task List page, under Task Viewer, under Project Name, expand SD.KBSubmission.

3 In the list of tasks, find and open a request that has the status Review Request to Remove the KB Submittal.
4 On the ticket’s Process View page, under My Actions, click Approve KB Removal Request.

5 In the Review Rejection dialog box, select one of the following options:

**Reject**

Select this option to overturn the original decision to reject the request. The request is returned to the queue for the knowledge base editor to reconsider the decision and possibly make changes.

In the Return Request dialog box, enter the reason for your decision, and then click Return.

In the Thank You dialog box, click Close.

**Approved**

Select this option when you agree that the original request should be rejected.

In the Thank You dialog box, click Close.
Processing requests for knowledge base entries

Reviewing a knowledge base entry for final resolution
Managing the knowledge base

This chapter includes the following topics:

- About knowledge base categories
- Adding a knowledge base category or subcategory
- Moving a knowledge base item to a different category
- Creating a knowledge base item from the Knowledge Base page
- Add Article dialog box
- Add Bulletin dialog box
- Add FAQ dialog box
- Add Wiki dialog box
- Adding entries and links to a wiki article
- Links in wiki articles

About knowledge base categories

ServiceDesk uses categories to classify its knowledge base items. The knowledge base categories help the ServiceDesk workers and users find the information that they need. You can use additional levels of categories to group the items further. A knowledge base category can have multiple subcategories, and you can nest the subcategories.
ServiceDesk contains a hierarchy of predefined knowledge base categories. You can add categories and manage the existing ones on the Knowledge Base page in the Process Manager portal.

See “Adding a knowledge base category or subcategory” on page 326.

You can set permissions for the knowledge base categories and subcategories. The permissions determine who can access a knowledge base category and all the items that it contains.

Adding a knowledge base category or subcategory

Knowledge base categories and subcategories help you organize all the knowledge base items in ServiceDesk.

To add a knowledge base category

To add a knowledge base subcategory

Organizing the items in categories helps users find the items they need more easily.

You can grant category permissions to users, groups, and organizational units. The category permissions provide or deny access to a category and all the knowledge base items within it. Permissions also determine who can create subcategories for a specific category.

To add a knowledge base category

1 In the Process Manager portal, click Knowledge Base.

2 On the Knowledge Base page, under Article Category List, click the Add Category symbol (file folder with green plus sign), and then click Add Root Category.

3 In the Add Root Category dialog box, on the Main Information tab, provide a title and description for the category.

   The title identifies the category in any list or display of knowledge base categories in the Process Manager portal.

4 Click the Permissions tab, and then specify the permissions for one or more users, groups, permissions, or organizational units.

   See “Setting permissions” on page 113.

5 When you finish defining the category, click Save.
To add a knowledge base subcategory

1. In the Process Manager portal, click Knowledge Base.

2. On the Knowledge Base page, under Article Category List, select the category to which you want to add the subcategory.

3. Click the Add Category symbol (file folder with green plus sign), and then click Add Sub Category.

4. In the Add Sub Category dialog box, on the Main Information tab, provide a title and description for the subcategory. The title identifies the subcategory in any list or display of knowledge base subcategories in the Process Manager portal.

5. Click the Permissions tab, and then specify the permissions for one or more users, groups, permissions, or organizational units. See “Setting permissions” on page 113.

6. When you finish defining the subcategory, click Save.

Moving a knowledge base item to a different category

You can reorganize the items in the knowledge base by assigning them to different categories or subcategories.

For example, you might have assigned all your FAQ articles to the How To category. Over time, that category becomes full and its contents become harder to find. You can create subcategories for the How To category, and then move items to the subcategories.

See “Adding a knowledge base category or subcategory” on page 326.

When you move a knowledge base item, it inherits the permissions of its new category.

To move a knowledge base item to a different category

1. In the Process Manager portal, click Knowledge Base.

2. Find or navigate to the item to move.

3. Under All Articles, to the right of the item, click the Actions symbol (orange lightning), and then click Move to Category.

4. In the Move Article dialog box, click Pick.

5. In the dialog box that appears, expand the categories if necessary, and then select the category to which you want to move the item.

6. In the Move Article dialog box, click Move.
Creating a knowledge base item from the Knowledge Base page

An administrator or other user who has the appropriate permissions can create knowledge base items outside the Knowledge Management process.

**To create a knowledge base item from the Knowledge Base page**

1. In the Process Manager portal, click **Knowledge Base**.
2. On the **Knowledge Base** page, under **Categories**, select the category to add the item to.
   
   If the appropriate category is not listed, you can add a new one.
   
   See “**Adding a knowledge base category or subcategory**” on page 326.
3. On the **Knowledge Base** page, in the right pane, click one of the following options:
   
   - **Add Article**
     
     See “**Add Article dialog box**” on page 329.
   
   - **Add Bulletin Board**
     
     See “**Add Bulletin dialog box**” on page 330.
   
   - **Add FAQ**
     
     See “**Add FAQ dialog box**” on page 332.
   
   - **Add Wiki**
     
     See “**Add Wiki dialog box**” on page 333.
4. In the dialog box that appears, perform any of the following actions:

   Note that the dialog box that appears depends on the type of item that you chose to add.

   - Add the title and contents of the item.
   - Add a description of what information the item contains.
   - Attach additional files (**Add Article** dialog box only).
   - Decide whether to send email notifications of the items event.
   - Add permissions for the item.
   - Add keywords for the item to make it more searchable.
   - Add tags to provide a second method of searching for the item.

5. When you finish entering the information, click **Save**.
Add Article dialog box

This dialog box lets you create knowledge base articles outside the Knowledge Management process.

See “Creating a knowledge base item from the Knowledge Base page” on page 328.

When you edit an article or an article entry, the Edit Article and Edit Entry Information To Article dialog boxes contain similar options.

When an article is first created, it consists of one entry. More entries can be added later. For example, instead of editing the original entry, you can add an entry that contains updates or corrections.

Table 29-1   Tabs in the Add Article dialog box

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article Information</td>
<td>Lets you define the contents of the article.</td>
</tr>
<tr>
<td>Description</td>
<td>Appears beneath the article title in any list or display of knowledge base items in the Process Manager portal. The description helps the users decide whether to view the article in more detail. When you edit an existing article, the Description box appears on the Article Information tab.</td>
</tr>
<tr>
<td>Attachment</td>
<td>Lets you add an attachment to the article. For example, you can add an attachment as a source to an article's premise.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Contains the Process Notifications option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. The notifications are sent to those who have notify permissions for the item. This option is selected by default.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Lets you set the permissions for the item. See “Setting permissions” on page 113.</td>
</tr>
<tr>
<td>Profiles</td>
<td>(Optional) Lets you apply profiles to the item.</td>
</tr>
<tr>
<td>Key Words</td>
<td>Lets you apply keywords to the item.</td>
</tr>
<tr>
<td>Tags</td>
<td>Lets you apply tags to the item.</td>
</tr>
</tbody>
</table>

In the Options on the Article Information tab table, the options that are marked as entry-specific apply to each entry. The other options apply to the entire article. You cannot edit the entry-specific options directly from the Knowledge Base page. Instead, you must open the article and select the option to edit an entry.
Table 29-2  Options on the Article Information tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Name</td>
<td>(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way that the category can be changed is by moving the item to a different category. See “Moving a knowledge base item to a different category” on page 327.</td>
</tr>
<tr>
<td>Article Title</td>
<td>Identifies the item in any list or display of knowledge base items in the Process Manager portal.</td>
</tr>
<tr>
<td>Entry Title</td>
<td>(Entry-specific) Appears on the page that opens when a user views the article.</td>
</tr>
<tr>
<td>Text</td>
<td>(Entry-specific) Lets you provide the more extensive information that appears when a user views the article. This information is associated with the entry title.</td>
</tr>
</tbody>
</table>

Add Bulletin dialog box

This dialog box lets you create bulletin board messages outside the Knowledge Management process.

See “Creating a knowledge base item from the Knowledge Base page” on page 328. When you edit a bulletin board message or a message entry, the Edit Bulletin and Edit Entry Information To Article dialog boxes contain similar options.

When a bulletin board message is first created, it consists of one entry. More entries can be added later. For example, instead of editing the original entry, you can add an entry that contains updates or corrections. The entries appear separately on the Bulletin Board.

In Table 29-3, the options that are marked as entry-specific apply to each entry. The other options apply to the entire message. You cannot edit the entry-specific options directly from the Knowledge Base page. Instead, you must open the message and select the option to edit an entry.

Table 29-3  Tabs in the Add Bulletin dialog box

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Information</td>
<td>Lets you define the contents of the bulletin board message.</td>
</tr>
<tr>
<td>Description</td>
<td>Appears beneath the bulletin board title on the Knowledge Base page. Because of space limitations, it does not appear on the Bulletin Board. When you edit an existing bulletin board message, the Description box appears on the Bulletin Information tab.</td>
</tr>
</tbody>
</table>
### Table 29-3  Tabs in the Add Bulletin dialog box (continued)

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifications</td>
<td>Contains the <strong>Process Notifications</strong> option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. The notifications are sent to those who have notify permissions for the item. This option is selected by default.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Lets you set the permissions for the item. See “Setting permissions” on page 113.</td>
</tr>
<tr>
<td>Profiles</td>
<td>(Optional) Lets you apply profiles to the item.</td>
</tr>
<tr>
<td>Key Words</td>
<td>Lets you apply keywords to the item.</td>
</tr>
<tr>
<td>Tags</td>
<td>Lets you apply tags to the item.</td>
</tr>
</tbody>
</table>

In **Options on the Bulletin Information** tab table, the options that are marked as entry-specific apply to each entry. The other options apply to the entire message. You cannot edit the entry-specific options directly from the Knowledge Base page. Instead, you must open the message and select the option to edit an entry.

### Table 29-4  Options on the Bulletin Information tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Name</td>
<td>(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way that the category can be changed is by moving the item to a different category. See “Moving a knowledge base item to a different category” on page 327.</td>
</tr>
<tr>
<td>Bulletin Board Title</td>
<td>Appears at the left of the message on the Bulletin Board. It also appears on the page that opens when a user views the bulletin board message.</td>
</tr>
<tr>
<td>Entry Title</td>
<td>(Entry-specific) Appears on the Bulletin Board as the message heading. It also appears on the page that opens when a user views the bulletin board message. The priority determines the color of the entry title when it appears on the Bulletin Board.</td>
</tr>
<tr>
<td>Priority</td>
<td>(Entry-specific) Lets you indicate the importance of a bulletin board entry. You can set the priority to Low, Medium, High, or Emergency.</td>
</tr>
<tr>
<td>Event Start</td>
<td>(Entry-specific) Indicates the date on which the event starts.</td>
</tr>
<tr>
<td>Event End</td>
<td>(Entry-specific) Indicates the date on which event ends.</td>
</tr>
</tbody>
</table>
### Table 29-4 Options on the **Bulletin Information** tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Display From</strong></td>
<td>(Entry-specific) Indicates the date on which the entry first appears on the Bulletin Board.</td>
</tr>
<tr>
<td><strong>Display Until</strong></td>
<td>(Entry-specific) Indicates the last date on which the entry appears on the Bulletin Board.</td>
</tr>
<tr>
<td><strong>Text</strong></td>
<td>(Entry-specific) Lets you provide the more extensive information that appears when a user opens the bulletin board message. For example, if the bulletin board message announces a planned outage, the text might describe when the outage is planned and which systems it affects. This information is associated with the entry title.</td>
</tr>
</tbody>
</table>

### Add FAQ dialog box

This dialog box lets you create FAQ (frequently asked question) items outside the Knowledge Management process.

See “Creating a knowledge base item from the Knowledge Base page” on page 328.

When you edit a FAQ item, the **Edit FAQ** dialog box contains similar options.

### Table 29-5 Tabs in the **Add FAQ** dialog box

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FAQ Information</strong></td>
<td>Lets you define the contents of the FAQ item.</td>
</tr>
</tbody>
</table>
| **Explanation of Question** | Lets you type information in **Explanation of the Question** to help the users decide whether they selected a FAQ that meets their needs. Typically, the explanation should explain the situation that the FAQ answers.  
For example, if the FAQ question is “How do I clear a printer jam?” you might provide the following explanation:  
**This FAQ describes what to do when paper is stuck in your printer.** |
| **Notifications**    | Contains the **Process Notifications** option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. 
The notifications are sent to those who have notify permissions for the item. 
This option is selected by default. |
| **Permissions**      | Lets you set the permissions for the item.                                                                                                  |
|                      | See “Setting permissions” on page 113.                                                                                                       |
| **Profiles**         | (Optional) Lets you apply profiles to the item.                                                                                                |
Table 29-5  Tabs in the Add FAQ dialog box (continued)

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Words</td>
<td>Lets you apply keywords to the item.</td>
</tr>
<tr>
<td>Tags</td>
<td>Lets you apply tags to the item.</td>
</tr>
</tbody>
</table>

Table 29-6  Options on the FAQ Information tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Name</td>
<td>(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way</td>
</tr>
<tr>
<td></td>
<td>that the category can be changed is by moving the item to a different category. See “Moving a knowledge base item to a different category” on page 327.</td>
</tr>
<tr>
<td>Question</td>
<td>Lets you type a question that the FAQ item answers. Try to write the question from the user’s point of view and in non-technical language. For</td>
</tr>
<tr>
<td></td>
<td>example: How do I clear a printer jam?</td>
</tr>
<tr>
<td>Answer</td>
<td>Lets you provide the solution to the user’s question. The answer format depends on the nature of the question. For example, if the question asks</td>
</tr>
<tr>
<td></td>
<td>how to perform a task, you can format the answer as a series of numbered steps. If the question asks for conceptual or reference information, you</td>
</tr>
<tr>
<td></td>
<td>can format the answer as a paragraph or a table, respectively.</td>
</tr>
</tbody>
</table>

Add Wiki dialog box

This dialog box lets you create wiki articles outside the Knowledge Management process. When you edit a wiki article or an article entry, the Edit Wiki and Edit Wiki Entry dialog boxes contain similar options. See “Creating a knowledge base item from the Knowledge Base page” on page 328.

Table 29-7  Tabs in the Add Wiki dialog box

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiki Information</td>
<td>Lets you define the contents of the wiki article.</td>
</tr>
</tbody>
</table>
### Table 29-7  
Tabs in the Add Wiki dialog box *(continued)*

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiki Description</td>
<td>Appears beneath the wiki article title in any list or display of knowledge base items in the Process Manager portal. The description helps the users decide whether to view the wiki article in more detail. When you edit an existing article, the <strong>Description</strong> box appears on the <strong>Article Information</strong> tab.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Contains the <strong>Process Notifications</strong> option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. The notifications are sent to those who have notify permissions for the item. This option is selected by default.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Lets you set the permissions for the item. See “<a href="#">Setting permissions</a>” on page 113.</td>
</tr>
<tr>
<td>Profiles</td>
<td>(Optional) Lets you apply profiles to the item.</td>
</tr>
<tr>
<td>Key Words</td>
<td>Lets you apply keywords to the item.</td>
</tr>
<tr>
<td>Tags</td>
<td>Lets you apply tags to the item.</td>
</tr>
</tbody>
</table>

### Table 29-8  
Options on the Wiki Information tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Name</td>
<td>(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way that the category can be changed is by moving the item to a different category. See “<a href="#">Moving a knowledge base item to a different category</a>” on page 327.</td>
</tr>
<tr>
<td>Wiki Title</td>
<td>Identifies the item in any list or display of knowledge base items in the Process Manager portal.</td>
</tr>
<tr>
<td>Mark as Obsolete</td>
<td>Indicates that the item is no longer current. By default, obsolete items do not appear on the Knowledge Base page. Obsolete items can be viewed if the Show Obsolete Articles option is selected.</td>
</tr>
</tbody>
</table>
Table 29-8 Options on the Wiki Information tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Lets you provide the more extensive information that appears when a user opens the wiki article. You can add links in the text area to provide access to related information. See “Adding entries and links to a wiki article” on page 335. See “Links in wiki articles” on page 336.</td>
</tr>
</tbody>
</table>

Adding entries and links to a wiki article

When you create a wiki article and its subentries, you can add links to the text area to provide access to related information. For example, you can link to another subentry, a knowledge base article, a document, or an image file.

See “Creating a knowledge base item from the Knowledge Base page” on page 328.

To add entries and links to a wiki article

1. In the Process Manager portal, click Knowledge Base.
2. On the Knowledge Base page, open an existing wiki article.
   You can also add a link at the same time that you create a new wiki article. However, you must save the article and then open it to connect the link to its target.
3. On the Links in wiki dialog box, click the Actions symbol (orange lightning), and then click Edit Entry.
4. In the Edit Wiki Entry dialog box, in Text, type a link in the appropriate format.
   See “Links in wiki articles” on page 336.
5. Enter any additional information as needed, and then click Save.
6. On the article view page reappears, click the link.
   The link appears in the following format:
   `??_<link>_??`
7. Depending on the type of link that you entered, you might be required to type text or select a file or document to add.
8. When you finish creating the new entry, click Save.
9. Close the Links in wiki dialog box.
When you create a wiki article and its subentries, you can add links to the text area to provide access to related information. Several types of links are available. See “Adding entries and links to a wiki article” on page 335.

<table>
<thead>
<tr>
<th>Link syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[[article]]</code></td>
<td>Links to any type of knowledge base item. The title of the knowledge base item becomes the link text. When you click this link during the entry creation, a small version of the Knowledge Base page appears, where you select the item to link to.</td>
</tr>
<tr>
<td><code>[[file]]</code></td>
<td>Links to any type of document file. The document title or file name becomes the link text. When you click this link during the entry creation, a small version of the Documents page appears, where you select the file to link to. If the file is not listed, you can add it. See “Adding a document to the Document Management system” on page 355.</td>
</tr>
<tr>
<td><code>[[home]]</code></td>
<td>Links to the main entry for the wiki article.</td>
</tr>
<tr>
<td><code>[[image]]</code></td>
<td>Links to an image file that is stored in the ServiceDesk document management system. When you click this link during the entry creation, a small version of the Documents page appears, where you select the image to link to. If the image is not listed, you can add it. See “Adding a document to the Document Management system” on page 355.</td>
</tr>
<tr>
<td><code>[[new entry title]]</code></td>
<td>Links to a new entry. The text that you type within the brackets becomes the title of the new entry and the name of the link that the user sees. When you click this link during the entry creation, a new entry page appears, where you can type information for the new entry.</td>
</tr>
<tr>
<td><code>[[owner]]</code></td>
<td>Links to the entry that is the parent of the current entry.</td>
</tr>
</tbody>
</table>
Table 29-9 Types of links in wiki articles (continued)

<table>
<thead>
<tr>
<th>Link syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| [[text to link|Title To Show]] | Links to another entry. The link that the user sees is not the same as the entry title. The `text to link` segment is the name of the link. You can specify any of the wiki links. The contents of the `text to link` segment becomes the name of the link that the user sees in the wiki article. Examples of how you can use this link format are as follows:  
  - [[article|Click here to open an article.]]
    The link text becomes “Click here to open an article.”  
  - [[About Wikis|Learn more about wikis.]]
    The title of the new entry becomes “About Wikis” and the link text becomes “Learn more about wikis.” |
Managing the knowledge base

Links in wiki articles
Using the knowledge base

This chapter includes the following topics:

- Searching the knowledge base
- Viewing an item in the knowledge base
- What you can do with a knowledge base item

Searching the knowledge base

You can search for knowledge base items on the Knowledge Base page. The knowledge base searches are performed as follows:

- The search is performed on the article title, text, and description fields.
- The search evaluates the items in all the knowledge base categories.
- Your permissions determine the categories and items that you can access, which in turn influences the results of your searches.

When you find a knowledge base item, you can open and view it or perform other actions.

See “What you can do with a knowledge base item” on page 340.

To search the knowledge base

1. In the Process Manager portal, click Knowledge Base.
2. On the Knowledge Base page, under Search Articles, type the text to search for, and then click the Search symbol (magnifying glass).

Viewing an item in the knowledge base

You view knowledge base items on the Knowledge Base page.
To view an item in the knowledge base

1. In the Process Manager portal, click **Knowledge Base**.

2. On the **Knowledge Base** page, take one of the following actions:

   - Under **Search Articles**, type the text to search for, and then click the **Search** symbol (magnifying glass).
   - Under **Article Category List**, select a category that is likely to contain the item.
   - Under **Tag Cloud**, select a tag that is likely to contain the item.

3. Under **All Articles**, scroll through the list of knowledge base items to find one that might provide the information you need.

   If you cannot find what you need, you can repeat step 2.

4. To open an item, click its article name or click the **Open** symbol (a magnifying glass) that appears at the far right of its name.

5. If the item contains multiple entries, you can expand and collapse them to view their information.

6. (Optional) Take any other actions that you need.

   Your permissions determine what you can do with a knowledge base item. For example, typical actions are to view the item’s history, print it, or export it.

   See “**What you can do with a knowledge base item**” on page 340.

---

### What you can do with a knowledge base item

When you open and view a knowledge base item, you might have additional options for interacting with that item.

See “**Viewing an item in the knowledge base**” on page 339.

All the options except **Add New Entry** are available on the drop-down list that appears when you click the **Actions** symbol (orange lightning) for an item.

Your permissions determine the options that are available to you. For example, typical actions are to view the item’s history, print it, or export it.

---

#### Table 30-1 Options for working with a knowledge base item

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Comment</td>
<td>Lets you comment on the knowledge base item.</td>
</tr>
</tbody>
</table>
Table 30-1  Options for working with a knowledge base item (continued)

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New Entry</td>
<td>Lets you add an entry to the knowledge base item. For example, a knowledge base article can consist of several entries.</td>
</tr>
<tr>
<td>Delete Entry</td>
<td>Lets you delete the selected entry.</td>
</tr>
<tr>
<td>Edit Entry</td>
<td>Lets you edit the entries of a knowledge base item.</td>
</tr>
<tr>
<td>Edit FAQ</td>
<td>FAQ items do not contain additional entries.</td>
</tr>
<tr>
<td>Export</td>
<td>Lets you save the knowledge base item to a file.</td>
</tr>
<tr>
<td>Send Entry</td>
<td>Lets you specify one or more email addresses to send the entry to.</td>
</tr>
<tr>
<td>Print</td>
<td>Lets you print the knowledge base item.</td>
</tr>
<tr>
<td>Rating</td>
<td>Displays five stars and lets you rate the item by selecting one of the stars. The first star is the lowest rating, and the last star is the highest rating.</td>
</tr>
<tr>
<td>View History</td>
<td>Displays the events that have occurred for the knowledge base item. For example, the list includes the additions and edits that were made to the item.</td>
</tr>
</tbody>
</table>
What you can do with a knowledge base item
Managing the documents in ServiceDesk

- Chapter 31. Adding and managing documents
- Chapter 32. Viewing documents
Adding and managing documents

This chapter includes the following topics:

- About Document Management
- About Document Management in the ServiceDesk processes
- About document categories
- Adding a document category
- Adding a document subcategory
- Category and Sub Category dialog boxes
- Editing a document category
- Setting permissions for a document category
- Deleting a document category
- Displaying the history of a document category
- Creating expected document messages
- Expected Documents dialog box
- Adding a document to the Document Management system
- Add Documents dialog box
- Add Advanced Document dialog box
- Setting permissions for a document
About Document Management

The Document Management system in ServiceDesk lets you store, track, and use, the documents and files that are associated with ServiceDesk processes. The ServiceDesk documents include the files and the screen images that are attached to process tickets and any plans that are created during a process.

See “About Document Management in the ServiceDesk processes” on page 347. Document Management lets you take the following actions:

- Set permissions at both the category level and the individual document level.
- Add documents with or without version information or keywords.
- Add messages to the Documents page to inform a set of users that a document is expected from them by a certain date.
- Add any type of document or file. Documents are not restricted to a set of defined file types.
- Find documents by performing a name search or an advanced keyword search.
- Set up a nested category hierarchy to organize documents and make them easier for users to find.
- Email documents.
- Edit the information data for existing documents.
- Add new versions of documents and display version and document history.
- Download documents in their native file formats or as compressed (.zip) files.
About Document Management in the ServiceDesk processes

Certain of the core ServiceDesk processes contain built-in Document Management functionality. By default, ServiceDesk stores some of the documents that are created in the processes and displays them on the Documents page.

The Knowledge Management process does not integrate with Document Management.

Table 31-1  Default Document Management functionality in ServiceDesk processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Process documents in Document Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Management</td>
<td>File attachments and screen shots</td>
</tr>
<tr>
<td>Change Management</td>
<td>Risk assessments, implementation plans, test plans, backout plans, and any other planning documents</td>
</tr>
<tr>
<td>Problem Management</td>
<td>Documents that you attach as part of the Problem Management process</td>
</tr>
<tr>
<td>Any process ticket</td>
<td>Documents that are attached to a process ticket</td>
</tr>
<tr>
<td></td>
<td>ServiceDesk creates a Process category, adds a subcategory for each process, and adds a subcategory for each process ticket. All the documents that are associated with a specific process ticket are assigned to that ticket’s category.</td>
</tr>
<tr>
<td></td>
<td>The process ticket categories are hidden categories. The Show Hidden Folders check box on the Documents page lets users show or hide the hidden categories.</td>
</tr>
</tbody>
</table>

About document categories

ServiceDesk uses categories to classify its documents. The document categories help the ServiceDesk workers find the documents that they need. You can use additional levels of categories to group the documents further. A document category can have multiple subcategories, and you can nest the subcategories.

ServiceDesk contains a hierarchy of predefined document categories. ServiceDesk also creates subcategories when it adds the documents that are attached to or created within a process. You can add categories and manage the existing ones on the Documents page in the Process Manager portal.

See “Adding a document category” on page 348.
Adding a document category

Document categories help you organize all the documents in ServiceDesk. The document categories help the ServiceDesk workers find the documents that they need.

You can set permissions for the document categories and subcategories. The permissions determine who can access a document category and all the documents that it contains. Permissions also determine who can create categories.

To add a document category

1. In the Process Manager portal, click **Documents**.
2. On the **Category View** page, expand the **Browse** section.
3. At the upper right of the **Browse** section, click the **Add Category** symbol (a file folder with a green plus sign).
4. In the **Add Category** dialog box, on the **Category Information** tab, define the new category, and then click **Save**.

Adding a document subcategory

You can create document subcategories to subdivide the contents of document categories and provide another level of document organization. You can add subcategories to any category.

You can set permissions for the document categories and subcategories. The permissions determine who can access a document category and all the documents that it contains. Permissions also determine who can create subcategories for a specific category.

See “About document categories” on page 347.

See “Setting permissions for a document category” on page 351.
To add a document subcategory

1. In the Process Manager portal, click **Documents**.
2. On the **Documents** page, expand the **Browse** section.
3. Select the category to which you want to add a subcategory.
4. In the right pane, at the far right of the category’s title bar, click the **Edit Folder** symbol (orange lightning), and then click **Add Sub Category**.
5. In the **Add Sub Category** dialog box, on the **Category Information** tab, define the new subcategory, and then click **Save**.

See “Category and Sub Category dialog boxes” on page 349.

Category and Sub Category dialog boxes

These dialog boxes let you add a document category, add a document sub category, or edit any document category. The action that you take in ServiceDesk determines which dialog box appears.

See “Adding a document category” on page 348.
See “Adding a document subcategory” on page 348.
See “Editing a document category” on page 350.

Some of the options differ depending on which dialog box appears.

These dialog boxes contain the following tabs:

- **Category Information**: Lets you define the category.
- **Profiles**: Lets you assign a profile to the category.
- **Advanced**: Displays the category ID for informational purposes only. No user actions are located on this tab. This tab appears in the **Edit Category** dialog box only.

### Table 31-2 Options on the **Category Information** tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the category in any list or display of document categories in the Process Manager portal.</td>
</tr>
<tr>
<td><strong>Header Text</strong></td>
<td>Lets you type additional information to describe the category. The description appears beneath the category title in the right pane of the <strong>Documents</strong> page.</td>
</tr>
</tbody>
</table>
Table 31-2  Options on the Category Information tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Type</td>
<td>Lets you select a document category type. The document category types provide an additional means of grouping and organizing the document categories. You can sort the category display on the Documents page by document category type instead of alphabetically. The use of document category types is optional. They are available only if the administrator added them.</td>
</tr>
<tr>
<td>Hidden</td>
<td>Lets you hide the category from all other users.</td>
</tr>
<tr>
<td>Process Notifications</td>
<td>Sends the email notifications when events occur on the documents that belong to the category. For example, notifications can be sent when a new version of a document is added. The notifications are sent to those who have notify permissions for the item. This option is selected by default.</td>
</tr>
<tr>
<td>Parent Category</td>
<td>(Lets you specify a parent category. This option appears in the Edit Category dialog box only.</td>
</tr>
</tbody>
</table>

Editing a document category

You can edit the existing document categories and document subcategories in ServiceDesk.

See “About document categories” on page 347.

To edit a document category

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the category or subcategory that you want to edit.
4. In the right pane, at the far right of the category’s title bar, click the Edit Folder symbol (orange lightning), and then click Edit.
5. In the Edit Category dialog box, edit the information as needed, and then click Save.

See “Category and Sub Category dialog boxes” on page 349.
Setting permissions for a document category

Document categories help you organize all the documents in ServiceDesk. The document categories help the ServiceDesk workers find the documents that they need.

See “About document categories” on page 347.

An administrator or other user who has the appropriate permissions can set permissions for the document categories and subcategories. The permissions determine who can access a document category and all the documents that it contains. Permissions also determine who can create categories and subcategories.

To set permissions for a document category

1 In the Process Manager portal, click Documents.
2 On the Category View page, expand the Browse section.
3 Select the category.
4 In the right pane, at the far right of the category’s title bar, click the Edit Folder symbol (orange lightning), and then click Permissions.
5 In the Permissions dialog box, add or edit the permissions as needed.
   See “Setting permissions” on page 113.
6 Click Close.

Deleting a document category

An administrator or other user who has the appropriate permissions can delete document categories. The selections that you make during the deletion process determine what happens to the subcategories and the documents that are contained in the document categories.

See “About document categories” on page 347.

To delete a document category

1 In the Process Manager portal, click Documents.
2 On the Category View page, expand the Browse section.
3 Select the category that you want to delete.
4 In the right pane, at the far right of the category’s title bar, click the Edit Folder symbol (orange lightning), and then click Delete.
5 In the **Delete Category** dialog box, under **SubCategories Delete Option**, select one of the following options for handling any subcategories that are contained in the category:

- **Don't delete SubCategories**
  - Retain all the subcategories and move them up to the next-highest level.

- **Delete SubCategories**
  - Delete all the subcategories. Any documents in the subcategory that also belong to another category are retained in the other category. Any documents that do not belong to other categories are moved to the Orphan category.

- **Delete SubCategories and all files in them**
  - Delete all the subcategories and the documents that they contain.

6 In the **Delete Category** dialog box, under **Documents Delete Option**, select one of the following options for handling any documents that are contained in the category:

- **Don't delete documents**
  - Retains all the documents that belong to the category.

- **Delete documents (that are linked only to the deleted category)**
  - Delete all the documents that belong to the category but that do not belong to another category. Any documents that belong to other categories are retained.

- **Delete documents even if linked to multiple categories**
  - Delete all the documents that belong to the category, even if they also belong to categories.

7 Click **Delete**.

**Displaying the history of a document category**

The document category history displays the creation history and change history for a document category.

See “**About document categories**” on page 347.

**To display the history of a document category**

1 In the Process Manager portal, click **Documents**.

2 On the **Category View** page, expand the **Browse** section.
3 Select the category.

4 In the right pane, at the far right of the category’s title bar, click the Edit Folder symbol (orange lightning), and then click History.

Creating expected document messages

You can use expected document messages to remind certain ServiceDesk users to provide a document by a certain date. The messages appear on the Documents page. You can display a message to a user, group, or organizational unit.

See “About document categories” on page 347.

To create an expected document message

1 In the Process Manager portal, click Documents.

2 On the Category View page, under Browse, select the expected document’s category.

3 In the right pane, at the far right of the category’s title bar, click the Edit Folder symbol (orange lightning), and then click Expected Documents.

4 (Optional) In the Expected Documents dialog box, click Add Expected Document.

This option is available if there is at least one existing expected documents item.

5 In the Expected Documents dialog box, define the message and specify its recipients.

See “Expected Documents dialog box” on page 354.

6 In the Select Source drop-down list, select the entity to show the message to: a user, group, permission, or organizational unit.

7 In User, Group, Permission, or Organization, type the name of the entity to display the message to.

You can also click Pick to select the appropriate entity.
8 If you clicked **Pick**, in the **Picker** dialog box, select a specific entity as follows:

- **User Picker** dialog box: Select a user. See “**Picking a user**” on page 114.
- **Group Picker** dialog box: Click the **Select** link to the right of the appropriate group.
- **Permission Picker** dialog box: Click the **Select** link to the right of the appropriate permission.
- **Organization Picker** dialog box: Expand the organizations if necessary, and then select an organization.

9 In the **Expected Documents** dialog box, click **Add Source**.

10 To add more sources, repeat step 6 through step 9.

11 When you finish defining the message and selecting the recipients, click **Save**.

### Expected Documents dialog box

This dialog box lets you define a message to remind certain ServiceDesk users to provide a document by a certain date. This dialog box is available from the **Documents** page.

See “**Creating expected document messages**” on page 353.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Document Name</strong></td>
<td>Lets you provide the name of the document that is expected.</td>
</tr>
<tr>
<td><strong>Group Name</strong></td>
<td>Lets you provide a name for the collected recipients of the message. For example, if you select three users, you can use this name to address them collectively, regardless of any actual groups that they belong to.</td>
</tr>
<tr>
<td><strong>Expected Date</strong></td>
<td>Lets you specify the date on which the document is needed.</td>
</tr>
<tr>
<td><strong>Document Type</strong></td>
<td>Lets you select from a list of document types, which lets the recipient know what type of document is expected.</td>
</tr>
</tbody>
</table>
Table 31-3 Options on the Expected Documents dialog box (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Lets you describe the document that is expected. For example, you can specify the document contents and explain the data that is required.</td>
</tr>
<tr>
<td></td>
<td>The description is included in the message display.</td>
</tr>
<tr>
<td>Select Source</td>
<td>Lets you select the entity to show the message to: a user, group, permission, or organizational unit.</td>
</tr>
<tr>
<td>User</td>
<td>Lets you type or pick the specific entity to display the message to.</td>
</tr>
<tr>
<td>Group</td>
<td></td>
</tr>
<tr>
<td>Permission</td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td></td>
</tr>
<tr>
<td>Add Source</td>
<td>Adds the selected recipient to the message.</td>
</tr>
</tbody>
</table>

Adding a document to the Document Management system

You can add any type of document to the Document Management system in ServiceDesk. The information that you provide when you add the document determines whether the document is considered "simple" or "advanced".

Advanced documents contain version information and search keywords in addition to the standard document information. Simple documents do not contain the version information or search keywords.


To add a document to the Document Management system

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the category to which you want to add a document.
4. In the right pane, at the far right of the category's title bar, click the Edit Folder symbol (orange lightning). Select one of the following options:
   - Add Simple
In the Add Documents or Add Advanced Document dialog box, define the new document, and then click Save.

See “Add Documents dialog box” on page 356.

See “Add Advanced Document dialog box” on page 357.

Add Documents dialog box

This dialog box appears when you add a simple document to the Document Management system. Simple documents do not contain the version information or search keywords.

See “Adding a document to the Document Management system” on page 355.

<table>
<thead>
<tr>
<th>Table 31-4</th>
<th>Options in the Add Documents dialog box</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab</td>
<td>Description</td>
</tr>
<tr>
<td>Documents Information</td>
<td>Lets you specify the location of the document file.</td>
</tr>
<tr>
<td>Optional</td>
<td>Lets you apply attributes to the document to make it easier to identify.</td>
</tr>
<tr>
<td>Expected Documents</td>
<td>Lets you indicate that the new document represents a response to an expected document request. This tab appears only if at least one expected document exists.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Lets you apply a profile value to the document.</td>
</tr>
<tr>
<td>Tags</td>
<td>Lets you tag the document. Tags provide another way to search for documents.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 31-5</th>
<th>Options on the Optional tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>Document Type</td>
<td>Lets you identify the document format or type. The ServiceDesk administrator creates the types that appear in the list. However, you can add any type of document to the Document Management system even if it is not listed.</td>
</tr>
</tbody>
</table>
Table 31-5  Options on the Optional tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Override Name   | Identifies this document in any list of documents in the Process Manager portal. Make the name descriptive enough for you and others to easily understand the purpose of the document.  
If you do not provide a name, the document’s file name is used. |
| Description     | Appears beneath the document name in any list or display of documents in the Process Manager portal. The description helps the users decide whether to view the document. |

Table 31-6  Options on the Expected Documents tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Expected Document      | Lets you select the expected document that the new document represents.  
When the new document is saved and added, the associated expected document message is removed. |
| Document Name          | Lets you name the new document. The options are as follows:  
- Missing document name  
- Uploaded document name  
- User specified name |

Add Advanced Document dialog box

This dialog box appears when you add an advanced document to the Document Management system. Advanced documents contain version information and search keywords in addition to the standard document information.

See “Adding a document to the Document Management system” on page 355.

Table 31-7  Tabs in the Advanced Document dialog box

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Information</td>
<td>Defines the document.</td>
</tr>
<tr>
<td>Versions to Keep</td>
<td>Determines the number of versions of the document to keep.</td>
</tr>
<tr>
<td>Version Information</td>
<td>Specifies the document’s version.</td>
</tr>
</tbody>
</table>
Table 31-7  Tabs in the **Advanced Document** dialog box *(continued)*

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
</table>
| Expected Documents | Lets you indicate that the new document represents a response to an expected document request.  
This tab appears only if at least one expected document exists. |
| Profiles           | (Optional) Lets you apply a profile value to the document.                    |

Table 31-8  Options on the **Document Information** tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Lets you specify the location of the document file.</td>
</tr>
</tbody>
</table>
| Name        | Identifies this document in any list of documents in the Process Manager portal. Make the name descriptive enough for you and others to easily understand the purpose of the document.  
If you do not provide a name, the document’s file name is used. |
| Category    | (Read only) Displays the category to which this document belongs.            |
| Document Type| Lets you identify the document format or type. The ServiceDesk administrator creates the types that appear in the list. However, you can add any type of document to the Document Management system even if it is not listed. |
| Description | Appears beneath the document name in any list or display of documents in the Process Manager portal. The description helps the users decide whether to view the document. |
| Keywords    | (Optional) Lets you associate keywords with the document. The keywords appear during a document search.  
When you type multiple keywords, separate them with a comma. |

Table 31-9  Options on the **Versions to Keep** tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Major Minor</td>
<td>Lets you specify the number of each version type that ServiceDesk keeps. Any versions beyond the specified numbers are removed.</td>
</tr>
<tr>
<td>Keep major versions of prior release versions</td>
<td>Lets you specify whether to keep major versions of previous release versions.</td>
</tr>
</tbody>
</table>
### Table 31-9 Options on the Versions to Keep tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep minor versions of prior major versions</td>
<td>Lets you specify whether to keep minor versions of previous major versions.</td>
</tr>
</tbody>
</table>

### Table 31-10 Options on the Version Information tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release version</td>
<td>Lets you define the document's version. The numbers of the different version levels are combined when the version number is displayed.</td>
</tr>
<tr>
<td>Major version</td>
<td>For example, in the version number 2.1.0, the release version is 2, the major version is 1, and the minor version is 0.</td>
</tr>
<tr>
<td>Minor version</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>(Optional) Lets you type additional information to display with the document.</td>
</tr>
</tbody>
</table>

### Table 31-11 Options on the Expected Documents tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Document</td>
<td>Lets you select the expected document that the new document represents.</td>
</tr>
<tr>
<td></td>
<td>When the new document is saved and added, the associated expected document message is removed.</td>
</tr>
<tr>
<td>Document Name</td>
<td>Lets you name the new document. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>▪ Missing document name</td>
</tr>
<tr>
<td></td>
<td>▪ Uploaded document name</td>
</tr>
<tr>
<td></td>
<td>▪ User specified name</td>
</tr>
</tbody>
</table>

### Setting permissions for a document

An administrator or other user who has the appropriate permissions can set permissions for a document in ServiceDesk. The permissions determine who can access and use a document. For example, you can specify which users or groups can view, edit, delete, or email a document.

To set permissions for a document
1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the document’s category.
   If you cannot find the document, you can perform a search.
5. In the right pane, to the far right of the document name, click the Edit Document symbol (orange lightning), and then click Edit > Permissions.
6. In the Permissions List dialog box, add or edit permissions as needed.
   See “Setting permissions” on page 113.
7. Click Close.

Editing document data

You can edit a document’s descriptive information, versions, and profiles.
You cannot edit the document itself from the Process Manager portal. However, you can import a new version of the document and associate it with the existing document.

See “Adding a new document version” on page 360.

To edit document data
1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the document’s category.
   If you cannot find the document, you can perform a search.
   See “Searching for documents” on page 367.
4. In the right pane, to the far right of the document name, click the Edit Document symbol (orange lightning), and then click Edit > Document Data.
5. In the Document Data dialog box, edit the data as needed, and then click Save.

Adding a new document version

You can update a document by importing a new version of the file. You specify the updated document and then specify whether the document represents a new
release, major version, or minor version. When the document is added, the version number is incremented.

**To add a new document version**

1. In the Process Manager portal, click **Documents**.
2. On the **Category View** page, expand the **Browse** section.
3. Select the document’s category.

   If you cannot find the document, you can perform a search.

   See “**Searching for documents**” on page 367.

4. In the right pane, to the far right of the document name, click the **Edit Document** symbol (orange lightning), and then click **Edit > Add New Version**.

5. In the **Document Versions** dialog box, click the **Add New Version** tab.

6. On the **Add New Version** tab, provide the following information:

   - **Version Type**: In the drop-down list, select the version type that the document represents, as follows:
     - Minor
     - Release
     - Major
   - **Notes**: Provide additional information about the nature of the new version.
   - **File**: Specify the location of the updated document file.

7. Click **Add**.

---

**Promoting a document version**

You can promote a document’s most recent version to the next version level. Promoting the version means incrementing the number of the next-highest version type. For example, if the original version of a document is 2.0.0 and you add a minor version, the new version number is 2.0.1. If you promote the version, the new version number becomes 2.1.0.

**To promote a document version**

1. In the Process Manager portal, click **Documents**.
2. On the **Category View** page, expand the **Browse** section.
Adding a document to additional categories

When a document is first added to the Document Management system, it is assigned to a single category. You can assign a document to any number of additional categories.

To add documents to additional categories

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the document’s category.
   If you cannot find the document, you can perform a search.
   See “Searching for documents” on page 367.
4. In the right pane, to the far right of the document name, click the Edit Document symbol (orange lightning), and then click Edit > Add to Category.
5. In the Add to Category dialog box, click the Add New Category tab.
6. In Category, type the name of the category to add the document to or click Pick to select from a list of categories.
7. Click Add.
8. Under Category List, confirm that the document has been added to the selected category.
9. Close the dialog box.
Deleting a document

You can delete a document that is obsolete or no longer useful.

To delete a document

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the document’s category.
   - If you cannot find the document, you can perform a search.
   - See “Searching for documents” on page 367.
4. In the right pane, to the far right of the document name, click the Edit Document symbol (orange lightning), and then click Delete.
5. In the confirmation dialog box, click OK.
Deleting a document
Viewing documents

This chapter includes the following topics:

- What you can do with ServiceDesk documents
- Searching for documents
- Previewing documents
- Viewing a document
- Downloading a document
- Downloading a document in .zip format
- Emailing a document
- Viewing a document’s versions
- Viewing a document’s history

What you can do with ServiceDesk documents

When you open and view a document, you might have additional options for interacting with it.

All of the options are available on the drop-down list that appears when you click the Actions symbol (orange lightning) for a document.

Your permissions determine the options that are available to you. For example, typical actions are to download a document, view its history, or send it by email.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New Version</td>
<td>Lets you update a document by importing a new version of the file and choosing how to increment the version number.</td>
</tr>
<tr>
<td></td>
<td>See “Adding a new document version” on page 360.</td>
</tr>
<tr>
<td>Add to Category</td>
<td>Lets you assign a document to other categories in addition to its original category.</td>
</tr>
<tr>
<td></td>
<td>See “Adding a document to additional categories” on page 362.</td>
</tr>
<tr>
<td>Delete</td>
<td>Lets you delete a document that is obsolete or no longer useful.</td>
</tr>
<tr>
<td></td>
<td>See “Deleting a document” on page 363.</td>
</tr>
<tr>
<td>Document Data</td>
<td>Lets you edit a document’s descriptive information, versions, and profiles.</td>
</tr>
<tr>
<td></td>
<td>See “Editing document data” on page 360.</td>
</tr>
<tr>
<td>Download</td>
<td>Lets you download a document.</td>
</tr>
<tr>
<td></td>
<td>See “Downloading a document” on page 369.</td>
</tr>
<tr>
<td>Download Zip</td>
<td>Lets you download a document as a compressed file.</td>
</tr>
<tr>
<td></td>
<td>See “Downloading a document in .zip format” on page 369.</td>
</tr>
<tr>
<td>Edit</td>
<td>Lets you select the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Document Data</td>
</tr>
<tr>
<td></td>
<td>■ Add New Version</td>
</tr>
<tr>
<td></td>
<td>■ Promote Document Version</td>
</tr>
<tr>
<td></td>
<td>■ Permissions</td>
</tr>
<tr>
<td></td>
<td>■ Add to Category</td>
</tr>
<tr>
<td>History</td>
<td>Lets you view the history of a document’s creation and updates in the Document Management system.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing a document’s history” on page 371.</td>
</tr>
<tr>
<td>Open Document</td>
<td>Lets you open a document so that you can view its contents.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing a document” on page 368.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Lets you set permissions for other users to access a document.</td>
</tr>
<tr>
<td></td>
<td>See “Setting permissions for a document” on page 359.</td>
</tr>
<tr>
<td>Promote Document Version</td>
<td>Lets you promote a document’s most recent version to the next version level, which increments the number of the next-highest version type.</td>
</tr>
<tr>
<td></td>
<td>See “Promoting a document version” on page 361.</td>
</tr>
</tbody>
</table>
### Table 32-1  Options for working with a document (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send</strong></td>
<td>Lets you attach a document to an email message or provide a link for the email recipient to download the document.</td>
</tr>
<tr>
<td></td>
<td>See “Emailing a document” on page 369.</td>
</tr>
<tr>
<td><strong>Show Versions</strong></td>
<td>Lets you view or download any existing version of a document.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing a document’s versions” on page 370.</td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Lets you select the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Open Document</td>
</tr>
<tr>
<td></td>
<td>■ Show Versions</td>
</tr>
<tr>
<td></td>
<td>■ History</td>
</tr>
</tbody>
</table>

### Searching for documents

You can search for documents on the **Documents** page.

The document searches are performed as follows:

- You can search on the document name or on keywords. Only the documents that have keywords (advanced documents) are included in a keyword search.
- The search evaluates the documents in all the document categories.
- Your permissions determine the categories and documents that you can access, which in turn influences the results of your searches.

You can preview the search results to decide whether to open it.

See “**Previewing documents**” on page 368.

When you find a document, you can open and view it or perform other actions.

See “**What you can do with ServiceDesk documents**” on page 365.

**To search for documents**

1. In the Process Manager portal, click **Documents**.
2. On the **Category View** page, under **Search Document**, type the text to search for, and then click the **Search** symbol (magnifying glass).
Previewing documents

The document viewer lets you quickly scan the documents in a category so you can decide whether to view or download them. The document viewer opens in a new window and lists the documents in the left pane. When you select a document, a preview of the document appears in the right pane.

The document viewer can display Microsoft Office documents and image files.

To preview documents

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the category.
   If you cannot find the document, you can perform a search.
   See “Searching for documents” on page 367.
4. In the right pane, at the far right of the category’s title bar, click the Edit Folder symbol (orange lightning), and then click Document Viewer.
5. When you finish previewing the documents, close the document viewer page.

Viewing a document

You can open a document from the Documents page to view it in a new window.

See “What you can do with ServiceDesk documents” on page 365.

To view a document

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the document’s category.
   If you cannot find the document, you can perform a search.
   See “Searching for documents” on page 367.
4. In the right pane, to the far right of the document name, click the Edit Document symbol (orange lightning), and then click View > Open Document.
5. When you finish viewing the document, you can close the document page.
Downloading a document

You can download a document so that you can use it outside of the Process Manager portal.

To download a document

1. In the Process Manager portal, click **Documents**.
2. On the **Category View** page, expand the **Browse** section.
3. Select the document’s category.
   - If you cannot find the document, you can perform a search.
   - See “Searching for documents” on page 367.
4. In the right pane, to the far right of the document name, click the **Download** symbol (blue diskette).
5. In your browser's download dialog box, click **Open** or **Save** and follow the prompts.

Downloading a document in .zip format

You can download a document as a compressed (.zip) file so that you can use it outside of the Process Manager portal. Compressing the file reduces the download time.

To download a document in .zip format

1. In the Process Manager portal, click **Documents**.
2. On the **Category View** page, expand the **Browse** section.
3. Select the document’s category.
   - If you cannot find the document, you can perform a search.
   - See “Searching for documents” on page 367.
4. In the right pane, to the far right of the document name, click the **Edit Document** symbol (orange lightning), and then click **Download Zip**.
5. In your browser's download dialog box, click **Open** or **Save** and follow the prompts.

Emailing a document

You can email a document by attaching it to an email message or by adding a link to the document’s location.
To email a document

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the document’s category.
   If you cannot find the document, you can perform a search.
   See “Searching for documents” on page 367.
4. In the right pane, to the far right of the document name, click the Edit Document symbol (orange lightning), and then click Send.
5. In the Send Document dialog box, type the following information:
   - Send To
   - CC
   - Subject
   - Message
6. In the Send Method drop-down list, select one of the following options:
   - Send as attachment: Attach the document to the email message.
   - Send download link: Add a link to the body of the email for downloading the document.
7. Click Send Document.

Viewing a document’s versions

You can view all of the available versions of a document. You can also download any of the available versions.

To view document version and history

1. In the Process Manager portal, click Documents.
2. On the Category View page, expand the Browse section.
3. Select the document’s category.
   If you cannot find the document, you can perform a search.
   See “Searching for documents” on page 367.
4 In the right pane, to the far right of the document name, click the **Edit Document** symbol (orange lightning), and then click **View > Show Versions**.

5 In the **Document Versions** dialog box, you can take the following actions for any of the displayed versions:
   - Download the document as a compressed (.zip) file.
   - Download the document.

### Viewing a document’s history

You can view the history of a document in the Document Management system. The document history consists of the following information:

- Actions
- Action by user
- Date and Time
- Version
- Notes

**To view a document’s history**

1 In the Process Manager portal, click **Documents**.
2 On the **Category View** page, expand the **Browse** section.
3 Select the document’s category.
   - If you cannot find the document, you can perform a search.
     - See “**Searching for documents**” on page 367.
4 In the right pane, to the far right of the document name, click the **Edit Document** symbol (orange lightning), and then click **View > History**.
5 When you finish viewing the history, in the **Documents History** dialog box, click **Cancel**.
Viewing a document's history
Communicating in the Process Manager portal

- Chapter 33. Emailing in the Process Manager portal
- Chapter 34. Holding discussions in the Process Manager portal
Emailing in the Process Manager portal

This chapter includes the following topics:

- Sending an email from a ticket's Process View page
- About automatic email notifications
- About process notifications

Sending an email from a ticket's Process View page

When working an incident or a change request ticket, you can send an email to users or groups about the ticket from the Process View page. The email is created from an email template that you select. You can also edit the email message.

Note: The Send Email process type action only appears on the ticket’s Process View page if you have created email templates for the process.

See “Creating email templates for Incident Management” on page 195.
See “Creating email templates for Change Management” on page 234.

To send an email from a ticket's Process View page

1. In the Process Manager portal, click My Task List.
2. On the My Task List page, under Task Viewer, under Project Name, open an existing incident or change request ticket.
3 On the ticket’s **Process View** page, under **Process Actions**, click **Send Email**.

Note that the **Send Email** process type action only appears if you have created email templates for the process.

4 In the **Send Email Notification** dialog box, in the **Select Template** drop-down list, select an email template to use.

The templates that appear in the list are associated with the specific ticket type. For example, if you send an email from a change ticket, the templates that you can select are change-related templates.

5 In the **Recipient** field, type the email address of the user or group to which you want to send the email and click **Add Recipient**.

6 (Optional) Use the **Pick** option to search for and select a user or group by taking any of the following actions:

   - In the **Add Recipient** drop-down list select **User** and then click **Pick**.
   - In the dialog box, type your search parameters in the appropriate field(s).
     For example, if you know the recipient’s first name, type the name in the **First Name** field.
     - Click **Search**.
     - To the right of the recipient to whom you want to send the email, click **Select**.
     - In the **Send Email Notification** dialog box, to the right of the recipient’s name, click **Add Recipient**.

   See “Picking a user” on page 114.

   - In the **Add Recipient** drop-down list select **Group** and then click **Pick**.
   - In the dialog box, in the **Group Name** field, type your search parameters.
     - Click **Search**.
     - To the right of the group to which you want to send the email, click **Select**.
     - In the **Send Email Notification** dialog box, to the right of the group’s name, click **Add Recipient**.

7 (Optional) Edit the contents, subject and from fields, if necessary.

8 (Optional) Add a process attachment.

These attachments are part of an incident or a change request ticket’s history. A link to these attachments appears in the **Attachment** section of the ticket. For an attachment to be a process attachment, you must first add it to the
ticket’s Attachment section. Your attachment then appears in the Add Process Attachment drop-down list.

To add a process attachment:

- In the Add Process Attachment drop-down list, select an attachment.
- Click Add Attachment.
- Your attachment appears in the Attachment field.

9 (Optional) Add an attachment.

These attachments are not part of an incident or a change request ticket’s history. The Attachment section of the ticket does not contain a link to this attachment.

To add an attachment:

- To the right of Attachment, click Browse.
- Select your attachment.
- Click Add Attachment.
- Your attachment appears in the Attachment field.

10 When you are finished, click Send.

11 In the Email Sent confirmation dialog box, click OK.

12 When the ticket’s Process View page reappears, you can continue to work the ticket or close it.

About automatic email notifications

ServiceDesk can send email notifications at various stages of a process, based on one or more events that occur within the process. The type of event determines the contents and the recipients of the email notifications.

ServiceDesk contains default notifications for the following core processes:

- Problem Management
  
  See “Email notifications from Problem Management” on page 267.

- Knowledge Management
  
  See “Email notifications from Knowledge Management” on page 311.

The default notifications are ready to use. However, you can customize the email notifications by editing the appropriate project in Workflow Designer. For example, you can change the event that triggers a notification or create a notification for a new event.
For more information about editing the email notifications, see the Symantec™ Workflow 7.5 User Guide.

You can also change the default contents of the automatic email notifications. See “About the contents of email notifications” on page 512.

These automatic email notifications are different from the process notifications that result from the events that occur on specific items within the Process Manager portal. For example, the process notifications can be sent when a document or a knowledge base entry is added, edited, or deleted. See “About process notifications” on page 378.

Email notifications for Incident Management and Change Management are handled through the Automation Rules. For these processes, you must create email templates and then create rules for sending them.

See “Creating email templates for Incident Management” on page 195.
See “Configuring new automation rules for Incident Management” on page 214.
See “Creating email templates for Change Management” on page 234.
See “Configuring change request rulesets” on page 232.

### About process notifications

ServiceDesk can send email notifications as a result of events that occur within the Process Manager portal. These notifications are known as process notifications.

For example, notifications can be sent for the events that can occur on documents, discussions, and knowledge base entries. Examples of events are when an item is added, edited, deleted, or accessed.

Process notifications are sent based on the following settings:

- **The item's permissions**
  - When you create or edit an item that has process notification capability, it includes notification permissions for the events that can occur on the item.
  - You can set the permissions on the Permissions tab that appears when you create or edit the item.

- **The Process Notification option**
  - When you create or edit an item that has process notification capability, this option appears in the editing dialog box. It typically appears on the Notifications tab.
  - This option is selected by default.
The process notifications are different from the automatic email notifications that ServiceDesk can send at various stages of a core process.

See “About automatic email notifications” on page 377.
Emailing in the Process Manager portal

About process notifications
Holding discussions in the Process Manager portal

This chapter includes the following topics:

- About discussions in the Process Manager portal
- Adding a discussion in the Process Manager portal
- Adding a thread to a discussion
- Participating in a discussion in the Process Manager portal

About discussions in the Process Manager portal

You can participate in discussions with other users within the Process Manager portal. Use the discussion feature to communicate with others in an open forum environment. Users can post comments and messages to offer insight or answer questions.

Discussions can be created from the Discussions page in the Process Manager portal. For example, a support technician can start a discussion thread about an incident to get information and feedback on resolving the incident from other technicians.

See “Adding a discussion in the Process Manager portal” on page 382.

See “Discussions page” on page 58.

Discussions can also be created from a problem ticket. When a user creates a new problem ticket, a new discussion is created. The name and description of the problem ticket become the title and description of the new discussion. The problem ticket’s process ID is added to the discussion title. Problem workers can access
the discussion from the problem ticket’s Process View page. A problem-related discussion can be a valuable tool for finding a resolution to the problem.

See “Reporting a problem” on page 270.

A discussion is displayed as a hierarchy of information, as follows:

- **Discussion**: The highest level in the hierarchy. Typically, a discussion encompasses a single subject or problem.

- **Thread**: A subtopic of a discussion. You can use threads to better organize the Discussions page.

- **Post**: A subtopic of a thread or of another post. You can create a new post for a thread, or you can reply to an existing post. Replies become the children of the original post. A single post can have multiple layers of replies.

Permissions can be set at the discussion level. The permissions determine who can create, edit, view, and participate in a discussion.

The participants in a discussion can rate the discussion’s posts. The participant ratings are accumulated and displayed on the Discussions page.

The discussion ratings are as follows:

- Poor(1)
- Average(2)
- Good(3)
- Very Good(4)
- Excellent(5)

**Adding a discussion in the Process Manager portal**

A discussion is the highest level in the discussion hierarchy. You can create a discussion in the Process Manager portal.

Typically, a discussion encompasses a single subject or problem.

Discussions can also be added through the Product Management process.

See “About discussions in the Problem Management process” on page 269.
To add a discussion

1. In the Process Manager portal, click Knowledge Base > Discussions.

2. On the Discussions page, click the Add Discussion symbol (a white page with a green plus sign).

3. On the Add Discussions dialog box, click the Edit Discussion Info tab and provide a title and a description for the discussion.
   This information identifies the discussion on the Discussions page.

4. (Optional) To enable email notifications of the events that occur on this discussion, click the Notifications tab, and then verify that Process Notifications is selected.
   See “About process notifications” on page 378.

5. In the Add Discussions dialog box, click the Permissions tab, and then specify the permissions for one or more users, groups, permissions, or organizational units.
   See “Setting permissions” on page 113.

6. When you finish defining the discussion, on the Add Discussions page, click Save.

Adding a thread to a discussion

A thread is a subtopic of a discussion. You can use threads to better organize the Discussions page.

See “About discussions in the Process Manager portal” on page 381.

Users cannot post messages at the discussion level. Instead, they can post to threads.

See “Participating in a discussion in the Process Manager portal” on page 384.

To add a thread to a discussion

1. In the Process Manager portal, click Knowledge Base > Discussions.

2. If the discussion does not appear in the list, in Search, type the text to search for, and then click the Search symbol (magnifying glass).

3. At the right of the discussion’s header bar, click the Add Thread symbol (a white page with a green plus sign).

4. In the Add Thread dialog box, on the Thread Information tab, type the title and the body text for the thread.
5  (Optional) In the Add Thread dialog box, on the Thread Description tab, type a description to further identify the thread.

6  When you finish defining the thread, click Save.

## Participating in a discussion in the Process Manager portal

You can participate in discussions with other users within the Process Manager portal. Use the discussion feature to communicate with others in an open forum environment.

When you participate in a discussion, you can add threads, add posts, and reply to existing posts. Your ServiceDesk permissions determine which discussions you can edit, view, and participate in.

See “About discussions in the Process Manager portal” on page 381.

### To participate in a discussion in the Process Manager portal

1  In the Process Manager portal, access the discussion in any of the following ways:

   From the portal  Click Knowledge Base > Discussions.

   If the discussion does not appear in the list, in Search, type the text to search for, and then click the Search symbol.

   From a problem ticket  On the problem ticket’s Process View page, under Assignments, expand Smart Tasks and then click Go to Discussion.

2  Expand the discussion section to view the posting history.

3  If a series of five stars appears under the post’s text, you can rate the post. To the right of How helpful was this?, select one of the stars.

   The first star is the lowest rating, and the last star is the highest rating.

   The stars do not appear for the posts that you created.
4 If you plan to post any information that is not related to the discussion’s existing threads, create a new thread.

See “Adding a thread to a discussion” on page 383.

5 You can add to the existing discussion in the following ways:

Post to a thread. At the right of the thread’s title bar, click the Add Post symbol (a white page with a green plus sign).

In the Add Post dialog box, type and post the message text.

Reply to a post. At the right of the post’s title bar, click the Reply symbol (a white text balloon).

In the Reply dialog box, type and save a reply to the selected post.
Holding discussions in the Process Manager portal

Participating in a discussion in the Process Manager portal
Managing reports

- Chapter 35. Viewing and organizing reports
- Chapter 36. Creating and customizing standard reports
- Chapter 37. Scheduling reports
Viewing and organizing reports

This chapter includes the following topics:

- About ServiceDesk reporting
- Viewing a report
- What you can do with a report
- Displaying reports in print view
- Setting permissions for a report
- Optimizing reports in the Process Manager portal
- Copying a report
- Exporting a report definition
- Importing reports
- Adding reports to a portal page
- Deleting reports
- About report categories
- Adding report categories
- Adding report subcategories
- Deleting report categories
- Setting permissions for a report category
About ServiceDesk reporting

ServiceDesk includes a large number of predefined reports that provide easy access to the ServiceDesk data. The predefined reports meet the ITIL need of many organizations. However, reports can be customized and new reports can be created to meet your organization’s specific requirements.

You can customize the ServiceDesk reports in the following ways:

- You can copy a report and edit the copy to quickly create a new report.
- You can use a wizard interface to create new reports, which eliminates the need to use SQL for report creation.
- You can add a report to any ServiceDesk portal page or dashboard, and you can define the size and placement of the report.
- During report creation, you can add run-time filters to the report definition. Run-time filters let users scope the reports based on the data that they want to see.

You can view and customize reports on the Reports page.

See “Reports page” on page 65.

Viewing a report

You can view reports in the Process Manager portal on the Reports page or on any portal page that includes reports. For example, the My Task List page and the Tickets pages include reports.

Your permissions determine the reports that you can view.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

To view a report on the Reports page

1. In the Process Manager portal, click Reports.
2. On the Reports page, under Report Categories, select the category that contains the report to view.
3 Expand the **Reports** section and do one of the following actions to view a report:

- Click the name of a report.
- To the right of the report name, click the **Actions** symbol (orange lightning) and the click **View**.

4 (Optional) To take action on the report, click the **Actions** symbol (orange lightning), and then select the appropriate option.

See “**What you can do with a report**” on page 391.

### What you can do with a report

When you view a report in ServiceDesk, you might have additional options for interacting with that report.

See “**Viewing a report**” on page 390.

All the options are available on the drop-down list that appears when you click the **Actions** symbol (orange lightning) on the **Reports** page.

Your permissions determine the options that are available to you. For example, typical actions are to print the report or export it.

#### Table 35-1 Options for working with reports

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Child Report</td>
<td>Lets you create a child report.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>About child reports</strong>” on page 402.</td>
</tr>
<tr>
<td>Categories</td>
<td>Lets you view the categories that the report belongs to and add the report to additional categories.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Adding reports to additional categories</strong>” on page 401.</td>
</tr>
<tr>
<td>Copy</td>
<td>Lets you make a copy of the report so that you can create a new report based on the current report. You can customize the copy of the report without having to recreate the report settings.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Copying a report</strong>” on page 395.</td>
</tr>
<tr>
<td>Delete</td>
<td>Lets you delete the report.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Deleting reports</strong>” on page 398.</td>
</tr>
<tr>
<td>Edit</td>
<td>Lets you edit the report.</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Modifying standard reports</strong>” on page 411.</td>
</tr>
</tbody>
</table>
Table 35-1 Options for working with reports (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Report</td>
<td>Lets you export the report definition to an XML schema file, which lets you or another user run the report from another ServiceDesk instance.</td>
</tr>
<tr>
<td></td>
<td>See “Exporting a report definition” on page 396.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Lets you set the permissions for the report.</td>
</tr>
<tr>
<td></td>
<td>See “Setting permissions for a report” on page 392.</td>
</tr>
<tr>
<td>Print View</td>
<td>Displays the report in Print View, which shows you how the report appears when it is printed.</td>
</tr>
<tr>
<td></td>
<td>See “Displaying reports in print view” on page 392.</td>
</tr>
<tr>
<td>Schedules</td>
<td>Lets you view the reports that contain the report or create a new schedule for the report.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a report schedule” on page 414.</td>
</tr>
<tr>
<td>View</td>
<td>Opens the report.</td>
</tr>
</tbody>
</table>

Displaying reports in print view

You can display any report in Print View, which shows you how the report appears when it is printed.

To display a report in print view

1. In the ServiceDesk portal, click Reports.
2. On the Reports page, under Report Categories, select the category that contains the report.
3. Under Reports, at the far right of the report name, click the Actions symbol (orange lightning), and then click Print View.

Setting permissions for a report

An administrator or other user who has the appropriate permissions can set permissions for a report. The report permissions control the access to and use of that report. For example, you can specify which users or groups can view, edit, delete, or create subreports for a report.
To set permissions for a report

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Permissions**.
4. In the **Report Permissions** dialog box, add or edit permissions as needed.
   See “Setting permissions” on page 113.
5. When you finish setting permissions, click **Close**.

**Optimizing reports in the Process Manager portal**

The Process Manager portal lets you view reports. You can view reports on the **Reports** page or you can include reports as part of a portal page. For example, the **Technician Dashboard** page contains several default reports.

When you open a report on the **Reports** page, all associated report data must be run and complied before the report can be rendered. When you navigate to or refresh a page in the Process Manager portal that contains one or more reports, all associated report data must be run and complied before the page can be rendered.

The more records that a report returns and displays the greater the effect that report has on the performance of the Process Manager. Reports increase the load time of a portal page and may even cause the page to time out.

The following are some ways that you can optimize the performance of your reports and lessen their effect on the performance of the Process Manager:

- **Optimize the reports on the Process Manager portal pages.**
  These steps let you optimize the performance of any Process Manager portal page that contains reports.
  **To optimize a report on a Process Manager portal page**

- **Optimize the reports for viewing them on the **Reports** page.**
  These steps let you optimize a report before you view it.
  **To optimize a report for viewing on the Reports page**

**To optimize a report on a Process Manager portal page**

1. In the Process Manager portal, open a portal page that contains a report.
2. In the **Site Actions** drop-down list, select **Modify Page**.
3 In the title bar of the section displaying the report, click the Actions symbol (orange lightening) and then click Edit.

4 In the Editor Zone, do the following:

- **Records to show**: Type the number of records that you want the report to return.
  
  For example, if you have a report that contains 1,000 records, you can choose to show only 250 of those records.

- **Use Paging**: Check Use Paging.
  
  This selection is the key to optimizing your report. This selection lets you paginate the report.
  
  The report displays the number of pages at the bottom of the page.

- **Rows per page**: Type the number of rows that you want the report to display on each page.

5 Scroll to the bottom of the page and click OK.

6 (Optional) Remove the Groups By selection:

- The Group By selection overrides the Use Paging option. If you want to use the Use Paging option, you must remove the Group By selection. After you remove the Group By selection, you may want to reorganize the report.

  ■ In the Process Manager portal, open the Reports page.

  ■ Select the report from which you want to remove the Groups By selection.

  ■ On the selected reports page to the right of the report, click the Actions symbol (orange lightening) and then click Edit Report.

  ■ In the report builder on the Report Designer tab, click Options.

  ■ In the Options section in the Group By drop-down list, select the option that leaves the field empty.

  ■ Click Save.

**To optimize a report for viewing on the Reports page**

1 In the Process Manager portal, open the Reports page.

2 Select the report that you want to view, and to the right of the report, click the Action symbol (orange lightening) and then click Edit.

3 On the selected report's page to the right of the report, click the Actions symbol (orange lightening) and then click Edit Report.
4 In the report builder on the Report Designer tab, click Options.

5 In the Options section, do the following:

**Limit Rows**
- Check Limit Rows.
- Type the number of records that you want the report to return.
  For example, if you have a report that contains 1,000 records, you can choose to show only 250 of those records.

**Use Paging**
- Check Use Paging.
  This selection is the key to optimizing your report. This selection lets you paginate the report.
  The report displays the number of pages at the bottom of the page.
- Type the number of rows that you want the report to display on each page.

6 (Optional) In the Group By drop-down list, select the option that leaves the field empty.

   The Group By selection overrides the Use Paging option. If you want to use the Use Paging option, you must remove the Group By selection.

   After you remove the Group By selection, you may want to reorganize the report.

7 Click Save.

See “Customizing a Process Manager portal page list” on page 88.

See “Changing the report for a Process Manager portal page list” on page 91.

See “Viewing a report” on page 390.

See “Adding reports to a portal page” on page 397.

See “Creating a standard report” on page 403.

See “Customizing the filtering and sorting for standard reports” on page 406.

See “Modifying standard reports” on page 411.

**Copying a report**

Copying an existing report lets you create a new report that is customized to your needs, without having to recreate the report settings. You can copy a report that has almost all of the information you need, and then add, remove, and edit the
To copy a report

1. In the ServiceDesk portal, select **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Copy**.
4. In the **Report Information** dialog, enter a new name for the report in the **Report Name** field.
5. Optionally, enter a description for the report in the **Report Description** field. The description text you enter appears under the report name on the **Reports** tab, when you expand a report entry.
6. Click **Save**.

Exporting a report definition

Any report definition can be exported to an XML schema file. When you export a report definition, the report settings are exported so that the report can be run from another ServiceDesk system. The actual report data is not exported when you use the export report feature. You have the option of saving or viewing the XML file. Any user that has access to view a report has permission to export it.

To export a report

1. In the ServiceDesk portal, select **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Export Report**.
4. In the **File Download** dialog box, click either of the following options:
   - **Open** Opens the XML file for viewing.
   - **Save** Saves the file on your computer.
Importing reports

You can import reports from another instance of ServiceDesk.

To import reports
1. In the ServiceDesk portal, click Reports.
2. On the Reports page, under Report Categories, select the category to import reports to.
3. Under Reports, at the far right of the report name, click the Actions symbol (orange lightning), and then click Import Reports.
4. In the Import dialog box, click Browse and select the report file that you want to import.
5. Select one of the following options to determine whether ServiceDesk overwrites or copies existing reports:
   - Overwrite existing reports - ServiceDesk overwrites reports with the same report ID.
   - Create new copy - ServiceDesk creates new copies of all the reports.
6. Click Import.

Adding reports to a portal page

Any ServiceDesk reports can be added to a portal page. Administrators and users with the appropriate permissions to modify portal pages can add reports.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

To add a report to a portal page
1. In the ServiceDesk portal, select the portal page you want to add the report to.
2. Select Site Actions > Modify Page.
3. Select Site Actions > Add Web Part.
4. Select Reports in the Catalog List.
5. Select the Standard Report Viewer check box to add a standard report.
6. In Add to, select the zone to add the report to.
7. Click Add. The Report Viewer web part is added to the portal page.
8 Click Close.

9 Click the Report Selection icon and select the report that you want to display in the Report Viewer web part.

Deleting reports

You can delete any report that you have delete permissions for from the Reports tab.

To delete a report

1 In the ServiceDesk portal, click Reports.

2 On the Reports page, under Report Categories, select the category that contains the report.

3 Under Reports, at the far right of the report name, click the Actions symbol (orange lightning), and then click Delete.

4 Click OK in the confirmation dialog box.

About report categories

ServiceDesk uses categories to classify its reports. The report categories help the ServiceDesk workers find the reports that they need. You can use additional levels of categories to group the reports further. A report category can have multiple subcategories, and you can nest the subcategories.

ServiceDesk contains a hierarchy of predefined report categories, which organize the default ServiceDesk reports. You can add categories and manage the existing ones on the Reports page in the ServiceDesk portal.

See “Adding report categories” on page 398.

You can set permissions for the report categories and subcategories. The permissions determine who can access a report category and all the reports that it contains.

See “Setting permissions for a report category” on page 400.

Adding report categories

Report categories assist you in organizing all of the reports that are located on the Reports page. Organizing the reports in categories helps users find the reports they need more easily. You can also apply permissions to categories, which deny or grant access to that category and all the reports within it.
See “Setting permissions for a report category” on page 400.

**To add a report category**

1. In the ServiceDesk portal, click **Reports**.
3. In the **Category Information** dialog box, in the **Name** text box, type a name for the category.
4. (Optional) In the **Header Text** text box, type descriptive text. The text is displayed under the category name on the right-hand side of the Reports page when a user selects the category.
5. Click **Save**.

**Adding report subcategories**

Report subcategories can assist with further organizing the categories and reports that are located on the Reports page. You can add subcategories to any category if you have the necessary permissions to do so.

**To add a report subcategory**

1. In the ServiceDesk portal, click **Reports**.
2. On the Reports page, under **Report Categories**, select the category that you want to add a subcategory to.
3. On the right side of the page, click the orange lightning symbol, and then click **New Sub Category**.
4. In the **Category Information** dialog box, in the **Name** text box, type a name for the subcategory.
5. (Optional) In the **Header Text** text box, type some descriptive text. The text is displayed under the category name on the right-hand side of the **Reports** page when a user selects the category.
6. Click **Save**.

**Deleting report categories**

Users with the appropriate permissions can delete report categories. When you delete report categories, the subcategories and the reports that are contained in that category are not necessarily deleted. You can make selections during the deletion process, which determines what happens to the subcategories and the reports that are contained in a report category.
To delete a report category

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category to delete.
3. On the right side of the page, click the **Actions** symbol (orange lightning), and then click **Delete**.
4. In the **Delete Category** dialog box, select one of the following options for handling any subcategories that are contained in the category:
   - **Don’t delete SubCategories** Retains all subcategories that are contained in the parent category. The subcategories are moved up to the root level.
   - **Delete SubCategories** Deletes all subcategories that are contained in the parent category. If reports in that category also belong to another category, they remain in the other categories. If reports do not belong to other categories, they are moved to the Orphan category.
   - **Delete SubCategories and all reports in them** Deletes all subcategories and the reports they contain.

Select one of the following options for handling any reports that are contained in the category:

- **Don’t delete reports** Retains all reports that are contained in the category.
- **Delete reports (that are linked only to the deleted category)** Deletes all the reports that are contained in the category, as long as they are linked only to the deleted category. If the reports are linked to additional categories, they are retained.
- **Delete reports even if linked to multiple categories** Deletes all reports that are contained in the category, even if they are linked categories other than the one being deleted.

5. Click **Delete**.

**Setting permissions for a report category**

Report categories help you organize all of the reports that are located on the Reports page. Organizing the reports in categories helps users find the reports they need more easily. You can apply permissions to categories, which deny or
grant access to that category and all the reports within it. By default, the category inherits the permissions of the user who created it. If you want the permissions to be different for other users of the category, you need to modify the category permissions.

An administrator or other user who has the appropriate permissions can set permissions on a report. The report permissions control the access to and use of that report. For example, you can specify what users or groups can view, edit, delete, or create subreports for a report.

To set permissions for a report category

1 In the ServiceDesk portal, click Reports.
2 On the Reports page, under Report Categories, select the category.
3 In the right pane, at the far right of the category's title bar, click the Actions symbol (orange lightning), and then click Permissions.
4 In the Category Permissions dialog box, add or edit permissions as needed. See “Setting permissions” on page 113.
5 When you finish setting permissions, click Close.

Adding reports to additional categories

When a report is first added to ServiceDesk, it is assigned to a single category. You can add a report to any number of additional categories.

To add a report to additional categories

1 In the ServiceDesk portal, click Reports.
2 On the Reports page, under Report Categories, select the report’s category.
3 In the right pane, at the far right of the category’s title bar, click the Actions symbol (orange lightning), and then click Categories.
4 In the Report Category Management dialog box, click the Add New Category tab.
5 Select the category that you want to add the report to and click Add.
6 Click Close.

Importing a report category

You can import report categories from another instance of ServiceDesk.
To import a report category

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, click **Import Category**.
3. In the **Import** dialog box, click **Browse** and select the report file.
4. Select one of the following options:

   - **Overwrite existing reports**: Overwrites any reports that have the same report ID as an imported report.
   - **Create new copy**: Creates new copies of all the reports.

5. Click **Import**.

About child reports

The use of child reports in ServiceDesk lets you create and edit a copy of a report. If you need to add custom information to a report, you can make the changes without affecting the original report definition. When you create a child report, you can add data but not subtract it.

Child reports are created from the **Reports** page, using the **Child Reports** option that appears when you click the **Actions** symbol (orange lightning).
Creating and customizing standard reports

This chapter includes the following topics:

- Creating a standard report
- Setting up or modifying the data in standard reports
- Customizing the layout of grid standard reports
- Customizing the filtering and sorting for standard reports
- Setting up or modifying Web Service access for standard reports
- Add/Edit Standard Report dialog box
- Modifying standard reports

Creating a standard report

Administrators and users with the appropriate permissions can create reports.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

To create a new report

1. In the ServiceDesk portal, select Reports.
2. In the Report Categories area, select the category that you want the report to reside in. The report that you create is added to the category that you select.
3. Click the Add Report icon, and select Add Standard Report.
4 In the **Name** field, enter a name for the report. Report names must be unique. The **Name** field has a 100 character limit.

5 In the **Report Designer** tab, specify the data that you want included in the report and the display of that data.

See “Setting up or modifying the data in standard reports” on page 404.

6 (Optional) In the **Description** tab, enter a description for the report which appears on the Reports portal page underneath the report. The description should make it easy for users to quickly understand the information that the report contains. The description text is also searched when users search for reports. The description has no character limit.

7 On the **Permissions** tab, add or edit the permissions as needed.

See “Setting permissions” on page 113.

8 (Optional) On the **WebServices** tab, set up Web Service access for the report.

See “Setting up or modifying Web Service access for standard reports” on page 407.

9 Click **Save**.

---

**Setting up or modifying the data in standard reports**

The data that is included and displayed in reports is completely customizable. On the **Report Designer** tab, you can specify the information that should be included in a report, as well as criteria to narrow the report results. The information that you specify in this tab can both add to and restrict the data that appears in the report.

Selecting a check box for a type of data to add to the report includes all of the fields available for that section in the report. The available fields are displayed in the **Data** section. Selecting the check box for one of the fields lets you apply filters to the data that is returned in that field.

For example, if you wanted information about Incident Management in the report, you would select the checkbox to expand the Incident Management section. Selecting that checkbox adds all of the fields in the Incident Management table to the report. If you want to display the data from a particular field, you need to add the particular column to the report.

However, you may only be interested in seeing the incidents that have an SLA status of “late”. When you select the “SLA Status” checkbox, the SLA Status dialog opens. This dialog lets you narrow the results of the report, by checking the “Late” checkbox and clicking OK. Selecting this checkbox narrows the report results so that only incidents with an SLA status of “late” are shown.
As you work in the Preview pane, it displays the results of the report as you build it. After every change that you make, the display refreshes. If the constant refreshing becomes cumbersome, you can uncheck the Auto Preview option as you work. You can reselect the option whenever you need to see an updated preview of the report.

To set up or modify the data and display of standard reports

1 In the ServiceDesk portal, select Reports.

2 On the Reports page, do one of the following:
   - Create a new report.
     See “Creating a standard report” on page 403.
   - Modify an existing report.
     See “Modifying standard reports” on page 411.

3 In the Add/Edit Standard Report dialog box, select the Report Designer tab.
   See “Add/Edit Standard Report dialog box” on page 408.

4 On the Data tab, select the check box for the type of data that you want to include in the report.

When you select a data type, all of the data fields of that type are added to the report. All of the data fields are available for display in the report. Data types that are included in the report have a green check mark next to them. Repeat this step for all of the data types that you want to include in the report.

5 (Optional) To filter the data that is included in the report, select the check box next to the field that you want to filter.

The fields to which you have applied filtering have a green check mark next to them. For example, you may want to filter incidents so that only those with a priority of high are shown in the report. In the dialog that appears, set the parameters for the filter, and click OK.

6 In the Columns area, select the check box for the columns that you want to display in the report. Repeat this step for all of the columns that you want to include in the report. Columns that are included in the report have a green check mark next to them, and are displayed at the top of the columns area.

7 (Optional) Customize the layout of the report.
   See “Customizing the layout of grid standard reports” on page 406.

8 (Optional) Customize the filtering and sorting of the report.
   See “Customizing the filtering and sorting for standard reports” on page 406.

9 Click Save.
Customizing the layout of grid standard reports

You can view the layout of a report as you work on it. The report preview pane, in the center of the Report Designer tab, shows you how the report currently looks.

See “Add/Edit Standard Report dialog box” on page 408.

When Auto Preview is selected, the changes you make to your report are shown as you make them. If you make a lot of changes, you may want to turn off Auto Preview. When Auto Preview is turned off, you do not have to wait for each change to be reflected in the preview pane. If you have turned off Auto Preview, you can click Generate to see the current report with all of your changes.

When Limit Results is selected, the report results are limited to the top 50 results. When you limit results, you can see how the report looks without showing a large amount of data in the report preview pane.

You can customize the layout of grid standard reports in the following ways:

- Move columns in the report by selecting the left arrow or right arrow for the column in the report preview pane.
- Delete a column by selecting the red x for the column in the report preview pane.
- Change the name of a column by moving your mouse over the column name in the Columns section, and clicking the Edit option. Edit the title of the column and click OK.
- Adjust column width by placing the mouse arrow over the column and dragging to get the desired width.
- Apply special formatting to columns in the report by adding renderers. For example, you can set up your report so that high priority incidents appear in red. To apply the formatting, you would move your mouse over the column name in the Columns section, and click the Edit option. Select the type of renderer to apply, click Add Renderer, enter the text to search for, select a fore color of red, and click OK.

Customizing the filtering and sorting for standard reports

You can specify the grouping, sorting, and paging options for a report.

For information about optimizing your reports to improve the performance of the Process Manager:
To customize the filtering and sorting for a report

1. In the ServiceDesk portal, select **Reports**.
2. On the Reports page, do one of the following:
   - Create a new report. See “Creating a standard report” on page 403.
   - Modify an existing report. See “Modifying standard reports” on page 411.
4. (Optional) In the **Report Designer** tab, select **Options**.
5. Select the **Limit Rows** check box to limit the number of rows that are returned with the report. The default number of rows that are returned is 50. When you select this option, the user is able to configure the number of rows that are returned at run time.
6. Select the **Use Paging** check box, and specify the number of rows per page for the report.
7. Select a column in the **Sort By** drop-down list to sort the report by that column, and select ascending or descending sort order.
8. Select up to three columns to group the report by in the **Group By** drop-down lists.
9. To add aggregations to your groups, under **Group Aggregations**, select a column to aggregate a group by and the type of aggregation, and then click **Add Aggregation**. Aggregations summarize mathematical data at the group level. For example, you can set up an aggregation that displays the average age of a ticket per location.
10. Click **Display SQL** to display the SQL statement that the report executes against the database.
11. Click **Save**.

**Setting up or modifying Web Service access for standard reports**

Setting up web service access for a report allows programmatic access to that report.
The Web service access is required if you plan to configure schedules automatically execute and email reports.

See “Scheduling automatic report emails” on page 413.

To set up or modify Web Service access for standard reports

1 In the ServiceDesk portal, click Reports.

2 On the Reports page, do one of the following:
   • Create a new report.
     See “Creating a standard report” on page 403.
   • Modify an existing report.
     See “Modifying standard reports” on page 411.

3 In the Add/Edit Standard Report dialog box, click the Web Services tab.
   See “Add/Edit Standard Report dialog box” on page 408.

4 On the WebService tab, click the check box to enable programmatic access to the report. To enable WebService Access, enter the following information:

   **Namespace**
   The namespace for the WebService and the objects that are used in the web service.

   **Namespace URL**
   The URL for the namespace.

   **WebService Name**
   A name that describes the service, such as “OpenIncidentsThisMonthReport”.

   **Class Name**
   The results of the report are an array of the class name that is supplied here. The class name has public properties for each of the columns in the report.

   Click Generate to compile the WebService and deploy it to a URL.

   The URL is displayed on the screen and can be used to access the WebService. When report data changes, you need to generate the WebService again to update the class.

5 Click Save.

---

**Add/Edit Standard Report dialog box**

This dialog box appears when you create or edit a standard report.

The Add/Edit Standard Report dialog box has four tabs.
Table 36-1  Tabs in the **Add/Edit Standard Report** dialog box

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Designer</td>
<td>Lets you specify what data is included in the report and specify options for that data. You can also specify the sorting and grouping of the resulting data, and specify columns for the resulting data set.</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you specify a description of the report which is displayed on the Reports page.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Lets you specify the permissions for the report.</td>
</tr>
<tr>
<td>Web Services</td>
<td>Lets you enable Web Service access to the report.</td>
</tr>
</tbody>
</table>

Table 36-2  Options on the **Report Designer** tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data tab</td>
<td>Lets you specify the type of data that is included in the report.</td>
</tr>
<tr>
<td>Grid</td>
<td>Displays the current report in grid view in the report preview pane. Whichever pane is displayed when you save the report is the type of report that anyone viewing the report sees.</td>
</tr>
<tr>
<td>Chart</td>
<td>Displays the current report in chart view in the report preview pane. Whichever pane is displayed when you save the report is the type of report that anyone viewing the report sees.</td>
</tr>
<tr>
<td>Auto Preview</td>
<td>Displays a preview of the current report as you build it. Auto Preview is selected by default.</td>
</tr>
<tr>
<td>Limit Results</td>
<td>Limits the result set of the report that is shown in the report preview pane to 50. The Limit Results option is selected by default.</td>
</tr>
<tr>
<td>Generate</td>
<td>When Auto Preview is not selected, clicking Generate lets you view the report in the report preview pane with all the changes you have made.</td>
</tr>
<tr>
<td>Columns</td>
<td>Lets you specify the columns that are displayed in the report.</td>
</tr>
<tr>
<td>Options tab</td>
<td>Lets you specify the grouping and sorting of the data in the report.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Limit Rows</td>
<td>Lets you specify the maximum number of rows that are included in the report. The default number of rows is 50, and users can configure the number of rows they want to see in the report at run time.</td>
</tr>
<tr>
<td>Use Paging</td>
<td>Lets you specify the number of rows per page in the report.</td>
</tr>
<tr>
<td>Sort By</td>
<td>Lets you specify the columns to sort by and whether the data in those columns should be sorted in ascending or descending order.</td>
</tr>
<tr>
<td>Group By</td>
<td>Lets you specify the columns to group by.</td>
</tr>
<tr>
<td>Group Aggregations</td>
<td>Lets you add group aggregations. Group aggregations summarize mathematical data at the group level. For example, you might want to add an aggregation to a report that shows the average age of a ticket per location.</td>
</tr>
<tr>
<td>Add Aggregation</td>
<td>Lets you add aggregations to the report. Any number of aggregations are allowed.</td>
</tr>
<tr>
<td>Display SQL</td>
<td>Displays the SQL statement for the report.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rows in the tab</td>
<td>Lists the current permissions that are assigned to the report.</td>
</tr>
<tr>
<td>Edit icon</td>
<td>Lets you edit the permissions for that user, group, permission, or organization.</td>
</tr>
<tr>
<td>Delete icon</td>
<td>Lets you delete that permission.</td>
</tr>
<tr>
<td>Add New Permission</td>
<td>Lets you add a new permission.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled for programmatic access</td>
<td>Lets you enable the report for programmatic access. Selecting this check box displays the fields that you need to specify to set up Web Service access.</td>
</tr>
<tr>
<td>Namespace</td>
<td>The namespace for the WebService and the objects that are used in the webservice.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Namespace URI</td>
<td>The URI for the namespace.</td>
</tr>
<tr>
<td>WebService Name</td>
<td>A name that describes the service, such as “OpenIncidentsThisMonthReport”.</td>
</tr>
<tr>
<td>Class Name</td>
<td>The results of the report are an array of the class name that is supplied here. The class name has public properties for each of the columns in the report.</td>
</tr>
<tr>
<td>Generate</td>
<td>Compiles the Web Service and deploys it to a URL. The URL is displayed on the screen and can be used to access the WebService. When report data changes, you need to generate the WebService again to update the class.</td>
</tr>
</tbody>
</table>

### Modifying standard reports

You can modify any report for which you have the appropriate permissions. You are more likely to spend time modifying existing reports than creating new reports. ServiceDesk includes many predefined reports that meet most of your reporting needs. When you want to make a small change to an existing report, copy the existing report and make your changes in the new report. By copying the report instead of making modifications directly to a predefined report, you can always go back to the original report.

For information about optimizing your reports to improve the performance of the Process Manager:

See “Optimizing reports in the Process Manager portal” on page 393.

To modify a standard report

1. In the ServiceDesk portal, select Reports.
2. On the Reports page, under Report Categories, select the category that contains the report that you want to modify.
3. Under Reports, at the far right of the report name, click the Actions symbol (orange lightning), and then click Edit.
4 In the **Edit Standard Report** dialog box, edit the report.

The dialog and tabs for editing and adding standard reports are the same.

See “Creating a standard report” on page 403.

See “Add/Edit Standard Report dialog box” on page 408.

5 Click **Save**.
Scheduling reports

This chapter includes the following topics:

■ Scheduling automatic report emails
■ Creating a report schedule
■ New Report Schedule dialog box
■ Adding a report to a report schedule
■ Options for scheduling reports and events

Scheduling automatic report emails

You can automatically execute and email reports on one or more schedules that you define. You can send the reports in Excel, CSV, or HTML format.

Before a report schedule can run, you must set up Web service access.

See “Setting up or modifying Web Service access for standard reports” on page 407.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a report schedule.</td>
<td>The schedule defines when the report emails are sent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating a report schedule” on page 414.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add reports to the schedule.</td>
<td>You can specify one or more reports to include in the scheduled email message.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding a report to a report schedule” on page 415.</td>
</tr>
</tbody>
</table>
Creating a report schedule

You can create a schedule for emailing reports in several formats. After you create the schedule, you must select the reports to send. See “Adding a report to a report schedule” on page 415.

To create a report schedule

1. In the ServiceDesk portal, click Admin > Reports > Report Schedule List.
2. In the upper right of the Report Schedules section, click the Add Report Schedule symbol (a white page with a green plus sign).
3. In the New Report Schedule dialog box, name and configure the schedule. The type of schedule that you select determines the schedule settings that appear.
4. When you finish configuring the schedule, in the New Report Schedule dialog box, click Save.

New Report Schedule dialog box

This dialog box lets you configure schedules for sending report emails.

Table 37-2 Options in the New Report Schedule dialog box

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lets you provide a unique, descriptive name for the schedule so that it can be easily recognized in the Report Schedules section.</td>
</tr>
<tr>
<td>Active</td>
<td>Makes the schedule active so that the report runs at the scheduled times. You can uncheck this check box at any time to disable this schedule temporarily.</td>
</tr>
<tr>
<td>Select type of schedule</td>
<td>Lets you schedule the report to run in one of the following intervals:</td>
</tr>
<tr>
<td></td>
<td>■ Daily (number of days)</td>
</tr>
<tr>
<td></td>
<td>■ Weekly</td>
</tr>
<tr>
<td></td>
<td>■ Monthly</td>
</tr>
<tr>
<td></td>
<td>■ One time only</td>
</tr>
<tr>
<td></td>
<td>The type of schedule that you select determines the remaining schedule options that appear in this dialog box. These schedule options are the same for several other types of schedules.</td>
</tr>
<tr>
<td></td>
<td>See “Options for scheduling reports and events” on page 415.</td>
</tr>
</tbody>
</table>
Table 37-2 Options in the New Report Schedule dialog box (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>Opens the Advanced dialog box, which lets you set the report task to repeat after a specified number of minutes or hours, until a specified time. For example, you can set a report to run every four hours on the scheduled days. This option is not available for a one-time-only schedule.</td>
</tr>
</tbody>
</table>

Adding a report to a report schedule

After you create a schedule for emailing one or more reports, you must select the reports to send.

See “Creating a report schedule” on page 414.

To add a report to a report schedule

1. In the ServiceDesk portal, click Admin > Reports > Report Schedule List.
2. Under Report Schedules, find the schedule, click the Actions symbol (orange lightning) at the far right of the schedule name, and then click Reports.
3. In the Reports dialog box, click Add Report.
4. Under Reports List, specify the report to run, the addresses to send it to, and the format to send, and then click Add.
5. To add more reports, repeat step 3 through step 4.
6. When you finish adding reports, in the Reports dialog box, click Close.

Options for scheduling reports and events

In ServiceDesk, you can create schedules to email reports.

See “Scheduling automatic report emails” on page 413.

You schedule the report emails in the New Report Schedule dialog box.


These schedule dialog boxes let you schedule the event to run in one of the following intervals:

- **Daily (number of days)**
  - See Table 37-3.

- **Weekly**
  - See Table 37-4.
- **Monthly**  
  See Table 37-5.

- **One time only**  
  See Table 37-6.

The options that appear for each of these intervals are the same regardless of the type of schedule you define.

**Table 37-3**  Daily scheduling options in the schedule dialog boxes

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start date &amp; time</td>
<td>The date and time at which the event begins.</td>
</tr>
<tr>
<td>End Date</td>
<td>The date on which the event ends.</td>
</tr>
<tr>
<td>Perform this task</td>
<td>Lets you specify the days on which the event should occur, as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Every Day</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Weekdays</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Every</strong> (number of days)</td>
</tr>
<tr>
<td></td>
<td>The interval of days between the event occurrences.</td>
</tr>
</tbody>
</table>

**Table 37-4**  Weekly scheduling options in the schedule dialog boxes

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>The time at which the event begins.</td>
</tr>
<tr>
<td>End Date</td>
<td>The date on which the event ends.</td>
</tr>
<tr>
<td>Every (number of weeks)</td>
<td>Lets you specify an interval of weeks between the event occurrences.</td>
</tr>
<tr>
<td>Select the day(s) of the week below</td>
<td>Lets you specify one or more days on which the event occurs every week. For example, you can run a report on Tuesday and Friday of the scheduled week.</td>
</tr>
</tbody>
</table>

**Table 37-5**  Monthly scheduling options in the schedule dialog boxes

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>The time at which the event begins.</td>
</tr>
<tr>
<td>End Date</td>
<td>The date on which the event ends.</td>
</tr>
</tbody>
</table>
### Table 37-5  Monthly scheduling options in the schedule dialog boxes (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perform this task</strong></td>
<td>Lets you specify the days of the month on which the event should occur, as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Day</td>
</tr>
<tr>
<td></td>
<td>The Days link that appears to the right of this option lets you select the days of the month on which the event should occur.</td>
</tr>
<tr>
<td></td>
<td>■ The</td>
</tr>
<tr>
<td></td>
<td>The Weeks and Weekdays links that appear to the right of this option let you select the weeks of the month and the days of the week on which the event should occur.</td>
</tr>
<tr>
<td><strong>Of the month(s)</strong></td>
<td>Lets you select the months in which the event should occur.</td>
</tr>
</tbody>
</table>

### Table 37-6  One-time-only scheduling options in the schedule dialog boxes

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start date &amp; time</td>
<td>The date and time at which the event occurs.</td>
</tr>
</tbody>
</table>
Scheduling reports

Options for scheduling reports and events
Setting up and managing ServiceDesk

- Chapter 38. Configuring ServiceDesk
- Chapter 39. Managing security, users, roles, groups, and permissions
- Chapter 40. Managing the Active Directory connections
- Chapter 41. Managing categories and the data hierarchy
- Chapter 42. Customizing forms
- Chapter 43. Customizing the email in ServiceDesk
- Chapter 44. Distributing the ServiceDesk documentation
- Chapter 45. Performing administrative tasks
Configuring ServiceDesk

This chapter includes the following topics:

■ About configuring ServiceDesk
■ Before you configure ServiceDesk
■ Configuring ServiceDesk
■ Additional ServiceDesk configurations
■ About migrating data to ServiceDesk 7.5
■ Advanced ServiceDesk customizations
■ About the incident priority
■ Default priority, urgency, and impact values
■ How the incident priority is calculated
■ Creating and Editing Service Level Agreements (SLAs)
■ About configuring the Service Level Agreement (SLA) late date
■ Default SLA levels
■ Configuring business hours
■ About configuring Data Mapping Routing Tables
■ About incident types
■ Creating and deleting incident types
■ About the Service Catalog and service items
■ Migrating data from ServiceDesk 7.1 SP2
The installation of the Workflow Platform and ServiceDesk modules includes an initial configuration of ServiceDesk and the Process Manager portal. The initial configuration lets you select the parts of ServiceDesk to install and configure communication settings.

See “Before you configure ServiceDesk” on page 423.

Before you use ServiceDesk in your production environment, you must configure ServiceDesk to meet your needs. First, you must add users and groups and set up their permissions. Also, ServiceDesk comes with a default set of business of hours. You need to configure the business hours and add holidays to meet your schedule.

Before you use the Problem Management and Knowledge Management processes, you may want to modify the email notifications and personalize the Process Manager portal.

Out-of-the-box, Change Management provides a default CAB and one preconfigured rule. The OnChangeReceived ruleset comes with a rule that routes all change requests to that default CAB. Before you put the Change Management process into production, you must perform certain tasks.

Examples of some of the tasks you must perform to configure the Change Management process are as follows:

- Create your Change Approval Boards.
- Creating email templates.
- Configure your Change Management rulesets.

Out-of-the-box, Incident Management provides a default Service Queue, two preconfigured routing rules, and default Service Level Agreement levels, escalations, and milestones. The OnIncidentReceived ruleset has a preconfigured rule that routes all incidents to the default Service Queue. The OnResolutionVerified ruleset has a preconfigured rule that sends out the Customer Satisfaction Survey when a ticket is resolved. Before you put the Incident Management process into production, you must perform certain tasks.

Examples of some of the tasks you must perform to configure the Incident Management process are as follows:

- Configure your Service Level Agreement levels, escalations, and milestones.
Before you configure ServiceDesk

Before you begin to configure ServiceDesk, you must use the ServiceDesk installer to install the Workflow framework and ServiceDesk modules on the ServiceDesk server.

The installation of the Workflow Platform and ServiceDesk modules includes an initial configuration of ServiceDesk and the Process Manager portal. The initial configuration lets you select the parts of ServiceDesk to install and configure communication settings.

Before you use ServiceDesk in your production environment, you must configure ServiceDesk to meet your needs.

See “Configuring ServiceDesk” on page 423.

Configuring ServiceDesk

Before you use ServiceDesk in your production environment, you must configure ServiceDesk to meet your needs. The configuration tasks are performed in the Process Manager portal and require administrator permissions.

See “About configuring ServiceDesk” on page 422.

You may want to perform some of these tasks again after your initial ServiceDesk configuration.

Before you begin to configure ServiceDesk, verify that it is installed and that you have performed the required setup steps.

See “Before you configure ServiceDesk” on page 423.

After you configure ServiceDesk, you may want to perform some additional configurations before you introduce ServiceDesk into your production environment.

See “Additional ServiceDesk configurations” on page 428.

If you migrated from a previous version of ServiceDesk or from Helpdesk Solution 6.x, you may want to migrate data to ServiceDesk 7.5.

See “About migrating data to ServiceDesk 7.5” on page 430.
Depending on your needs, you may want to perform some advanced customizations before you introduce ServiceDesk into your production environment.

See “Advanced ServiceDesk customizations” on page 430.

Table 38-1  ServiceDesk configuration tasks

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Import users and groups from Active Directory, verify, and assign permissions. | If you use Active Directory authentication for ServiceDesk, you can set up Active Directory server connections and Active Directory sync profiles. Once you add the sync profiles, you can import the users and groups from Active Directory into ServiceDesk.  
See “Configuring Active Directory sync profiles” on page 467.  
Review the imported information to verify its accuracy, edit it if necessary, and assign permissions.  
See “Copying permissions between groups” on page 456.  
See “Adding or removing permissions for groups” on page 456. |
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Customize the appearance of the Process Manager portal.** | You can customize the Process Manager portal in the following ways:  
- Customize the general appearance by adding a company logo.  
  You can perform this customization in the Process Manager portal, in the **Customization** section of the **Master Settings** page.  
  See “Editing the Process Manager portal master settings” on page 530.  
- Customize individual portal pages for the entire organization or for users, groups, or organizational groups, or permission groups.  
  Administrators have permission to customize portal pages and to grant customization permissions to other ServiceDesk users.  
  See “About customizing the contents of Process Manager portal pages” on page 80. |
| **Configure your business hours and holidays.** | Business hours are the hours during which your business is commonly conducted. ServiceDesk provides a set of default business hours.  
  The default business hours are Monday thru Friday, 8:00 A.M. to 5:00 P.M. You can modify the default business hours or add your own business hours configurations.  
  See “Configuring business hours” on page 438. |
| **Configure Service Level Agreement (SLA) levels, escalations, and milestones.** | A Service Level Agreement (SLA) is a contract between an organization and its service provider, which sets the expectations and requirements for service delivery. The SLA includes the allowable time frame for the service delivery.  
  Incident Management provides default Service Level Agreement levels, escalations, and milestones. You can use the default settings or you can configure SLA levels, escalations, and milestones to meet your needs.  
  See “Creating and Editing Service Level Agreements (SLAs)” on page 435. |
| **Configure incident categories and the data hierarchy.** | Categories are used to classify ServiceDesk incidents. ServiceDesk contains predefined incident categories, which you can use immediately or edit to meet your organization’s requirements. If you migrated incidents or categories from Helpdesk Solution, those categories are added to the Process Manager portal for use in future incidents.  
  Review the existing categories and edit or add to them if necessary.  
  See “About Incident Management classifications and the data hierarchy” on page 499.  
  See “Default categories for incidents and default classifications for problems” on page 559. |
### Table 38-1  ServiceDesk configuration tasks (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify or edit the incident types.          | During incident submission, support technicians can specify an incident type to identify the general nature of the incident. The incident type can be modified whenever an incident is worked.  
If an incident type has not been provided, the support technician must provide an incident type when an incident is resolved.  
ServiceDesk contains a set of predefined incident types that are ready to use. Review them to ensure that they meet your needs. If necessary, you can create or delete incident types.  
See “About incident types” on page 440.  
See “Creating and deleting incident types” on page 441. |
| Verify or edit the default impact, urgency, and priority values. | During incident entry, the submitter specifies the incident’s impact and urgency. Support technicians can also specify the priority. When a user submits an incident, the priority level is assigned based on the impact and the urgency that the user specified.  
See “About the incident priority” on page 432.  
ServiceDesk contains default values for the impact, urgency, and priority settings. You can change the available impact and urgency values and the priority that is assigned to the combination of the two values. |
| Create Incident Management service queues  | The Incident Management process lets you route incidents to service queues. Before you can configure rules to route incidents, you must first create your service queues. These service queues are then available when you create your routing rules to route incoming incidents or to reassign an incident.  
Service queues consist of a group or multiple groups that you associate with it. You can change users and group without reconfiguring your routing rules. You can add or remove the users that are in the group that you associate with the service queue. You can add or remove the groups that are associated with the service queue.  
See “Creating incident service queues” on page 189. |
| Configure your Data Mapping Routing Tables  | The Incident Management process lets you configure routing tables so that you can route incidents by specific classifications or by specific locations.  
Before you can configure rules to route incidents by specific classifications or locations, you must first configure the Routing Tables.  
These routing tables can then be used when you create your routing rules to route your incidents.  
See “About configuring Data Mapping Routing Tables” on page 440. |
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create email templates for Incident Management.</td>
<td>Email notifications for Incident Management are handled through the Process Automation rules. Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. These templates are then available when you create your email notification rules and select the <strong>Send Email</strong> action. See “Creating email templates for Incident Management” on page 195.</td>
</tr>
<tr>
<td>Configure the Incident Management Process Automation rules.</td>
<td>Rules determine which incidents are routed to which queues when new ServiceDesk incidents are submitted. Rules determine when email notifications are sent. Rules determine what happens when incident SLAs are late. This step requires time for testing and configuration. To set up automation rules properly, it’s important to understand the underlying process. The actions available in the rule builder give you the ability to change information about the ticket while the ticket executes. See “Incident Management Process Automation rules components” on page 203.</td>
</tr>
<tr>
<td>Verify or edit the incident close codes.</td>
<td>When an incident is closed, the support technician must provide a close code to indicate the nature of the resolution. ServiceDesk contains a set of predefined close codes that are ready to use. Review them to ensure that they meet your needs. If necessary, you can delete or add to the default close codes. See “About incident close codes” on page 528. See “Adding and deleting incident close codes” on page 529.</td>
</tr>
<tr>
<td>Create change team groups for Change Management.</td>
<td>In the Change Management process, a change team is a group of people who can assess, plan, authorize, schedule, implement, and test a change request. The change team includes the change advisory board (CAB). The members of the CAB advise the change manager in the assessment, planning, and authorization of changes. During the initial approval phase of the Change Management process, the change manager selects the members of the change team. You can create predefined change team groups to facilitate the team selection. See “Configuring Change Management” on page 229.</td>
</tr>
</tbody>
</table>
### Table 38-1  ServiceDesk configuration tasks (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create email templates for Change Management</td>
<td>Email notifications for Change Management are handled through the Process Automation rules. Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. These templates are then available when you create your email notification rules and select the <strong>Send Email</strong> action. See “Creating email templates for Change Management” on page 234.</td>
</tr>
<tr>
<td>Configure the Change Management Process Automation rules</td>
<td>This step requires time for testing and configuration. To set up automation rules properly, it’s important to understand the underlying process. The actions available in the rule builder give you the ability to change information about the ticket while the ticket executes. See “Configuring Change Management” on page 229.</td>
</tr>
<tr>
<td>(Optional) Make the ServiceDesk documentation available to your users</td>
<td>Each organization has specific requirements for providing documentation to their process workers and the users of the Process Manager portal. Therefore, the ServiceDesk documentation is not installed with ServiceDesk. Symantec recommends that you download these guides and make them available to your users as needed. See “Making the ServiceDesk documentation available to users” on page 515.</td>
</tr>
<tr>
<td>(Optional) Add a MIME type for remote control through RDP</td>
<td>When a process worker works a task that is associated with an equipment configuration item (CI), the worker can access the <strong>Remote Control (Via RDP)</strong> link. The link runs a tool, which generates and downloads an RDP file that contains the configuration item’s IP address. The worker can use the RDP file to open a Remote Desktop Connection to the computer that the CI represents. This functionality requires that IIS (Internet Information Services) contains a MIME type for RDP. If you plan to use the remote control tool, you must add the new MIME type. In Internet Information Services Manager, you can edit the local computer’s Properties and add a new MIME type. In the new MIME type, both the extension and MIME type are .rdp. After you add the new MIME type, you must restart IIS for the change to take effect.</td>
</tr>
</tbody>
</table>

## Additional ServiceDesk configurations

After you configure ServiceDesk, you may want to perform some additional configurations before you introduce ServiceDesk into your production environment.

See “Configuring ServiceDesk” on page 423.
Table 38-2  Additional configuration tasks you can perform

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create incident templates.</td>
<td>In Incident Management, incident templates are special incident forms containing predefined, standard values for common issues. Using templates speeds the entry of incidents and helps to standardize and increase the accuracy of the incident information. Create incident templates for any issues that are reported frequently. You can edit and update them at any time. See “About incident templates” on page 152. See “Creating an incident template” on page 159.</td>
</tr>
<tr>
<td>Create incident subtask templates.</td>
<td>In Incident Management, incident subtask templates are special incident forms containing predefined, standard values for common issues. Using subtask templates speeds the subtask assignment process and helps to standardize and increase the accuracy of the information. See “About subtask templates” on page 180. See “Creating subtask templates” on page 184.</td>
</tr>
<tr>
<td>Create change request templates.</td>
<td>In Change Management, change templates are special change forms containing predefined, standard values for common issues. Using templates speeds the entry of changes and helps to standardize and increase the accuracy of the change request information. See “About change templates” on page 243. See “Creating a new change template” on page 244.</td>
</tr>
<tr>
<td>Create and edit reports.</td>
<td>You can customize the ServiceDesk reports in the following ways:</td>
</tr>
<tr>
<td></td>
<td>■ You can copy a report and edit the copy to quickly create a new report.</td>
</tr>
<tr>
<td></td>
<td>■ You can use a wizard interface to create new reports, which eliminate the need to use SQL for report creation</td>
</tr>
<tr>
<td></td>
<td>■ You can add a report to any Process Manager portal page or dashboard, and you can define the size and placement of the report.</td>
</tr>
<tr>
<td></td>
<td>■ You can optimize your reports on the Process Manager portal pages to improve the performance of the Process Manager.</td>
</tr>
<tr>
<td></td>
<td>See “What you can do with a report” on page 391.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a standard report” on page 403.</td>
</tr>
<tr>
<td></td>
<td>See “Modifying standard reports” on page 411.</td>
</tr>
<tr>
<td></td>
<td>See “Optimizing reports in the Process Manager portal” on page 393.</td>
</tr>
</tbody>
</table>
About migrating data to ServiceDesk 7.5

Depending on your needs, you may want to migrate data to ServiceDesk before you introduce ServiceDesk into your production environment.

**Note:** Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See “Configuring ServiceDesk” on page 423.

If you migrated from a previous version of ServiceDesk or from Helpdesk Solution 6.x, you can migrate data to ServiceDesk 7.5.

**Table 38-3** Data migration options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate data from ServiceDesk 7.1 SP2.</td>
<td>You can leverage some data from ServiceDesk 7.1 SP2 in ServiceDesk 7.5.</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data from ServiceDesk 7.1 SP2” on page 442.</td>
</tr>
<tr>
<td>Migrate data from ServiceDesk 7.1 SP1.</td>
<td>You can leverage some data from ServiceDesk 7.1 SP1 in ServiceDesk 7.5.</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data from ServiceDesk 7.1 SP1” on page 443.</td>
</tr>
<tr>
<td>Migrate data from ServiceDesk 7.0 MR2.</td>
<td>You can leverage some data from ServiceDesk 7.0 MR 2 in ServiceDesk 7.5.</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data from ServiceDesk 7.0 MR2” on page 444.</td>
</tr>
<tr>
<td></td>
<td>See “About migrating data from Helpdesk Solution 6.x” on page 444.</td>
</tr>
</tbody>
</table>

Advanced ServiceDesk customizations

Depending on your needs, you may want to perform some advanced customizations before you introduce ServiceDesk into your production environment.

See “Configuring ServiceDesk” on page 423.
The advanced customization tasks are configured in Workflow Designer. To view the projects that are available for advanced customization, you need to open Workflow Manager and then click **File > Open Project**.

For more information about using Workflow Designer to configure the workflow projects, see the **Symantec™ Workflow 7.5 User Guide**.

For more information about the advanced customizations that you can perform in ServiceDesk, see the **Symantec Connect**.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the appearance and content of</td>
<td>In the Process Manager portal, a form is the screen or page that users and workers interact with during a process.</td>
</tr>
<tr>
<td>forms.</td>
<td>ServiceDesk contains predefined forms for all its processes. These predefined forms are complete and ready to use immediately. However, you can customize any of the forms to meet your organization’s established process requirements.</td>
</tr>
<tr>
<td></td>
<td>See “About customizing forms” on page 505.</td>
</tr>
<tr>
<td>Examples of common form customizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Setting permissions for forms.                                                                                                         See “Setting permissions for a form” on page 508.</td>
</tr>
<tr>
<td></td>
<td>■ Editing the Customer Satisfaction Survey to change the frequency with which it is sent and the data that it collects.                                                                                     See “About the Customer Satisfaction Survey” on page 508.</td>
</tr>
<tr>
<td></td>
<td>You can use Workflow Designer to customize the appearance and behavior of the forms in the Process Manager portal.</td>
</tr>
<tr>
<td>Customize email for ServiceDesk processes.</td>
<td>ServiceDesk can send email notifications when various Problem Management and Knowledge Management process events occur. It can also create incidents from inbound email.</td>
</tr>
<tr>
<td></td>
<td>These email capabilities are predefined and ready to use. However, you can customize them as needed.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing the email actions for ServiceDesk processes” on page 511.</td>
</tr>
<tr>
<td>Verify the problem categories.</td>
<td>During the entry of a problem ticket, the process worker specifies a category to help classify the root cause of the problem.</td>
</tr>
<tr>
<td></td>
<td>ServiceDesk contains default values for the problem category. You can add and edit the problem categories. You can make these changes by editing the <strong>SD.ProblemManagement</strong> project in Workflow Designer.</td>
</tr>
</tbody>
</table>
About the incident priority

Every incident that is submitted to the ServiceDesk is assigned a priority. This priority lets you determine how the incident is routed and when it is escalated. The prioritization of incidents helps you manage Service Level Agreements (SLA) and comply with the concepts of ITIL service management.

A user who submits an incident can specify the urgency and the impact. You can use these values to calculate the incident’s priority and to create routing rules for its initial routing. This automatic calculation eliminates guesswork and prevents the user from assigning a high priority to every incident. The support technician who works the incident can change the urgency values and impact values as well as the calculated priority.

See “How the incident priority is calculated” on page 434.

A support technician who uses the advanced incident form can specify the urgency, impact, and priority. The priority is not calculated automatically because the support workers can assess an incident’s priority better than the users can.

ServiceDesk contains default values for the urgency, impact, and priority settings. The values that are available differ between the standard incident form and the advanced incident form. For the user’s benefit, the values that appear on the standard incident form are more descriptive.

See “Default priority, urgency, and impact values” on page 433.

Most ServiceDesk implementations either use the default priority, impact, and urgency values or make only minor changes.

To change these values and make them available in your Incident Management process, you need to modify different areas of the process as follows:

- In the Process Manager portal, you can edit these values on the Application Properties page.
  These are the values that you can choose from on the advanced incident form and on the "simple" incident form.

- In the Process Manager portal, you can change the impact, urgency, and priority values in the Impact/Urgency Matrix to match those on the Application Properties page.
  You can use the mappings in the Impact/Urgency Matrix to create routing rules to set the priority of your incidents. To use these mappings, select the Set Priority action and then in the next drop-down list select the Using Impact/Urgency Matrix option.
  You can edit this matrix from the Data Mapping page. Click Admin > Process Automation. Expand Incident Management and click Service Dashboard.
  Under Actions: INCIDENT-MGMT, click Manage Data Mappings.
In Workflow Designer, you can edit the advanced feeder form to reconfigure the **Auto-calculate Priority** link on the advance incident form. Changing the values requires caution and a good understanding of the Symantec Workflow software. You can change the available impact and urgency values and the priority that is assigned to the combination of the two values. You make these changes by editing the advanced feeder form in Workflow Designer.

For more information about forms customization and project modifications, see the Symantec™ Workflow 7.5 User Guide.

### Default priority, urgency, and impact values

During incident entry, the submitter specifies the urgency and impact. When a user submits an incident, the priority is assigned based on the urgency and the impact that the user specified. The support technicians can change an assigned priority. Support technicians who create new incidents can specify the priority.

ServiceDesk contains default values for the priority, urgency, and impact settings. See “About the incident priority” on page 432.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Urgency</strong></td>
<td>Represents an assessment of how much the issue affects the submitter or the primary contact. The end users and support technicians can select from the following values:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Core Business Service</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Support Service</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Non-urgent Services</strong></td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>Defines the extent of the issue by specifying how many people are affected. The users and support technicians can select from the following values:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Department/LOB/Branch</strong></td>
</tr>
<tr>
<td></td>
<td>(LOB means line of business)</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Small group or VIP</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Single User</strong></td>
</tr>
</tbody>
</table>
Table 38-5  Default priority, urgency, and impact values (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default values</th>
</tr>
</thead>
</table>
| Priority | Determines how the incident is routed and when it is escalated. This setting is available on the advanced incident form only. The default values are as follows:  
  ■ Low  
  ■ Minor  
  ■ Normal  
  ■ High  
  ■ Urgent  
  ■ Emergency |

How the incident priority is calculated

When a user submits an incident, the incident is assigned a priority based on the impact and the urgency that the user specified. This automatic calculation can eliminate guesswork and prevents the user from assigning a high priority to every incident.

On the Create a New Incident page that the user sees, the option to specify the impact is named Who is Affected?

See “About the incident priority” on page 432.

You can configure the values and the way that they combine to arrive at the priority.

Table 38-6  How the incident priority is calculated

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Impact</th>
<th>Calculated priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-urgent Services</td>
<td>Single User</td>
<td>Low</td>
</tr>
<tr>
<td>Non-urgent Services</td>
<td>Small group or VIP</td>
<td>Normal</td>
</tr>
<tr>
<td>Non-urgent Services</td>
<td>Department/LOB/Branch</td>
<td>High</td>
</tr>
<tr>
<td>Support Service</td>
<td>Single User</td>
<td>Normal</td>
</tr>
<tr>
<td>Support Service</td>
<td>Small group or VIP</td>
<td>High</td>
</tr>
<tr>
<td>Support Service</td>
<td>Department/LOB/Branch</td>
<td>High</td>
</tr>
<tr>
<td>Core Business Service</td>
<td>Single User</td>
<td>High</td>
</tr>
</tbody>
</table>
### Table 38-6

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Impact</th>
<th>Calculated priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Business Service</td>
<td>Small group or VIP</td>
<td>Urgent</td>
</tr>
<tr>
<td>Core Business Service</td>
<td>Department/LOB/Branch</td>
<td>Urgent</td>
</tr>
</tbody>
</table>

## Creating and Editing Service Level Agreements (SLAs)

A Service Level Agreement (SLA) is a contract between an organization and its service provider. It sets the expectations and requirements for service delivery. The SLA can be between an external customer and your customer support team or between your organization’s employees and your IT department. The corporate policy typically defines the overall SLA. The SLA formally defines the agreed-upon services, priorities, and responsibilities that are required to support the customers and users.

SLAs use a Business Hours Configuration to determine if an SLA is late or not. The predefined SLAs are configured to use the Default Business Hours. Before you create an SLA, you should configure your business hours.

See "[Configuring business hours](#)" on page 438.

**Video:** For more information about configuring business hours, creating SLAs, and rule sets for SLAs, see [ServiceDesk Configuration: SLA Framework Overview](#) on Symantec Connect.

When you create or edit SLA levels, you can configure the **Late Date**. SLA Configuration late date is made up of days and minutes. You can enter whole or fractional amounts into the **Days** field, in decimal format. You can also use a combination of days and minutes.

See "[About configuring the Service Level Agreement (SLA) late date](#)" on page 436.

### To create or edit Service Level Agreements (SLAs)

1. In the **Process Manager**, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Incident Management** and click **Service Dashboard**.
3. Under **Actions: INCIDENT-MGMT**, click **Manage SLA Levels**.
4 On the **SLA Levels Configuration** page, under **SLA Levels**, perform one of the following actions:

- **Edit an existing SLA level**
  - In the **SLA Levels** table, in the row for the SLA level that you want to edit, click the **Actions** symbol (orange lightning). Then click **Edit SLA Level**.

- **Add a new SLA level**
  - In the lower right, click **Add SLA Level**.

5 In the **SLA Level Editor**, provide information for the following items:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
<td>Provide a descriptive name to identify the SLA level.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Provide a description of the purpose of the SLA level.</td>
</tr>
<tr>
<td><strong>Milestone</strong></td>
<td>Select the milestone for which the SLA level applies.</td>
</tr>
<tr>
<td><strong>Escalation</strong></td>
<td>Indicate whether or not the escalation is <strong>Late</strong> or <strong>Warn</strong>.</td>
</tr>
<tr>
<td><strong>Late Date</strong></td>
<td>Provide the amount of time that must pass for the SLA to be considered <strong>Late</strong> or <strong>Warn</strong>.</td>
</tr>
<tr>
<td><strong>Use Business Hours</strong></td>
<td>Indicate whether or not you want to associate business hours with this SLA level.</td>
</tr>
<tr>
<td><strong>Business Hours</strong></td>
<td>Select the <strong>Business Hours Configuration</strong> that you want to associate with this SLA level to determine when a service is considered <strong>Late</strong> or <strong>Warn</strong>.</td>
</tr>
</tbody>
</table>

6 Click **Save**.

---

**About configuring the Service Level Agreement (SLA) late date**

When you create or edit SLA levels, you can configure the **Late Date**. SLA Configuration late date is made up of days and minutes. You can enter whole or fractional amounts into the **Days** field, in decimal format. You can also use a combination of days and minutes.

See “Creating and Editing Service Level Agreements (SLAs)” on page 435.

ServiceDesk converts the total **Late Date** into minutes. It converts the days into minutes and then adds the total to the **Minute's** field.

When configuring your SLA Level late dates you have the following options:
You can use your business hours to configure your late dates.

(Check **Use Business Hours**.)

- ServiceDesk calculates the late date into business minutes. It excludes the time that falls in holidays, weekends, off hours, and periods when the SLA is paused.
- When you use the **Using Business Hours** option, one day equals the hours in a business day.
  
  For example, you use a work day from 9:00 A.M. to 5:00 P.M. The business day equals 8 hours or 480 minutes.

You can use a 24 hour day to configure your late dates.

(Do not check **Use Business Hours**.)

- ServiceDesk calculates the late date into minutes. It excludes time periods when the SLA is paused.
- When you do not use the **Using Business Hours** option, one day equals 24 hours or 1,441 minutes.

## Default SLA levels

A Service Level Agreement (SLA) defines the expectations and requirements for delivering a service, including the allowable time frame for the response and resolution.

A default SLA is built in to the Incident Management process. The SLA levels are configured according to the default business hours, which are set up for a nine hour day, 8:00 A.M. - 5:00 P.M. You can edit the default business hours and SLA levels to comply with your organization’s business hours and SLAs.

See “**Configuring business hours**” on page 438.

You manage your SLA levels from the **SLA Levels Configuration** page. To access the page, in the Process Manager portal, click **Admin > Process Automation**. Expand **Incident Management** and click **Service Dashboard**. Then, under **Actions: INCIDENT-MGMT** click **Manage SLA Levels**.

See “**Creating and Editing Service Level Agreements (SLAs)**” on page 435.
Table 38-7  Default SLA levels

<table>
<thead>
<tr>
<th>SLA level</th>
<th>Description</th>
<th>Time frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Response</td>
<td>The initial response levels monitor how much time a worker is allowed to respond to an incident according to its priority. Responses include opening the ticket to set ownership, making comments, or resolving the incident.</td>
<td>The default SLA Levels for initial response are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Emergency: 60 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ High: 120 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Normal: one business day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Low: two business days</td>
</tr>
<tr>
<td>Resolution</td>
<td>The resolution level monitors how much time a worker is allowed to resolve an incident according to its priority.</td>
<td>The default SLA Levels for resolution are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Emergency: one business day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ High: two business days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Normal: five business days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Low: 10 business days</td>
</tr>
</tbody>
</table>

Configuring business hours

Business hours are the hours during which your business is conducted. Typical business hours can vary by location.

You can define multiple sets of business hours and holidays depending on your business locations and your SLA policy, such as the following:

- **Default**
  The default business hours are included with ServiceDesk. The hours are set from Monday through Friday, 8:00 A.M. to 5:00 P.M.
  You can edit the default business hours to meet your organizations requirements. You can define the beginning and ending business hours, holidays, and weekend days.

- **Custom**
  You can create additional custom business hours. For example, if a specific department operates through the weekend while other departments operate during the business week. Or a retail industry might require special project-level business hours.
Video: For more information about configuring business hours, creating SLAs, and rulesets for SLAs, see ServiceDesk Configuration: SLA Framework Overview on Symantec Connect.

To configure business hours:

1. In the Process Manager, go to Admin > Data > Business Hours.

2. On the Business Hours page, do one of the following:
   - Modify the Default Business Hours configuration. In the Default Business Hours row, click the Action symbol (orange lightning), and then click Edit.
   - Create a custom Business Hours configuration. Click the Add symbol (green plus sign).

3. On the Business Hours Configuration page, provide information for the following items:
   - Name: Provide a descriptive name that indicates the purpose of the Business Hours Configuration. For example, U.S. East Sales Team Extended Business Hours.
   - Begin Business Hours: Provide the time of day when the business hours begin.
   - End Business Hours: Provide the time of day when the business hours end.
   - Holidays: In the Date field, enter the date of a holiday that is included in these Business Hours. In the Description field, enter a description of the holiday and click Add Holiday. Note that holidays are excluded from the business hours. Repeat this process for all of the holidays that apply to this Business Hours Configuration.
   - Weekends: Select any days which should be excluded from the Business Hours Configuration.

4. Click Save.

See “Creating and Editing Service Level Agreements (SLAs)” on page 435.
About configuring Data Mapping Routing Tables

The Incident Management process lets you configure data mapping routing tables so that you can route incidents by specific classifications or by specific locations. These tables reduce the number of routing rules that you need to create.

For example, you have several classifications that you want routed to specific service queues. You can configure the Routing Table: Classification to contain all the necessary classifications and which service queues to assign them. Then you can create one rule to route incidents by classification. In this rule, you can use the classification Routing Table to route the incidents with those specific classifications to the proper service queues.

You can configure these routing tables in the Process Manager portal. Click Admin > Process Automation, expand Incident Management, and click Service Dashboard. Under Actions: INCIDENT MGMT, click Manage Data Mapping.

Warning: The Data Mapping Routing Tables' editing process lets you delete data mapping records from the Impact/Urgency Matrix, Routing Table: Classification, and Routing Table: Location tables after they are used in your automation rules. Deleting a data mapping record that an automation rules relies on to execute, causes the rule to error out.

Video: For more information about configuring the Data Mapping Routing Tables, see ServiceDesk Configuration: Data Mapping and Routing Rules on Symantec Connect.

About incident types

You can use incident types to indicate the general nature of an incident. When support technicians use the advanced incident form to submit an incident, they can provide an incident type. An incident type is not required to submit an incident.

The incident type can be modified anytime an incident is worked. However, if an incident type has not been provided, the support technician must provide an incident type when the incident is resolved.

ServiceDesk contains a set of predefined incident types that are ready to use. If necessary, you can add to or delete the default incident types. You can edit the incident types in the Process Manager portal on the Application Properties page.

The incident type lets you select a type that best indicates the general nature of the incident.

The default incident types are as follows:
How To
Break Fix
Add or Install
Change or Move
Backup
Authorize or Approve
Delete or Remove
Request

See “Creating and deleting incident types” on page 441.

Creating and deleting incident types

ServiceDesk contains a set of predefined incident types that you can use to identify the general nature of an incident. If necessary, you can create your own incident types to use. You can also delete incident types.

See “About incident types” on page 440.

As a best practice, do not delete incident types after they are used in your incidents.

To create or delete incident types

1. In the Process Manager portal, click Admin > Data > Application Properties.
3. At the far right of the ServiceDeskSettings title bar, click the Actions symbol (orange lightning), and then click Edit Values.
4. In the Edit Profile Definition Instance dialog box, scroll down to Incident Type, and under the list of incident types, click Edit.
5. In the dialog box that appears, take any of the following actions:
   - To create an incident type: In the field at the bottom of the dialog box, type the new incident type, and then click Add.
   - To delete an incident type: To the right of the incident type, Click the Delete symbol (a red X).
6. When you finish editing the incident types, click Save.
7. In the Edit Profile Definition Instance dialog box, click Save.
About the Service Catalog and service items

The Service Catalog is a Web part that appears on several Process Manager portal pages and that lets users select service items. A service item automates the routine actions that are performed in ServiceDesk. Service items are available for both process workers and users.

The service items are organized in categories, which appear in a tree view in the Service Catalog. You can control the use of the service items by setting permissions on a category or on individual items.

The Service Catalog contains many predefined service items, which can be used to initiate some of the ServiceDesk processes. For example, the default service items are used to submit an incident, submit a knowledge base request, and create a problem ticket.

Users who submit incidents can first search the Service Catalog for any self-service items that help them resolve the incident on their own. The self-service items can reduce incident submissions and reduce the amount time that support workers spend resolving incidents. During the incident submission process, users can search the Service Catalog for any items that can help them solve the issue on their own. A support technician can resolve an incident by suggesting a self-serve item.

See “About the Active Directory self-service catalog” on page 121.

Migrating data from ServiceDesk 7.1 SP2

You can leverage some data from ServiceDesk 7.1 SP2 in ServiceDesk 7.5.

**Note:** Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See “Configuring ServiceDesk” on page 423.

You cannot migrate the following data:

- Open process data
- Active process data

You can migrate the following ticket types:

- Closed Incident Management tickets
- Closed Change Management tickets
Migrating data from ServiceDesk 7.1 SP1

You can leverage some data from ServiceDesk 7.1 SP1 in ServiceDesk 7.5.

---

**Note:** Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See “Configuring ServiceDesk” on page 423.

You cannot migrate the following data:

- Open process data
- Active process data

You can migrate the following ticket types:

- Closed Incident Management tickets
- Closed Change Management tickets
- Close Problem Management tickets
- Closed knowledge base submission tickets
- End User Surveys
- User-defined processes

You can access this historical ticket data from ServiceDesk 7.5 for reporting purposes.
For instructions on how to migrate this data and to access to the migration scripts, see the article Migrate existing closed ServiceDesk 7.0 MR2, 7.1 SP1, and 7.1 SP2 tickets to ServiceDesk 7.5.

See “About migrating data to ServiceDesk 7.5” on page 430.

Migrating data from ServiceDesk 7.0 MR2

You can leverage some data from ServiceDesk 7.0 MR2 in ServiceDesk 7.5.

Note: Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See “Configuring ServiceDesk” on page 423.

You cannot migrate the following data:
- Open process data
- Active process data

You can migrate the following ticket types:
- Closed Incident Management tickets
- Closed Change Management tickets
- Close Problem Management tickets
- Closed knowledge base submission tickets
- End User Surveys
- User-defined processes

You can access this historical ticket data from ServiceDesk 7.5 for reporting purposes.

For instructions on how to migrate this data and to access to the migration scripts, see the article Migrate existing closed ServiceDesk 7.0 MR2, 7.1 SP1, and 7.1 SP2 tickets to ServiceDesk 7.5.

See “About migrating data to ServiceDesk 7.5” on page 430.

About migrating data from Helpdesk Solution 6.x

You can leverage specific data from Helpdesk Solution 6.x in ServiceDesk. You can migrate your categories and knowledge base contents. You can link your
Helpdesk Solution incidents to corresponding incident tasks in ServiceDesk. You can then work these incidents in ServiceDesk. You use the Helpdesk Solution migration links in the Service Catalog to migrate Helpdesk Solution data to ServiceDesk. When migrating data from Helpdesk Solution to ServiceDesk, you must keep both environments operational.

**Note:** Symantec ServiceDesk replaces the functionality of Helpdesk Solution 6.x and earlier. ServiceDesk does not upgrade or install over Helpdesk Solution. ServiceDesk is installed on a different server and uses different databases.

You use the Helpdesk Solution migration links in the Service Catalog to migrate Helpdesk Solution data to ServiceDesk. When migrating data from Helpdesk Solution to ServiceDesk, you must keep both environments operational.

Not all data is supported for migration. The following table includes the data items that can be migrated and links to instructions on how to migrate each item.

**Table 38-8** The Helpdesk Solution 6.x data that ServiceDesk can use

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helpdesk Solution incidents</td>
<td>Incidents cannot be directly migrated to the ServiceDesk server. However, each Helpdesk Solution incident can be linked to a new, corresponding incident task in ServiceDesk. You can see and work those incidents in the ServiceDesk portal, but their data always remains on the Helpdesk Solution server. Best practice is to stop entering new incidents into Helpdesk Solution after the ServiceDesk system is operational and the incident migration is performed.</td>
</tr>
<tr>
<td>Helpdesk Solution categories</td>
<td>The categories are migrated from Helpdesk Solution to ServiceDesk.</td>
</tr>
<tr>
<td>Helpdesk Solution knowledge base contents</td>
<td>The knowledge base (KB) articles are migrated from Helpdesk Solution to ServiceDesk.</td>
</tr>
</tbody>
</table>

See “About migrating data to ServiceDesk 7.5” on page 430.
Managing security, users, roles, groups, and permissions

This chapter includes the following topics:

- About ServiceDesk security and permissions
- About group-level permissions
- About ServiceDesk authentication
- About adding users from Active Directory
- About adding groups from Active Directory
- Creating a group
- Add Group dialog box
- Editing a group
- Deleting a group
- Adding users to a group
- Adding or removing permissions for groups
- Copying permissions between groups
- Viewing the list of ServiceDesk permissions
- Viewing the permissions for a group
- Creating an organizational unit
About ServiceDesk security and permissions

ServiceDesk manages access to the Process Manager portal through native authentication or Active Directory authentication.

See “About ServiceDesk authentication” on page 450.

ServiceDesk provides a high level of security within the Process Manager portal through the use of users, groups, organizational units, and permissions. The ServiceDesk permissions control all the views and possible actions in the Process Manager portal.

For example, permissions can grant or deny access to certain functions within ServiceDesk. Permissions can grant the ability to create users, and they can deny access to view and edit articles in the knowledge base.

The ServiceDesk permissions are hierarchical. The permission that is applied at the most specific level takes precedence. For example, a group is denied access to view a knowledge base article. However, a specific user within that group has permission to view the article. In this case, the user’s specific permission overrides the group setting, and the user is able to view the article.

Table 39-1  ServiceDesk permissions hierarchy

<table>
<thead>
<tr>
<th>Permissions level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Any user of the portal who can log on. Users can have permissions assigned to them. User can also inherit permissions from the groups and organizational units to which they belong.</td>
</tr>
</tbody>
</table>
Table 39-1  ServiceDesk permissions hierarchy (continued)

<table>
<thead>
<tr>
<th>Permissions level</th>
<th>Description</th>
</tr>
</thead>
</table>
| Group             | A collection of users.  
|                   | For example, the Support group might contain all your support technicians. The KB Editors group might contain all the people who can review and edit knowledge base articles. Users can be members of multiple groups.  
|                   | ServiceDesk permissions are almost always granted at the group level rather than at the user level.  
|                   | See “About group-level permissions” on page 449.  
|                   | See “Default ServiceDesk user groups” on page 539. |
| Permission        | Permissions control the access to and use of the Process Manager portal. What users can view and what actions they can perform are based on permissions.  
|                   | For example, permissions may grant access to certain functions within ServiceDesk, such as the ability to create users. Or permissions may grant or deny access to view and edit articles in the knowledge base. Access to everything in ServiceDesk is controlled through permissions. |
| Organizational unit | A collection of users or groups.  
|                   | An organizational unit is generally a very large group. For example, an organizational unit may be a department, office, or division of an organization.  
|                   | The ServiceDesk organizational units do not correspond to the Active Directory organization units. |

About group-level permissions

Groups are collections of ServiceDesk users. The use of groups lets you assign permissions more efficiently and helps simplify the ongoing administration of ServiceDesk permissions. Instead of assigning permissions to each user individually, you can specify the permissions for a group. The permissions for a group are valid for each user who is a member of that group. ServiceDesk permissions are almost always granted at the group level rather than at the user level.

When you apply permissions to groups, you do not have to edit the permission settings for the individual users. The permissions changes that you make at the group level are updated for every user who is a member of that group.

You can use the default groups that are provided with ServiceDesk, create new groups, or import groups from Active Directory.
For more information, see the lists of default permissions in ServiceDesk in the Symantec™ ServiceDesk 7.5 User Guide.
See “Default ServiceDesk permissions by category” on page 533.
See “Default ServiceDesk user groups” on page 539.
See “Creating a group” on page 452.

About ServiceDesk authentication

The authentication method can be defined in the Process Manager Active Directory Settings section in the Process Manager portal on the Master Settings page. You can use native authentication or Active Directory (AD) authentication.

See “Master Settings: Process Manager Active Directory Settings section” on page 531.

Table 39-2  Authentication methods for ServiceDesk users

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native authentication</td>
<td>With native authentication, users are authenticated against the Process Manager database. This authentication method requires that you create user accounts in ServiceDesk.</td>
</tr>
<tr>
<td>Active Directory authentication</td>
<td>With Active Directory authentication, a mixed mode authentication is used. Active Directory users are authenticated against Active Directory. Any users who are not found in Active Directory are authenticated against the Process Manager database (native authentication). When Active Directory authentication is selected, the Active Directory users and groups are imported to ServiceDesk during synchronizations. The imported users and groups are stored in the Process Manager database. However, Active Directory passwords and other sensitive information are not stored in the Process Manager database.</td>
</tr>
</tbody>
</table>

See “About Active Directory synchronization” on page 466.
You can add additional Active Directory server connections or edit the settings for an existing server connection. You manage the Active Directory server connections in Workflow Explorer.

See “Managing Active Directory server connections” on page 469.
After you add an Active Directory server connection, you can add sync profiles. You can use the sync profiles to target the entire domain, organizational units and groups on the Active Directory server, and specific LDAP queries. These options are available on the Active Directory Sync Profiles page, which is accessed from the Admin menu.

See “Managing Active Directory sync profiles” on page 483.
See “Configuring Active Directory sync profiles” on page 467.
About adding users from Active Directory

When your organization uses Active Directory (AD) authentication, the Active Directory users and groups are imported to ServiceDesk during Active Directory synchronizations. The ServiceDesk users and groups are stored in the Process Manager database.

See “About ServiceDesk authentication” on page 450.

Table 39-3 How Active Directory users can be added to ServiceDesk

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>During the synchronization between ServiceDesk and Active Directory</td>
<td>You can schedule full or update ServiceDesk synchronizes with Active Directory to obtain new and updated users and groups from Active Directory. During synchronization, the user and the group data from Active Directory overwrites the user and the group data that is in ServiceDesk. See “About Active Directory synchronization” on page 466.</td>
</tr>
<tr>
<td>Manually</td>
<td>If a new user needs to access ServiceDesk between synchronization, you can add the user manually from Active Directory. See “Adding new ServiceDesk users from Active Directory manually” on page 460.</td>
</tr>
<tr>
<td>Automatically when a user logs on</td>
<td>This method is available only if the option <strong>Auto Create Users on Initial Login</strong> is selected for the Active Directory server. Users in Active Directory that have not been imported into ServiceDesk can be added to ServiceDesk when they log on to the Process Manager portal. When such a user enters their logon credentials, ServiceDesk checks the credentials against the Process Manager database. If the credentials are not there, ServiceDesk checks the credentials against Active Directory and adds the user to ServiceDesk. See “Adding Active Directory sync profiles” on page 486.</td>
</tr>
</tbody>
</table>

See “About adding groups from Active Directory” on page 451.

About adding groups from Active Directory

When your organization uses Active Directory (AD) authentication, the Active Directory users and groups are imported to ServiceDesk during sync profile synchronizations. When Active Directory users are imported to ServiceDesk, they
retain their group associations from Active Directory. The ServiceDesk users and groups are stored in the Process Manager database.

See “About ServiceDesk authentication” on page 450.

Table 39-4  How Active Directory groups can be added to ServiceDesk

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>During manually run synchronizations</td>
<td>During the installation of the ServiceDesk application software, the users and groups from your Active Directory are imported to ServiceDesk. See “Methods for synchronizing Active Directory sync profiles” on page 493.</td>
</tr>
<tr>
<td></td>
<td>You can create sync schedules for when ServiceDesk synchronizes with Active Directory to obtain new and updated users and groups from Active Directory. During synchronization, the user and the group data from Active Directory overwrites the user and the group data that is in ServiceDesk. See “About Active Directory synchronization” on page 466.</td>
</tr>
</tbody>
</table>

When you import your groups from Active Directory, your Active Directory groups are added with only All Users permissions by default. You must assign additional permissions to those groups after they are imported.

See “Copying permissions between groups” on page 456.

See “About adding users from Active Directory” on page 451.

See “Managing Active Directory sync profiles” on page 483.

Creating a group

Groups are collections of ServiceDesk users. The use of groups lets you assign permissions more efficiently and helps simplify the ongoing administration of ServiceDesk permissions. Instead of assigning permissions to each user individually, you can specify the permissions for a group. The permissions for a group are valid for each user who is a member of that group. ServiceDesk permissions are almost always granted at the group level rather than at the user level.

See “About group-level permissions” on page 449.

An administrator or other user who has the appropriate permissions can create ServiceDesk groups. Groups can also be added by importing them from Active Directory.
See “About adding groups from Active Directory” on page 451.

You can copy permissions from another group and assign them to the new group. If you do not copy the permissions from another group, you must assign the permissions to the new group in a separate task.

See “Adding or removing permissions for groups” on page 456.

See “Copying permissions between groups” on page 456.

**To create a group**

1. In the Process Manager portal, click **Admin > Users > Accounts > List Groups**.
2. On the **List Groups** page, at the upper right of the **All Groups** section, click the **Add Groups** symbol (white page with green plus sign).
3. In the **Add Group** dialog box, perform the following actions:
   - Type the name of the new group.
   - (Optional) Copy permissions from another group.
   - (Optional) Specify the group’s home page.
   - (Optional) Specify the group’s email address

   See “Add Group dialog box” on page 453.

4. Click **Save**.

**Add Group dialog box**

This dialog box lets you add a user group to the Process Manager portal.

See “Creating a group” on page 452.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Name</strong></td>
<td>Lets you type the name of the new group.</td>
</tr>
<tr>
<td></td>
<td>You can use special characters but you cannot enter a name that is already assigned to another group.</td>
</tr>
</tbody>
</table>
### Table 39-5  Options in the Add Group dialog box (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Permissions From Group checkbox</td>
<td>Lets you use another group’s permissions for this group. You can type the name of the other group or click <strong>Pick</strong> to select a group from the Group Picker dialog box. All the permissions from the group that you specify are replicated for the new group. If you do not copy the permissions from another group, you must assign the permissions to the new group in a separate task. See “Adding or removing permissions for groups” on page 456.</td>
</tr>
<tr>
<td>Home Page</td>
<td>Lets you specify the name of the portal page that should appear when users in this group log on to the Process Manager portal.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Lets you type an email address to be used for group-level communications.</td>
</tr>
</tbody>
</table>

### Editing a group

An administrator or other user who has the appropriate permissions can edit ServiceDesk groups.

See “About group-level permissions” on page 449.

See “Creating a group” on page 452.

**To edit a group**

1. In the Process Manager portal, click **Admin > Users > Accounts > List Groups**.
2. On the **List Groups** page, under **All Groups**, select the group whose details you want to edit.
3. In the right pane, at the right of the group’s title bar, click the **Actions** symbol (orange lightning), and then click **Edit**.
4. In the **Edit Group** dialog box, edit the group as necessary.
5. Click **Save**.

### Deleting a group

An administrator or other user who has the appropriate permissions can delete ServiceDesk groups. Note that deleting a group does not delete the users who belong to that group.
Warning: Use caution when deciding to delete a group. If you delete a group that is used in any ServiceDesk processes, you break all the processes in which that group is used. As a best practice, Symantec recommends that you do not delete any groups.

See “About group-level permissions” on page 449.
See “Creating a group” on page 452.

To delete a group
1 In the Process Manager portal, click Admin > Users > Accounts > List Groups.
2 On the List Groups page, under All Groups, at the right of the group’s title bar, click the Actions symbol (orange lightning), and then click Delete
3 In the confirmation dialog box, click OK to confirm the deletion.

Adding users to a group

When you add users to a ServiceDesk group, each user inherits the permissions that are defined for that group. An administrator or other user who has the appropriate permissions can add users to ServiceDesk groups.

See “About group-level permissions” on page 449.
See “Creating a group” on page 452.

To add users to a group
1 In the Process Manager portal, click Admin > Users > Accounts > List Groups.
2 On the List Groups page, under All Groups, select the group to which you want to add users.
3 In the right pane, at the right of the group’s title bar, click the Actions symbol (orange lightning), and then click Add User.
4 In the Add User dialog box, take the following actions:
   ■ In Add user to group, type the user’s email address or click Pick to search for a user.
      See “Picking a user” on page 114.
   ■ (Optional) In Relationship Type, select the type of relationship.
      The relationship type is used if your organization customized ServiceDesk to assign tickets based on user relationships.
   ■ Click Add to add the user to the list at the top of the Add User dialog box.
5 When you finish adding users, in the Add User dialog box, click Close.
Adding or removing permissions for groups

In ServiceDesk, a group’s permissions determine the permissions that are granted to individual ServiceDesk users. When you assign permissions for a group, each user that is a member of that group is granted those permissions.

See “About group-level permissions” on page 449.

An administrator or other user who has the appropriate permissions can add or remove the permissions that are associated with a group.

To add or remove permissions from a group

1. In the Process Manager portal, click Admin > Users > Accounts > List Groups.
2. On the List Groups page, under All Groups, select the group that you want to add or remove the permissions.
3. In the right pane, at the right of the group’s title bar, click the Actions symbol (orange lightning), and then click Permissions.
4. In the Permissions For Group dialog box, take any of the following actions:
   - Select the check box for each permission to assign to this group
   - Uncheck the checkbox for each permission to remove from this group.
   - Click Select All to add all available permissions to a group.
   - Click Unselect All to remove all permissions from a group.
5. Click Save.

Copying permissions between groups

You can copy all the ServiceDesk permissions from one group to another group. Typically, you can import the permissions from another group when you create a new group in the Process Manager portal.

See “About adding groups from Active Directory” on page 451.

The ability to copy permissions between existing groups is useful when you import an Active Directory group. The imported groups are added with only All Users permissions by default and you must assign additional permissions yourself. Copying the permissions from another group eliminates the need to assign the permissions manually.

See “About group-level permissions” on page 449.
An administrator or other user who has the appropriate permissions can add or remove the permissions that are associated with a group.

To copy permissions between groups

1. In the Process Manager portal, click Admin > Users > Accounts > List Groups.
2. On the List Groups page, under All Groups, find the group for which you want to set permissions.
3. At the right of the group’s title bar, click the Actions symbol (orange lightning), and then click Copy Permissions From.
4. On the Copy Permissions From Groups page, in the Group Name field, specify the group from which to copy the permissions.
   You can type the name of the other group or click Pick to select a group from the Group Picker dialog box.
5. Click Save.

Viewing the list of ServiceDesk permissions

In the Process Manager portal, an administrator or other user who has the appropriate permissions can view the ServiceDesk permissions and their descriptions by category.

See “About group-level permissions” on page 449.
See “Default ServiceDesk permissions by category” on page 533.

To view the list of permissions

1. In the Process Manager portal, click Admin > Users > Accounts > List Permissions.
2. On the List Permissions page, under Browse Permissions, select the category of permissions to view.
3. In the right pane, you can view the permissions that are assigned to the selected category, and you can perform several permission-related actions.

Viewing the permissions for a group

An administrator or other user who has the appropriate permissions can view the permissions that are associated with a specific ServiceDesk group. A group’s permissions determine the permissions that are granted to the users who are members of that group. You can view a group’s permissions to discover what the users in that group can do.
Creating an organizational unit

Organizational units are large groups of ServiceDesk users or groups. A typical organizational unit might be a department within a company.

An administrator or other user who has the appropriate permissions can create organizational units.

To create an organizational unit

1. In the Process Manager portal, click Admin > Users > Accounts > List Organizations.
2. On the List Organizations page, at the upper right corner of the page, click the Add Root Organization symbol (a white page with a green plus sign).
3. In the Add Organization dialog box, in the Organization Name field, type a descriptive name for the organization.
   You can use special characters in the name. Duplicate names are not allowed.
4. (Optional) In the Description field, type a description to further identify the organizational unit.
5. Click Save.

Creating a new user

An administrator or other user who has the appropriate permissions can create new ServiceDesk users.

Users can also be added to ServiceDesk through Active Directory.

See “About adding users from Active Directory” on page 451.
Every ServiceDesk user requires permissions to perform any actions in the Process Manager portal. By default, every new user is assigned to the All Users group, which provides general permissions. However, you must assign the user to one or more of the groups that provide the permissions that are appropriate for that user’s role.

See “About group-level permissions” on page 449.

The easiest way to assign groups and permissions to a new user is by cloning them from another user during the user entry. If you do not clone the user information, you must assign the user to groups manually.

See “Adding users to a group” on page 455.

To create a new user

1  In the Process Manager portal, click Admin > Users > Accounts > Manage Users.

2  On the Manage Users page, at the right of the All Users title bar, click the Add User symbol (a person’s head with a green plus sign).

3  In the Add User dialog box, on the Main Information tab, enter the information to identify the user.

4  (Optional) Add additional user information on the following tabs:

   **Clone User**
   Lets you clone groups, permissions, or organizations for this user from an existing user.

   See “Add User dialog box: Clone User tab” on page 460.

   **Process Manager Settings**
   Contains the options for setting the theme, home page, and time zone.

   **Email Settings**
   Lets you add and delete additional email addresses and set the primary email address.

   **Phone Numbers**
   Lets you add phone numbers, along with additional details about the phone numbers, for the user.

   **Messengers ID**
   Lets you add multiple instant messenger IDs for the user, and designate one messenger ID as the primary contact.

   **Profiles**
   Lets you add profile information for the user.

5  In the Add User dialog box, click Save.
Add User dialog box: Clone User tab

This tab lets you clone information from an existing user to a new user, which can speed the creation of the new user. It is especially useful when you need to add several users of the same type.

See “Creating a new user” on page 458.

Table 39-6 Options on the Clone User tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Lets you specify the user to clone. You can type the user's name or click Pick to search for a user. See “Picking a user” on page 114.</td>
</tr>
<tr>
<td>Clone User's Groups</td>
<td>Clones the group settings of this user for the new user.</td>
</tr>
<tr>
<td>Clone User's Permissions</td>
<td>Clones the permissions settings of this user for the new user.</td>
</tr>
<tr>
<td>Clone User's Organization Units</td>
<td>Clones the organization unit settings of this user for the new user.</td>
</tr>
</tbody>
</table>

Adding new ServiceDesk users from Active Directory manually

You can manually add new users to ServiceDesk from Active Directory. Normally, ServiceDesk synchronizes its data with Active Directory on a regular schedule. However, you may want to add new users before the next scheduled update.

The ability to add users from Active Directory is available only if your organization chose the option to use Active Directory authentication.

See “About ServiceDesk authentication” on page 450.

The list of users that appears under Add Active Directory Users is current as of the last synchronization with Active Directory.

Every ServiceDesk user requires permissions to perform any actions in the Process Manager portal. By default, every new user is assigned to the All Users group, which provides general permissions. However, you must assign the user to one or more of the groups that provide the permissions that are appropriate for that user’s role.

See “Adding users to a group” on page 455.
To add new ServiceDesk users from Active Directory manually

1. In the Process Manager portal, click Admin > Users > AD Users.


3. Search for the users to add in one of the following ways:
   - To search for specific users: Type your search criteria in the Name field or Department field and then click Search Users.
   - To search for specific users using advanced search features: Check Advanced Search. Select the criteria by which you want to perform your advanced search and then click Search Users.

4. Under Select Users, select the users that you want to add, and then click Add Users at the bottom of the page.
   - If the list of users consists of multiple pages, you must select the users and click Add Users one page at a time. For example, if you select users on page 2 of the display, click Add Users before you go to page 3 and add users there.

5. When you finish adding users, you can leave the Add Active Directory Users page.

Editing a user account

An administrator or other user who has the appropriate permissions can edit the data for ServiceDesk users. Any of the user information that can be set during the user creation is available for editing.

See “Creating a new user” on page 458.

To edit a user account

1. In the Process Manager portal, click Admin > Users > Accounts > Manage Users.

2. On the Manage Users page, under All Users, scroll to the user whose information you want to edit.

3. At the far right of the user name, click the Actions symbol (orange lightning), and then click Manage User.
4 On the Manage User page, edit the account information that appears on any of the following tabs:

- **Account Info**: Lets you edit the information that identifies the user.
- **Password Settings**: Lets you clone groups, permissions, or organizations for this user from an existing user. See “Add User dialog box: Clone User tab” on page 460.
- **Process Manager Settings**: Contains the options for setting the theme, home page, and time zone.
- **Email Settings**: Lets you add and delete additional email addresses and set the primary email address.
- **Phone Numbers**: Lets you add phone numbers, along with additional details about the phone numbers, for the user.
- **Messengers ID**: Lets you add multiple instant messenger IDs for the user, and designate one messenger ID as the primary contact.
- **Profiles**: Lets you add profile information for the user.

5 When you finish editing the account information, on the Manage User page, click Save.

**Disabling and enabling a user**

An administrator or other user who has the appropriate permissions can disable a user so that the user cannot use ServiceDesk. Disabled users can be enabled so that they can access ServiceDesk again.

If you disable a user who is currently logged onto the Process Manager portal, the user is not locked out of the session. However, a disabled user cannot save any data or navigate to any other pages. Disabled users continue to be listed under the All Users section, but are not indicated as being active.

Before you disable a user who has process ticket assignments, reassign those tickets.

See “Reassigning incidents, problems, or change tickets” on page 289.
To disable or enable a user

1. In the Process Manager portal, click Admin > Users > Accounts > Manage Users.

2. On the Manage Users page, under All Users, scroll to the user that you want to edit.

3. At the far right of the user name, click the Actions symbol (orange lightning), and then click Enable/Disable.

4. In the Enable/Disable User dialog box, click Disable This User or Enable This User, whichever is appropriate.
Managing security, users, roles, groups, and permissions

Disabling and enabling a user
Managing the Active Directory connections

This chapter includes the following topics:

■ About Active Directory synchronization
■ Configuring Active Directory sync profiles
■ Managing Active Directory server connections
■ Adding Active Directory server connections
■ Editing the settings of an Active Directory server connection
■ Deleting an Active Directory server connection
■ Selecting Active Directory as the authentication method
■ Testing an Active Directory server connection
■ New AD Connections Profile and Edit AD connection settings dialog boxes
■ Managing Active Directory sync profile schedules
■ Adding Active Directory sync profile schedules
■ Editing an Active Directory sync profile schedule
■ Deleting an Active Directory sync profile schedule
■ Managing Active Directory sync profiles
■ Adding Active Directory sync profiles
■ Editing an Active Directory sync profile
About Active Directory synchronization

You can choose to use Active Directory authentication as its authentication method for ServiceDesk. You can synchronize ServiceDesk with Active Directory. This synchronization lets you add and update Active Directory users, organizational units, and groups in the Process Manager database. During synchronization, data from Active Directory updates data that are in the Process Manager database. The Process Manager database does not store sensitive information such as passwords.

You add Active Directory synchronization profiles, after you connect ServiceDesk to an Active Directory server. These synchronization profiles let you import the entire Active Directory domain or specific organizational units and groups. These units and groups are not the same as the organizational groups that ServiceDesk uses to categorize users.

The communication between ServiceDesk and Active Directory occurs by means of LDAP queries against the Active Directory database. ServiceDesk provides several ways to initiate the synchronization.

The Active Directory synchronization performs the following actions:

- Imports and updates the Active Directory users in ServiceDesk
- Imports and updates the Active Directory organizational units and groups in ServiceDesk

When you use Active Directory authentication, you still can create user accounts and organizational units in ServiceDesk. For example, you might create an account for a short-term contractor who you do not want to add to Active Directory.

After you install ServiceDesk, you can set up your Active Directory server connections, synchronization schedules, and sync profiles. ServiceDesk can then synchronize with Active Directory to obtain new and updated users and groups.
Active Directory synchronization affects the changes and deletions of ServiceDesk user accounts as follows:

- When you delete a user from Active Directory, the user is not deleted from ServiceDesk. The user is only disabled in ServiceDesk.
- Any changes that you make to a user in ServiceDesk are overwritten during the next synchronization.

If you edit user information or delete a user in Active Directory instead, the information is updated in ServiceDesk during the next synchronization. This rule applies to the users group, manager, and organizational unit information.

See “About ServiceDesk authentication” on page 450.

See “Methods for synchronizing Active Directory sync profiles” on page 493.

See “About adding users from Active Directory” on page 451.

See “About adding groups from Active Directory” on page 451.

See “Creating a new user” on page 458.

See “Creating an organizational unit” on page 458.

See “Configuring Active Directory sync profiles” on page 467.

### Configuring Active Directory sync profiles

If your organization chooses to use Active Directory authentication as its authentication method for ServiceDesk, you can configure Active Directory sync profiles. You can use these sync profiles to target an entire Active Directory domain, organizational units and groups, or specific LDAP queries.

After you configure your Active Directory sync profiles, ServiceDesk can synchronize these sync profiles with Active Directory. During synchronization, ServiceDesk can obtain new and updated users and organizational units and groups.

After you configure your Active Directory sync profiles, you can add, edit, or delete your Active Directory server connections, sync profile schedules, and sync profiles. You can manage your Active Directory server connections in Workflow Explorer. You can manage your Active Directory sync profile schedules and sync profiles in ServiceDesk.

See “About Active Directory synchronization” on page 466.

See “Methods for synchronizing Active Directory sync profiles” on page 493.

See “Managing Active Directory server connections” on page 469.

See “Managing Active Directory sync profile schedules” on page 478.
See “Managing Active Directory sync profiles” on page 483.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Add Active Directory server connections.</td>
<td>In Workflow Explorer, you can connect ServiceDesk with your Active Directory servers. See “Adding Active Directory server connections” on page 470.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Active Directory Authentication</strong> as the authentication type.</td>
<td>In ServiceDesk, you can select Active Directory as your authentication method. See “Selecting Active Directory as the authentication method” on page 475. Note that after you select Active Directory as your authentication method, you do not need to do it again. Active Directory is now your authentication method.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add automatic sync profile schedules.</td>
<td>In ServiceDesk, you can add automatic Active Directory sync profile schedules. See “Adding Active Directory sync profile schedules” on page 479. When adding your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations: ■ Update synchronization ■ Full synchronization</td>
</tr>
<tr>
<td>Step 4</td>
<td>Add Active Directory sync profiles.</td>
<td>In ServiceDesk, you can add sync profiles for your Active Directory server connections. See “Adding Active Directory sync profiles” on page 486.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) Test an Active Directory server connection.</td>
<td>In ServiceDesk, you can test each ServiceDesk to Active Directory server connection. See “Testing an Active Directory server connection” on page 476.</td>
</tr>
</tbody>
</table>
### Table 40-1 Process for configuring an Active Directory sync profile (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>(Optional) Manually perform a full synchronization for an Active Directory sync profile.</td>
<td>In ServiceDesk, you can manually run full synchronization for the Active Directory sync profiles that you specify. See “Running a full Active Directory sync profile synchronization manually” on page 495.</td>
</tr>
<tr>
<td>Step 7</td>
<td>(Optional) Manually perform a full Active Directory synchronization for all Active Directory sync profiles.</td>
<td>In ServiceDesk, you can manually perform full synchronization for all your Active Directory sync profiles. See “Synchronizing all Active Directory sync profiles manually” on page 496.</td>
</tr>
<tr>
<td>Step 8</td>
<td>(Optional) Check the status of an Active Directory sync profile synchronization.</td>
<td>In ServiceDesk, you can view information about the users and organizational units and groups that are synchronized. You can also view the status of the Active Directory sync profile synchronization. See “Checking the status of an Active Directory sync profile synchronization” on page 497.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Assign permissions to your imported groups.</td>
<td>By default, the imported groups are added to the All Users group. Therefore your imported groups have All User permissions. You must assign your Active Directory groups additional permissions. See “Copying permissions between groups” on page 456.</td>
</tr>
</tbody>
</table>

---

### Managing Active Directory server connections

In Workflow Explorer, you can add one or more Active Directory server connections. After you add your Active Directory server connections, you may need to edit the settings of an Active Directory server connection. You may also need to delete an Active Directory server connection. In Workflow Explorer, you can manage your Active Directory server connections.

After you add your Active Directory server connections, you can then add sync profile schedules and sync profiles for them. You can use these sync profile
schedules to schedule update and full synchronizations with Active Directory. You can use these sync profiles to import data from Active Directory to the Process Manager database. You can import the entire domain, organizational units and groups on the Active Directory server, or for specific LDAP queries. In ServiceDesk, you can manage these sync profile schedules and sync profiles.

See “Managing Active Directory sync profile schedules” on page 478.

See “Managing Active Directory sync profiles” on page 483.

Table 40-2 Process for managing Active Directory server connections

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Add Active Directory server connections.</td>
<td>In Workflow Explorer, you can connect ServiceDesk with your Active Directory servers. See “Adding Active Directory server connections” on page 470.</td>
</tr>
<tr>
<td>Step 2</td>
<td>(Optional) Edit the settings of an Active Directory server connection.</td>
<td>In Workflow Explorer, you can edit the settings of an Active Directory server connection. See “Editing the settings of an Active Directory server connection” on page 473.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) Delete an Active Directory connection.</td>
<td>In Workflow Explorer, you can delete an Active Directory server connection. See “Deleting an Active Directory server connection” on page 475.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Test an Active Directory server connection.</td>
<td>In ServiceDesk, you can test the Active Directory server connection. See “Testing an Active Directory server connection” on page 476. Note that you can only test an Active Directory server connection after you add a sync profile for that server connection.</td>
</tr>
</tbody>
</table>

Adding Active Directory server connections

If your organization uses Active Directory authentication as its authentication method for ServiceDesk, you may need to add one or more Active Directory server connections. In Workflow Explorer, you can add Active Directory server
connections at any time. For example, you might need to connect to an Active
Directory server in a new location.

See “Configuring Active Directory sync profiles” on page 467.

See “Managing Active Directory server connections” on page 469.

Before you add an Active Directory server connection, you need to collect the
following information:

■ NETBIOS domain name of the Active Directory server

■ Credentials for Active Directory
  The user name and password of an account that can connect to the Active
  Directory and retrieve user information

■ Domain controller host name or IP address

**To add Active Directory server connections**

1. On the ServiceDesk server on the Windows Start menu, click Start > All
   Programs > Symantec > Workflow Designer > Tools > Workflow Explorer.

2. On the Symantec Workflow Explorer page in the toolbar at the top of the
   page, click Credentials.

3. In the left pane, click Active Directory.

4. In the right pane, click Add New.
5 In the **New AD Connection Profile** dialog box, type the following information for your Active Directory connection:

- **Domain Controller**: Lets you type the IP address or host name of your domain controller.
- **Domain**: Lets you type the NETBIOS domain name of your Active Directory. The correct format is as follows: `<MyDom>`
  
  Do not use the fully qualified domain name unless it is necessary. For example, your organization might not allow NETBIOS in your network. If you use the fully qualified domain name, the option to create a ServiceDesk user account automatically does not work.

  The format for the fully qualified domain name is as follows:
  
  `<MyDomain.com>`

- **Username**
- **Password**: Lets you specify the credentials of the account that can connect to the Active Directory and retrieve user and group information.

  You can specify any user in your domain whose privileges are high enough to retrieve users and groups from Active Directory.

  For security purposes, you must retype the password every time you add or edit an Active Directory server connection.

- **Default Timeout**: Lets you specify the parameters for the default timeout.
  
  Note that 20000 is the default setting.

- **Name**
- **Is Default check box**: Lets you specify a name for the Active Directory connection profile.

  Lets you choose whether to use the Active Directory connection profile as the default profile.

6 When you are finished, click **OK**.

7 Repeat the steps in this procedure to add additional server connections.

8 (Optional) If you have not selected Active Directory as your authentication method, then you need to select **Active Directory Authentication** as your authentication method.

  See “**Selecting Active Directory as the authentication method**” on page 475.
To Test your Active Directory server connection

1. In the right pane, select the Active Directory server connection that you want to test.
2. Click Test.
3. (Optional) If the test fails, recheck your Active Directory setting by doing the following:
   - In the right pane, select the Active Directory server connection that failed.
   - Click Edit.
   - In the Edit AD connection settings dialog box, edit the settings as needed and then click OK.
   - Test the Active Directory server connection. See Step 1.
4. In the AD connection succeeded dialog box, click OK.

Editing the settings of an Active Directory server connection

After you add your Active Directory server connections, you may need to edit the settings of an Active Directory server connection. In Workflow Explorer, you can edit any of the Active Directory servers to ServiceDesk connections. For example, if you need to change the user name and password for an Active Directory server connection, you can change it.

If you need to convert native users to Active Directory users, you can do so in ProcessManager Active Directory Settings. These settings appear in the Process Manager portal on the Master Settings page.

See “Managing Active Directory server connections” on page 469.

See “Master Settings: Process Manager Active Directory Settings section” on page 531.

To edit the settings of an Active Directory server connection

1. On the ServiceDesk server on the Windows Start menu, click Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer.
2. On the Symantec Workflow Explorer page in the toolbar at the top of the page, click Credentials.
3. In the left pane, click Active Directory.
4. In the right pane, select the Active Directory server connection profile that you want to edit.
5 In the right pane, click **Edit**.

6 In the **Edit AD connection settings** dialog box, edit the following settings as needed:

- **Domain Controller**
  - Lets you type the IP address or host name of your domain controller.

- **Domain**
  - Lets you type the NETBIOS domain name of your Active Directory. The correct format is as follows:
    - `<MyDomain>`
  - Do not use the fully qualified domain name unless it is necessary. For example, your organization might not allow NETBIOS in your network. If you use the fully qualified domain name, the option to create a ServiceDesk user account automatically does not work.
  - The format for the fully qualified domain name is as follows:
    - `<MyDomain.com>`

- **Username**
  - Lets you specify the credentials of the account that can connect to the Active Directory and retrieve user and group information.

- **Password**
  - You can specify any user in your domain whose privileges are high enough to retrieve users and groups from Active Directory.
  - For security purposes, you must retype the password every time you add or edit an Active Directory server connection.

- **Default Timeout**
  - Lets you specify the parameters for the default timeout.
    - Note that 20000 is the default setting.

- **Name**
  - Lets you specify a name for the Active Directory connection profile.

- **Is Default** check box
  - Lets you choose whether to use the Active Directory connection profile as the default profile.

7 When you are finished, click **OK**.

8 Close Workflow Explorer.

9 (Optional) After you edit the settings of an Active Directory server connection, you may want to test the server connection.

See “**Testing an Active Directory server connection**” on page 476.
Deleting an Active Directory server connection

After you add your Active Directory server connections, you may need to delete an Active Directory server connection. For example, you may need to replace your current Active Directory server computer. In Workflow Explorer, you can delete an Active Directory server connection.

**Note:** You cannot delete an Active Directory server connection that any of your Active Directory sync profiles currently use to import data. Before you can delete that Active Directory server connection, you must perform one of the following actions: Delete all the sync profiles for that Active Directory server connection, or switch all the sync profiles to another server connection.

See “Managing Active Directory sync profiles” on page 483.

**To Delete an Active Directory server connection**

1. On the ServiceDesk server on the Windows Start menu, click **Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.
2. On the Symantec Workflow Explorer page in the toolbar at the top of the page, click **Credentials**.
3. In the left pane, click **Active Directory**.
4. In the right pane, select the Active Directory server connection profile that you want to delete.
5. In the right pane, click **Delete**.
6. In the confirmation message dialog box, click **OK**.

See “Managing Active Directory server connections” on page 469.

Selecting Active Directory as the authentication method

If you want to use Active Directory as your authentication method for ServiceDesk, you must first add an Active Directory server connection. Then, you can select Active Directory as your authentication method in the Process Manager portal on the **Master Settings** page.

**Note:** You do not need to reselect Active Directory as your authentication method to add additional Active Directory server connections or sync profiles.
After you select Active Directory as your authentication method, you can add Active Directory sync profiles for your Active Directory server connections. See “Configuring Active Directory sync profiles” on page 467.

See “Adding Active Directory server connections” on page 470.

To select Active Directory as the authentication method

1. In the Process Manager portal, click Admin > Portal > Master Settings.
2. On the Master Settings page, expand the Process Manager Active Directory Settings section.
4. (Optional) In the Process Manager Active Directory Settings section, select any of the other options that are appropriate for your environment. You can also type information for the Active Directory users that you do not want to import to ServiceDesk. See “Master Settings: Process Manager Active Directory Settings section” on page 531.
5. Scroll down to the bottom of the Master Settings page and click Save.

Testing an Active Directory server connection

Testing an Active Directory server connection

After you configure your Active Directory sync profiles, you can test any of your Active Directory server connections. For example, you may want to test the server connection before you run a manual synchronization or after an automatic synchronization fails. In ServiceDesk, you can test the connection on the Active Directory Sync Profiles page.

Note: If the connection test fails, report it to the administrator who manages your Active Directory servers.

See “Configuring Active Directory sync profiles” on page 467.
See “Managing Active Directory server connections” on page 469.
See “Managing Active Directory sync profiles” on page 483.
To test an Active Directory server connection

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.

2. On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profiles**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Test AD Server**.

3. After you view the message that reports the success or failure of the connection, you can close the message dialog box.

New AD Connections Profile and Edit AD connection settings dialog boxes

If your organization chooses to use Active Directory authentication as its authentication method for ServiceDesk, you need to add Active Directory server connections. You may also need to edit the settings for an Active Directory connection. During the addition or the edit of a server connection, you open the New AD Connection Profile or the Edit AD connection settings dialog box. These dialog boxes let you add information for an Active Directory server connection or edit an existing one.

See “Adding Active Directory server connections” on page 470.

See “Editing the settings of an Active Directory server connection” on page 473.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller</td>
<td>Lets you type the IP address or host name of your domain controller.</td>
</tr>
<tr>
<td>Domain</td>
<td>Lets you type the NETBIOS domain name of your Active Directory. The correct format is as follows: &lt;MyDom&gt;</td>
</tr>
<tr>
<td></td>
<td>Do not use the fully qualified domain name unless it is necessary. For example, your organization might not allow NETBIOS in your network.</td>
</tr>
<tr>
<td></td>
<td>If you use the fully qualified domain name, the option to create a ServiceDesk user account automatically does not work. The format for the fully qualified domain name is as follows: &lt;MyDomain.com&gt;</td>
</tr>
</tbody>
</table>
Table 40-3 Options on the New AD Connection Profile and Edit AD connection settings dialog boxes (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Lets you specify the credentials of the account that can connect to the Active Directory and retrieve user and group information. You can specify any user in your domain whose privileges are high enough to retrieve users and groups from Active Directory. For security purposes, you must retype the password every time you add or edit an Active Directory server connection.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Default Timeout</td>
<td>Lets you specify the parameters for the default timeout. <strong>Note:</strong> 20000 is the default setting for Default Timeout.</td>
</tr>
<tr>
<td>Name</td>
<td>Lets you specify a name for the Active Directory connection profile.</td>
</tr>
<tr>
<td>Is Default check box</td>
<td>Lets you choose whether to use the Active Directory connection profile as the default profile.</td>
</tr>
</tbody>
</table>

Managing Active Directory sync profile schedules

In ServiceDesk, you can add Active Directory sync profile schedules. These schedules let you schedule automatic update and full synchronizations between your sync profiles and the Active Directory servers to which they are connected. After you add your Active Directory sync profile schedules, you may need to edit a sync profile schedule. You may also need to delete a sync profile schedule. In ServiceDesk, you can manage your Active Directory sync profile schedules.

See “Managing Active Directory sync profiles” on page 483.
### Table 40-4 Process for managing Active Directory sync profile schedules

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Add automatic synchronization schedules.            | In ServiceDesk, you can add automatic Active Directory sync profile schedules. See “Adding Active Directory sync profile schedules” on page 479. When adding or editing your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations:  
  - Update synchronization  
  - Full synchronization |
| Step 2 | (Optional) Edit automatic synchronization schedules. | In ServiceDesk, you can edit an automatic Active Directory sync profile schedule. See “Editing an Active Directory sync profile schedule” on page 481. |
| Step 3 | (Optional) Delete an automatic synchronization schedule. | In ServiceDesk, you can delete an automatic Active Directory sync profile schedule. See “Deleting an Active Directory sync profile schedule” on page 482. |

---

**Adding Active Directory sync profile schedules**

In ServiceDesk, you can add Active Directory sync profile schedules so that they are available when adding your Active Directory sync profiles.

For example, you add an Active Directory server connection. You know the organizational units and groups that you want your Active Directory sync profiles to import from Active Directory to the Process Manager database. Now, you need to add Active Directory sync profile schedules. After you add these schedules, you can use them to schedule update and full synchronization when adding these Active Directory sync profiles.
Note: Name your Active Directory sync profile schedules so that you can easily associate them with the sync profiles to which you want to assign them. If you ever need to edit the synchronization schedules for any of your Active Directory sync profiles, you must do so on the Active Directory Sync Profile Schedule page. You cannot edit the schedule while editing an Active Directory sync profile; you can only select a different schedule or add a new one.

After you add your Active Directory sync profile schedules, they appear in the drop-down lists for the Schedule For Full Sync Profile or Schedule For Update Sync Profile fields. These fields appear in the Add Schedule for Active Directory Server dialog box. This dialog box appears during the addition of an Active Directory sync profile.

The Schedule For Update Sync Profile field lets you schedule an automatic synchronization that only updates the changes that have been made to Active Directory since the last synchronization. The Schedule For Full Sync Profile field lets you schedule an automatic synchronization that updates the entire Active Directory domain or entire organizational units or groups.

See “Configuring Active Directory sync profiles” on page 467.
See “Managing Active Directory sync profiles” on page 483.
See “Managing Active Directory sync profile schedules” on page 478.
See “Methods for synchronizing Active Directory sync profiles” on page 493.

To add Active Directory sync profile schedules

1. In the Process Manager portal, click Admin > Active Directory > Sync Profile Schedule.

2. On the Sync Profile Schedule page, at the far right of the title bar, click the Add Sync Profile Schedule symbol (green plus sign).

3. In the Sync Profile Schedule dialog box, enter the following information:

   Name  Lets you name your synchronization schedule.
Select type of schedule

Let you select when you want the synchronization to occur.

The following options let you make additional choices for when the synchronization occurs:

- **Weekly**
  - Lets you select which day or days of the week you want the synchronization to occur.

- **Monthly**
  - Lets you specify which day of the month you want the synchronization to occur.

- **One time only**
  - Lets you select the date that you want the one time synchronization to occur.

Start time

Let you select what time you want the synchronization to start.

4. When you are finished, click **Save**.

## Editing an Active Directory sync profile schedule

After you add your Active Directory sync profile schedules, you can edit any synchronization schedule. In ServiceDesk, you can edit an Active Directory sync profile schedule. For example, after you add an Active Directory sync profile schedule, you discover that it interferes with a maintenance schedule. Now, you need to change the start time of a full synchronization or the time that you want the synchronization to occur.

**Note:** The changes that you make to an Active Directory sync profile schedule affect any of the sync profiles to which you added that schedule.

After you edit an Active Directory sync profile schedule, the edited schedule appears in the drop-down lists for the **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile** fields. These fields appear in the **Edit Schedule for Active Directory Server** dialog box. This dialog box appears during the edit of an Active Directory sync profile.

The **Schedule For Update Sync Profile** field lets you schedule an automatic synchronization that only updates the changes that have been made to Active Directory since the last synchronization. The **Schedule For Full Sync Profile** field lets you schedule an automatic synchronization that updates the entire Active Directory domain or entire organizational units or groups.
To edit an Active Directory sync profile schedule

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profile Schedule**.

2. On the **Sync Profile Schedule** page, at the far right of the specific sync profile schedule name, click the **Actions** symbol (orange lightning), and click **Edit AD Sync Profile Schedule**.

3. In the **Edit Active Directory Sync Profile Schedule** dialog box, edit any of the following information:

   - **Name**: Lets you name your synchronization schedule.
   - **Select type of schedule**: Lets you select when you want the synchronization to occur.
     
     The following options let you make additional choices for when the synchronization occurs:
     
     - **Weekly**: Lets you select which day or days of the week you want the synchronization to occur.
     - **Monthly**: Lets you specify which day of the month you want the synchronization to occur.
     - **One time only**: Lets you select the date that you want the one time synchronization to occur.
   
   - **Start time**: Lets you select what time you want the synchronization to start.

4. When you are finished, click **Save**.

---

Deleting an Active Directory sync profile schedule

After you add your Active Directory sync profile schedules, you can delete update or full synchronization schedules. For example, you may need to delete an obsolete schedule.

After you delete your Active Directory sync profile schedule, it no longer appears in the drop-down lists for the **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile** fields. These fields appear in the **Add Schedule for Active Directory sync profile schedule**.
Directory Server or Edit Schedule for Active Directory Server dialog boxes. These dialog boxes appear during the addition or edit of an Active Directory sync profile.

**Note:** You cannot delete a sync profile schedule that any of your Active Directory sync profiles currently use. You must edit the sync profiles that use that schedule and select a different update or full synchronization schedule for them to use.

See “Editing an Active Directory sync profile schedule” on page 481.

**To delete an Active Directory sync profile schedule**

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profile Schedule**.

2. On the **Sync Profile Schedule** page, at the far right of the specific sync profile schedule name, click the **Actions** symbol (orange lightning), and click **Delete Schedule**.

3. In the confirmation message dialog box, click **OK**.

See “Managing Active Directory sync profile schedules” on page 478.

See “Managing Active Directory sync profiles” on page 483.

**Managing Active Directory sync profiles**

After you add your Active Directory server connections and select Active Directory as your authentication method, you can then add sync profiles for the connections. You can also edit and delete Active Directory sync profiles. In ServiceDesk, you can manage your Active Directory sync profiles.

You can use these Active Directory sync profiles to import data from Active Directory to the Process Manager database. You can target the entire domain, organizational units and groups on the Active Directory server, or specific LDAP queries. You manage these sync profiles in the Process Manager portal.

Before you begin adding your Active Directory sync profiles, you can add synchronization schedules for the sync profiles. After you add or edit an Active Directory sync profile, you may want to run a full synchronization manually before the next scheduled, automatic synchronization.

See “Managing Active Directory server connections” on page 469.

See “Managing Active Directory sync profile schedules” on page 478.

See “Methods for synchronizing Active Directory sync profiles” on page 493.
### Table 40-5  Process for managing Active Directory sync profiles

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Add automatic synchronization schedules. | In ServiceDesk, you can add automatic Active Directory sync profile schedules. See “Adding Active Directory sync profile schedules” on page 479. When adding or editing your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations.  
- Update synchronization  
- Full synchronization |
<p>| Step 2 | Add Active Directory sync profiles. | In ServiceDesk, you can add sync profiles for your Active Directory server connections. See “Adding Active Directory sync profiles” on page 486. |
| Step 3 | (Optional) Edit automatic synchronization schedules. | In ServiceDesk, you can edit an automatic Active Directory sync profiles schedule. See “Editing an Active Directory sync profile schedule” on page 481. |
| Step 5 | (Optional) Edit an Active Directory sync profile. | In ServiceDesk, you can edit an Active Directory sync profile. See “Editing an Active Directory sync profile” on page 489. |
| Step 6 | (Optional) Delete an Active Directory sync profile. | In ServiceDesk, you can delete an Active Directory sync profile. See “Deleting an Active Directory sync profile” on page 492. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>(Optional) Manually perform a full synchronization for an Active Directory sync profile.</td>
<td>In ServiceDesk, you can manually perform full synchronizations for the Active Directory sync profile that you specify. See “Running a full Active Directory sync profile synchronization manually” on page 495.</td>
</tr>
<tr>
<td>Step 8</td>
<td>(Optional) Manually perform update synchronization for an Active Directory sync profile.</td>
<td>In ServiceDesk, you can manually perform update synchronizations for the Active Directory sync profile that you specify. See “Running update Active Directory sync profile synchronization manually” on page 496.</td>
</tr>
<tr>
<td>Step 9</td>
<td>(Optional) Manually perform a full synchronization for all Active Directory sync profiles.</td>
<td>In ServiceDesk, you can manually perform full synchronizations for all your Active Directory sync profiles. See “Synchronizing all Active Directory sync profiles manually” on page 496.</td>
</tr>
<tr>
<td>Step 10</td>
<td>(Optional) Check the status of an Active Directory sync profile synchronization.</td>
<td>In ServiceDesk, you can view information about the users and groups that are synchronized and the status of the Active Directory sync profile’s synchronization. See “Checking the status of an Active Directory sync profile synchronization” on page 497.</td>
</tr>
<tr>
<td>Step 11</td>
<td>(Optional) Test an Active Directory server connection.</td>
<td>In ServiceDesk, you can test each Active Directory server connection. For example, the synchronization of an Active Directory sync profile fails. You may want to test the Active Directory server connection. See “Testing an Active Directory server connection” on page 476.</td>
</tr>
</tbody>
</table>
Adding Active Directory sync profiles

If your organization uses Active Directory authentication as its authentication method for ServiceDesk, you may need to add Active Directory sync profiles. These sync profiles let you import data from Active Directory to the Process Manager database. After you add your Active Directory server connections, you can add sync profiles for those connections. In ServiceDesk, you can add Active Directory sync profiles at any time.

You can add Active Directory sync profiles to target the entire domain, organizational units and groups on the Active Directory server, or specific LDAP queries. For example, you add a new organizational unit to Active Directory. You can add a sync profile for it in the Process Manager portal.

See “Configuring Active Directory sync profiles” on page 467.

See “Managing Active Directory sync profiles” on page 483.

See “Methods for synchronizing Active Directory sync profiles” on page 493.

To add Active Directory sync profiles

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.

2. On the **Active Directory Sync Profiles** page, at the far right of the **Active Directory Sync Profiles** title bar, click the **Actions** symbol (orange lightning), and click **Add AD Sync Profile**.
3 In the **Add Active Directory Sync Profile** dialog box, type or select the following information:

- **AD Sync Profile Name**
  - Lets you specify a name for the sync profile.

- **Select Connection**
  - Lets you choose which Active Directory server connection you want the sync profile to target.

- **AD Server Email Domain**
  - Lets you specify an email address for the users that you obtain from Active Directory. Use the following format:
    
    `<domain.com>`

  ServiceDesk requires that all users have an email address, but Active Directory does not. This domain is appended to the user name of any user who does not have an email address.

- **Auto Create User On Initial Login**
  - Lets you have a ServiceDesk user account created automatically when a new user logs on.

  A new user who logs on to ServiceDesk is authenticated against the Process Manager database. If the user does not have an account there, and this check box is checked, the user is authenticated against Active Directory. If the user has an Active Directory account, a mirror account is created in the Process Manager database.

- **AD Users Default Groups**
  - Lets you select the group to which users are added when their accounts are created automatically.

  The **All Users** group is the most typical selection.

  This option is available when you check **Auto Create User on Initial Login**.

4 When you are finished, click **Next**.

Note that if you do not enter the critical information or a connection cannot be made, a warning is displayed and you cannot proceed.
5 Under **Synchronization Option**, select one of the following options:

- **Entire Domain**: Connects ServiceDesk with your entire Active Directory.
- **Organization units**: Connects ServiceDesk with one or more Active Directory organizational units, which you select from the tree view that appears in this dialog box. The tree view displays the organization units that are defined in the specified Active Directory.
- **Groups**: Connects the ServiceDesk with one or more Active Directory groups, which you select from the tree view that appears in this dialog box. The tree view displays the groups that are defined in the specified Active Directory.
- **Specify LDAP Queries**: Connects ServiceDesk to a specific LDAP Query.

6 When you are finished, click **Next**.

7 In the **Add Active Directory Field Mapping** dialog box, select which fields in Active Directory you want to map to which fields in Process Manager and click **Next**.

   Note that normally you do not need to change any field mapping settings. Symantec recommends that you do not change any mappings to key fields, such as Primary Email ID (Email address), first names, and last names.

8 In the **Add Schedule for Active Directory Server** dialog box, select a schedule in the drop-down lists for **Schedule For Full Sync Profile** and **Schedule For Update Sync Profile**.

   Note that if the proper schedules do not appear in the drop-down lists for **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile**, you must add schedules.

   To add a schedule, click **Add Schedule**, add your schedules, and click **Save**. Repeat the process if you need to add another schedule. When you are done, the added schedules appear in the drop-down lists.

   See “Adding Active Directory sync profile schedules” on page 479.

9 When you are finished, click **Finish**.
Editing an Active Directory sync profile

After you add your Active Directory sync profiles, you can edit the settings for any sync profile. In ServiceDesk, you can change the sync profile settings to target a different organizational unit or group on the Active Directory server. You can map a different Active Directory field to a Process Manager field.

See “Managing Active Directory sync profiles” on page 483.

To edit an Active Directory sync profile

1. In the Process Manager portal, click Admin > Active Directory > Sync Profiles.

2. On the Active Directory Sync Profiles page, at the far right of the specific sync profile name, click the Actions symbol (orange lightning), and click Edit AD Sync Profile.
3 In the **Edit Active Directory Sync Profiles** dialog box, you can edit the following information:

<table>
<thead>
<tr>
<th>AD Sync Profile Name</th>
<th>Lets you specify a name for the sync profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Connection</td>
<td>Lets you choose which Active Directory server connection you want the sync profile to target.</td>
</tr>
<tr>
<td>AD Server Email Domain</td>
<td>Lets you specify an email address for the users that you obtain from Active Directory. Use the following format: &lt;domain.com&gt;</td>
</tr>
<tr>
<td></td>
<td>ServiceDesk requires that all users have an email address, but Active Directory does not. This domain is appended to the user name of any user who does not have an email address.</td>
</tr>
<tr>
<td>Auto Create User On Initial Login</td>
<td>Lets you have a ServiceDesk user account created automatically when a new user logs on.</td>
</tr>
<tr>
<td></td>
<td>A new user who logs on to ServiceDesk is authenticated against the Process Manager database. If the user does not have an account there, and this check box is checked, the user is authenticated against Active Directory. If the user has an Active Directory account, a mirror account is created in the Process Manager database.</td>
</tr>
<tr>
<td>AD Users Default Groups</td>
<td>Lets you select the group to which users are added when their accounts are created automatically.</td>
</tr>
<tr>
<td></td>
<td>The <strong>All Users</strong> group is the most typical selection.</td>
</tr>
<tr>
<td></td>
<td>This option is available when you check <strong>Auto Create User on Initial Login</strong>.</td>
</tr>
</tbody>
</table>

4 When you are finished, click **Next**.

Note that if you do not enter the critical information or a connection cannot be made, a warning is displayed and you cannot proceed.
5 In the **Edit Active Directory Sync Profile** dialog box under **Synchronization Option**, you can select a different target for the synchronization. If the target of your synchronizations has changed, select one the following options:

- **Entire Domain**: Synchronizes ServiceDesk with your entire Active Directory.
- **Organization units**: Synchronizes ServiceDesk with one or more Active Directory organizational units, which you select from the tree view that appears in this dialog box. The tree view displays the organization units that are defined in the specified Active Directory.
- **Groups**: Synchronizes ServiceDesk with one or more Active Directory groups, which you select from the tree view that appears in this dialog box. The tree view displays the groups that are defined in the specified Active Directory.
- **Specify LDAP Queries**: Synchronizes ServiceDesk to a specific LDAP Query.

6 When you are finished, click **Next**.

7 In the **Edit Active Directory Field Mapping** dialog box, you can edit which fields in Active Directory you want to map to which fields in Process Manager.

   Note that normally you do not need to change any field mapping settings. Symantec recommends that you do not change key fields mapping, such as Primary Email Id (Email address), first names, and last names.

8 When you are finished, select one of the following options:

- **Save**: If you do not want to edit the sync profile schedules, click **Save**. The dialog box closes, your changes are saved, and you are finished.

- **Next**: If you want to edit the sync profile schedules, click **Next**. Go to step 9.

   Note that editing a sync profile schedule means selecting or adding a different schedule. If you want to edit the sync profile schedule, you must edit it from the **Active Directory Sync Profiles Schedule** page.

   See “Editing an Active Directory sync profile schedule” on page 481.
In the Edit Schedule for Active Directory Server dialog box, you can select a different schedule in the drop-down lists for Schedule For Full Sync Profile and Schedule For Update Sync Profile.

Note that if the proper schedule does not appear in the drop-down lists for Schedule For Full Sync Profile or Schedule For Update Sync Profile, you must add a schedule.

To add schedule, click Add Schedule, add your schedules, and click Save. When you are done, the added schedule appears in the drop-down lists.

See “Adding Active Directory sync profile schedules” on page 479.

When you are finished, click Finish.

Deleting an Active Directory sync profile

After you add your Active Directory sync profiles, you can delete any of the Active Directory sync profiles that you no longer need. For example, you may need to delete an obsolete sync profile.

To delete an Active Directory sync profile

1 In the Process Manager portal, click Admin > Active Directory > Sync Profiles.

2 On the Active Directory Sync Profiles page, under Active Directory Sync Profile, at the far right of the specific sync profile name, click the Actions symbol (orange lightning), and click Delete AD Sync Profile.

3 In the confirmation message dialog box, click OK.

See “Managing Active Directory sync profiles” on page 483.

Add Active Directory Sync Profiles and Edit Active Directory Sync Profiles dialog boxes

If your organization uses Active Directory authentication for its authentication method for ServiceDesk, you need to add Active Directory sync profiles. You may also need to edit an Active Directory sync profile. During the addition or edit of your Active Directory sync profiles, you open the Add AD Sync Profile or the Edit AD Sync Profile dialog box. These dialog boxes let you add information for a new Active Directory sync profile or edit an existing one.

See “Adding Active Directory sync profiles” on page 486.

See “Editing an Active Directory sync profile” on page 489.
Table 40-6 Options on the Add Active Directory Sync Profiles dialog box and Edit Active Directory Sync Profiles dialog boxes

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD Sync Profile Name</td>
<td>Lets you specify a name for the sync profile.</td>
</tr>
<tr>
<td>Select Connection</td>
<td>Lets you choose which Active Directory server connection you want the sync profile to target.</td>
</tr>
<tr>
<td>AD Server Email Domain</td>
<td>Lets you specify an email address for the users that you obtain from Active Directory. Use the following format: domain.com. ServiceDesk requires that all users have an email address, but Active Directory does not. This domain is appended to the user name of any user who does not have an email address.</td>
</tr>
<tr>
<td>Auto Create User On Initial Login</td>
<td>Lets you have a ServiceDesk user account created automatically when a new user logs on. A new user who logs on to ServiceDesk is authenticated against the Process Manager database. If the user does not have an account there, and this check box is checked, the user is authenticated against Active Directory. If the user has an Active Directory account, a mirror account is created in the Process Manager database.</td>
</tr>
<tr>
<td>AD Users Default Groups</td>
<td>Lets you select the group to which users are added when their accounts are created automatically. The All Users group is the most typical selection. This option is available when the following check box is checked: Auto Create User on Initial Login.</td>
</tr>
</tbody>
</table>

Methods for synchronizing Active Directory sync profiles

When your organization uses Active Directory authentication as its authentication method for ServiceDesk, ServiceDesk can synchronize with Active Directory. The synchronization lets you add and update Active Directory users and groups in the Process Manager database. You can add automatic synchronization schedules to your Active Directory sync profiles. You can also manually run Active Directory sync profile synchronizations.

When ServiceDesk synchronizes with Active Directory, you can view information about the users and groups that are synchronized and the status of the synchronization.
See “About Active Directory synchronization” on page 466.

See “Configuring Active Directory sync profiles” on page 467.

See “Managing Active Directory sync profiles” on page 483.

See “Checking the status of an Active Directory sync profile synchronization” on page 497.

Table 40-7 Methods for synchronizing Active Directory sync profiles

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Run automatic update and full synchronizations. | In ServiceDesk, you can add automatic Active Directory sync profile schedules. See “Adding Active Directory sync profile schedules” on page 479. When adding your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations:  
  ■ Update synchronization  
  ■ Full synchronization  
  See “Adding Active Directory sync profiles” on page 486. |
| Manually run a full synchronization.         | In ServiceDesk, you can manually run a full Active Directory sync profile synchronization at any time. This process lets you run a full synchronization on the specified Active Directory sync profile. See “Running a full Active Directory sync profile synchronization manually” on page 495. |
| Manually run update synchronization.         | In ServiceDesk, you can manually run update Active Directory sync profile synchronization at any time. This process lets you synchronize an Active Directory sync profile with only the changes that have been made to it since the last synchronization. See “Running update Active Directory sync profile synchronization manually” on page 496. |
| Manually synchronize all the Active Directory sync profiles. | In ServiceDesk, you can manually run a full synchronization of all your Active Directory sync profiles at any time. This process lets you synchronize all your sync profiles for each Active Directory server connection. See “Synchronizing all Active Directory sync profiles manually” on page 496. |
Running a full Active Directory sync profile synchronization manually

In ServiceDesk, you can manually synchronize an Active Directory sync profile with Active Directory at any time between the automatic synchronization intervals. For example, when you add a new Active Directory sync profile, you can manually synchronize it immediately instead of waiting for the next automatic synchronization.

This process runs a full synchronization as follows:

- If the Active Directory sync profile includes the entire Active Directory server domain, the entire domain is synchronized.
- If the Active Directory sync profile includes only specific Active Directory organizational units or groups, the entire contents of those units and groups are synchronized.

See “About Active Directory synchronization” on page 466.
See “Configuring Active Directory sync profiles” on page 467.
See “Managing Active Directory sync profiles” on page 483.
See “Methods for synchronizing Active Directory sync profiles” on page 493.

**Warning:** Any users that are connected to Process Manager might be disconnected during the synchronization.

You can check the status of the synchronization during the process or after the process finishes.

See “Checking the status of an Active Directory sync profile synchronization” on page 497.

**To run a full Active Directory sync profile synchronization manually**

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profiles**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Run Reset Sync Profile**.
3. When the dialog box that announces the start of the synchronization appears, you can close it.
Running update Active Directory sync profile synchronization manually

In ServiceDesk, you can manually run update synchronization of an Active Directory sync profile with Active Directory at any time between automatic synchronization intervals. With this synchronization process, you synchronize only the changes that were made to Active Directory since the last synchronization.

For example, after you add or remove users in Active Directory, you want to apply those changes to Active Directory sync profile immediately. You can check the status of the synchronization during the process or after the process finishes.

See “About Active Directory synchronization” on page 466.
See “Managing Active Directory sync profiles” on page 483.
See “Methods for synchronizing Active Directory sync profiles” on page 493.
See “Checking the status of an Active Directory sync profile synchronization” on page 497.

To run update Active Directory sync profile synchronization manually

1. In the Process Manager portal, click Admin > Active Directory > Sync Profiles.
2. On the Active Directory Sync Profiles page, under Active Directory Sync Profiles, at the far right of the specific sync profile name, click the Actions symbol (orange lightning), and click Run Update Sync Profile.
3. When the dialog box that announces the start of the synchronization appears, you can close it.

Synchronizing all Active Directory sync profiles manually

In ServiceDesk, you can manually synchronize all your Active Directory sync profiles with all Active Directory servers to which ServiceDesk is connected. For example, you might need to recover after a power loss. This synchronization method includes the synchronization of all the Active Directory sync profiles for each Active Directory server connection.

See “About Active Directory synchronization” on page 466.
See “Configuring Active Directory sync profiles” on page 467.
See “Managing Active Directory sync profiles” on page 483.
See “Methods for synchronizing Active Directory sync profiles” on page 493.
To synchronize all Active Directory sync profiles

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.

2. On the **Active Directory Sync Profiles** page, at the far right of the **Active Directory Sync Profiles** title bar, click the **Actions** symbol (orange lightning), and click **Run AD Sync Profile**.

3. When the dialog box that announces the start of the synchronization appears, you can close it.

---

**Checking the status of an Active Directory sync profile synchronization**

When ServiceDesk synchronizes with Active Directory, you can view information about the users and groups that are synchronized and the status of the synchronization. For example, if your Active Directory is large, you might periodically check the status as the synchronization runs. If a synchronization is not running, the status check shows information for the last synchronization that occurred. For example, you can verify that an overnight synchronization completed successfully. You can check the status of an Active Directory synchronization in the Process Manager portal from the **Active Directory Sync Profiles** page.

See “Configuring Active Directory sync profiles” on page 467.

See “Managing Active Directory sync profiles” on page 483.

See “Methods for synchronizing Active Directory sync profiles” on page 493.

To check the status of an Active Directory sync profile synchronization

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.

2. On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profiles**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Check Sync Status**.

3. The **Sync Process Status** dialog box opens and displays status of the sync profile synchronization.

4. If you check the status of a synchronization during the synchronization, you can click **Refresh** to update the display.

5. When you are finished viewing the status information, click **Close**.
Managing the Active Directory connections

Checking the status of an Active Directory sync profile synchronization
Managing categories and the data hierarchy

This chapter includes the following topics:

- About Incident Management classifications and the data hierarchy
- Adding an incident classification
- Deleting an incident classification
- Importing incident classifications
- Exporting incident classifications

About Incident Management classifications and the data hierarchy

The Incident Management process contains predefined incident classifications. You can use the default classifications immediately or create your own. Support technicians use the classifications to classify the incidents. The incident classifications help route the tickets to the appropriate service queue. The incident classifications also help sort incidents for reports.

If the parent classification is too broad, you can add levels of classifications to make the classification process more granular. You can define up to 10 levels of classifications in the hierarchy tree. The Incident Management hierarchy tree contains your incident classifications.

Set up your classification system to meet your needs without making it too complex. Add the categories that are vital to populating your reports. Provide only enough levels for the workers to accurately classify the incidents.
Too many classifications can make it difficult and time-consuming for workers to select the correct one. Mis-categorization can lead to inaccurate reporting. An overabundance of categories can make trend reporting less meaningful. The more categories that you have, the greater the number of routing rules you must create.

For more information see the following topics:

See “Adding an incident classification” on page 500.
See “Deleting an incident classification” on page 501.
See “Importing incident classifications” on page 502.
See “Exporting incident classifications” on page 502.

**Video:** For more information about managing the classification hierarchy, see *ServiceDesk Configuration: Manage Classification Hierarchy* on Symantec Connect.

# Adding an incident classification

ServiceDesk lets you add incident classifications to the Incident Management process. Your new classifications are available for any incidents that you create and to populate your reports. To add incident classifications, you use the **Add Hierarchy Items** option on the **Hierarchy Data Services** page.

---

**Note:** Best practices recommend that you add incident classifications before you set up your rulesets. Best practices recommend that you export and save the *Incident_Management.csv* file before you make any modifications to the Incident Management classification tree.

---

**To add an incident classification**

1. In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.

2. On the **Hierarchy Data Service** page, under **Hierarchy Tree**, select the parent classification in which you want the new incident classification to be located.

   For example, if you want the classification to appear under **Handheld**, expand **Incident Management > Hardware** and click **Handheld**

3. Under the bottom right corner of the **Hierarchy: Incident Management** section, click **Add Hierarchy Items**.
4 In the **Add Hierarchy Items** dialog box, under **Add New Hierarchy Item (one per line)**, type the classifications that you want to add.

To add multiple items, press **Enter** after each item so that it appears on its own line.

5 When you are finished, click **Add Items**.

See “**Exporting incident classifications**” on page 502.

See “**About Incident Management classifications and the data hierarchy**” on page 499.

## Deleting an incident classification

ServiceDesk lets you delete incident classifications from the Incident Management process. You can delete the classifications that are not valid or that are no longer useful. For example, you might decide to delete a predefined category that does not apply to your organization. If the classification that you delete contains any subclasses, they are also deleted. Any incidents that belong to a deleted classifications remain unchanged.

**Warning:** Best practices recommend that you do not delete a classification after you set up your rulesets and begin using ServiceDesk. Rules that use the incident break. Any incidents that are still assigned to a deleted category do not appear in the reports and searches that are run. Best practices recommend that you export and save the **Incident_Management.csv** file before you make any modifications to the Incident Management classification tree.

### To delete an incident classification

1 In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.

2 On the **Hierarchy Data Service** page, under **Hierarchy Tree**, select the parent classification from which you want to delete the classification.

   For example, if you want to delete a classification that appears under **Handheld**, expand **Incident Management > Hardware** and click **Handheld**.

3 In the **Hierarchy: Incident Management** section, to the right of the classification that you want to delete, click the **Delete** symbol (red X).

4 In the **Message from webpage** dialog box, click **OK**

See “**Exporting incident classifications**” on page 502.

See “**About Incident Management classifications and the data hierarchy**” on page 499.
Importing incident classifications

ServiceDesk lets you import incident classifications into the Incident Management process. You can import a .csv file that already contains the incident classifications and levels.

For example, you have more than one ServiceDesk server. You set up the incident classifications in the Process Manager portal on your first ServiceDesk server. You can export and save a copy of the Incident_Management.csv file. Then, you can import the Incident_Management.csv file and use it to populate the incident classifications in the Process Manager portal on your second ServiceDesk server.

**Note:** Best practices recommend that you import incident classifications before you set up your rulesets. Best practices recommend that you export and save the original .csv file before you import the new .csv file.

To import incident classifications

1. In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.
2. On the **Hierarchy Data Service** page, on the **Hierarchy Tree** title bar, click the **Actions** symbol (orange lightning) and then click **Import Category**.
3. In the **Import Category** dialog box, browse for and select the .csv file to import and then click **Import**.

See “Exporting incident classifications” on page 502.

See “About Incident Management classifications and the data hierarchy” on page 499.

Exporting incident classifications

ServiceDesk lets you export your incident classifications. You can export the Incident_Management.csv file from ServiceDesk that contains the incident classifications and levels.

Best practice recommends that you export a copy of the Incident_Management.csv file before you begin modifying or deleting your default Incident Management classifications.
To export incident classifications

1. In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.

2. On the **Hierarchy Data Service** page, under the **Hierarchy Tree** section, click **Incident Management**.

3. On the right side of the **Hierarchy: Incident Management** title bar, click the **Action** symbol (orange lightning) and then click **Export Category**.

4. In the **File Download** dialog box, click **Save**.

5. In the **Save As** dialog box, select the location where you want to save the **Incident_Management.csv** file and then click **Save**.

6. In the **Download complete** dialog box, click **Close**.

See “**Importing incident classifications**” on page 502.

See “**About Incident Management classifications and the data hierarchy**” on page 499.
Managing categories and the data hierarchy

Exporting incident classifications
Customizing forms

This chapter includes the following topics:

■ About customizing forms
■ Editing a form in the Process Manager portal
■ Setting permissions for a form
■ About the Customer Satisfaction Survey

About customizing forms

In the Process Manager portal, a form is the screen or page that workers and users interact with during a process. The forms feed the process data into the database. For example, a change worker uses the Request Change form to submit a new change request. Users use the Create New Incident form to submit incidents.

ServiceDesk contains predefined forms for all its processes. These predefined forms are complete and ready to use immediately. However, you can customize any of the forms to meet your organization's established process requirements.

For example, many organizations customize the Customer Satisfaction Survey form that is sent to the submitting user when an incident is resolved and confirmed. In the survey, the user rates how satisfied they are with the service that they received.

See “About the Customer Satisfaction Survey” on page 508.

The form customization can be performed at different levels and from different places.
### Table 42-1  Levels of form customization

<table>
<thead>
<tr>
<th>Level</th>
<th>Where to edit</th>
<th>What you can customize</th>
</tr>
</thead>
<tbody>
<tr>
<td>The form itself</td>
<td>Workflow Designer</td>
<td>Examples of how you can customize a form are as follows:</td>
</tr>
<tr>
<td></td>
<td>For more information about customizing forms, see the Symantec™ Workflow 7.5 User Guide.</td>
<td>■ Change the theme or the template style.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can select from a range of theme and template styles or you can create your own.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can also change the form size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Change the text that appears on a form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Change the images that appear on a form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Rearrange the elements on the form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Change error messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The predefined forms contain the error messages that appear when a required field is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not populated. You can edit these error messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Change the confirmation pages that are presented to users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Several process actions result in a confirmation message being sent to the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, when a user submits an incident, a Thank You page appears; when a log on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fails, an error page appears. You can change the contents of these pages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Add data to a form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, you might add a field to the incident form so that the support technicians</td>
</tr>
<tr>
<td></td>
<td></td>
<td>can assign the incident to a cost center.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Remove data from a form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Warning:</strong> Use caution when you remove data components from a form. Any of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>output variables that those components designate become invalid after the removal,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>which breaks the process.</td>
</tr>
</tbody>
</table>
### Table 42-1  Levels of form customization (continued)

<table>
<thead>
<tr>
<th>Level</th>
<th>Where to edit</th>
<th>What you can customize</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aspects of the form’s appearance and behavior in the Service Catalog</td>
<td>Process Manager portal, on the <strong>Edit Form</strong> page.</td>
<td>On the <strong>Edit Form</strong> page, you can edit the form information on the following tabs:</td>
</tr>
</tbody>
</table>
|                                                                      | See “Editing a form in the Process Manager portal” on page 507.               | ■ **Form Information**  
The name, description, and other information regarding the form’s display in the Process Manager portal.  |
|                                                                      |                                                                              | ■ **WebPart Information**  
Lets you define the form as a Web part.                                      |
|                                                                      |                                                                              | ■ **User Information**  
Information about passing the user ID.                                          |
|                                                                      |                                                                              | ■ **Session Information**  
Information about passing a session ID.                                            |
|                                                                      |                                                                              | ■ **Permissions**  
Lets you determine who can access a process by setting permissions on the form that provides access to that process.  
See “Setting permissions for a form” on page 508.  |
|                                                                      |                                                                              | ■ **Profiles**  
Lets you assign a default form profile to the form.  |

### Editing a form in the Process Manager portal

In the Process Manager portal, a form is the screen or page that workers and users interact with during a process. You can customize the aspects of a form’s appearance and behavior in the Service Catalog.

See “About customizing forms” on page 505.

To edit a form in the Process Manager portal

1. In the Process Manager portal, click **Admin > Service Catalog Settings**.
2. Under **Browse Category**, select the form’s category.
3. In the right pane, at the far right of the form’s title bar, click the **Actions** symbol (orange lightning), and then click **Edit Form**.
4. On the **Edit Form** page, edit the information on one or more tabs as necessary.
5. Click **Save**.
Setting permissions for a form

A form is the screen or page that the users and workers interact with during a process. The ServiceDesk forms appear in the Service Catalog. You can determine who can access a process by setting permissions on the form that provides access to that process.

See “About customizing forms” on page 505.

To set permissions for a form

1. In the Process Manager portal, click Admin > Service Catalog Settings.
2. Under Browse Category, select the form’s category.
3. In the right pane, at the far right of the form’s title bar, click the Actions symbol (orange lightning), and then click Edit Form.
4. On the EditForm page, click the Permissions tab and add or edit permissions as needed.
   See “Setting permissions” on page 113.
5. Click Save.

About the Customer Satisfaction Survey

After an incident is resolved, the submitting user receives a task to view its history, comments, and other information about its resolution. If the resolution is satisfactory, the user marks the incident as resolved. When the incident resolution is verified, the user can be asked to complete a Customer Satisfaction Survey to rate the service and the resolution. The Incident Management OnResolutionVerified ruleset comes with a preconfigured rule that can send out the Customer Satisfaction Survey when an incident is resolved.

You can customize the Customer Satisfaction Survey.

Examples of how you might change the Customer Satisfaction Survey are as follows:

- Change the frequency with which the survey is sent.
  By default, the OnResolutionVerified ruleset comes with a preconfigured rule that sends out the Customer Satisfaction Survey. Each time an incident is resolved, there is a 50% chance that the rule sends out the Customer Satisfaction Survey.
  You can change the frequency that the Customer Satisfaction Survey is sent out. Edit the condition in the preconfigured rule that sends out the survey.
  In the Process Manager portal, click Admin > Process Automation. Expand Incident Management and then click Service Dashboard. Expand Ruleset:
OnResolutionVerified and select the Customer Survey rule. In the title bar, click the Actions symbol (orange lightning) and then click Edit Rule. On the Edit Rule page, to the right of the condition, click the Edit symbol (note pad and green pencil).

- Change the data that the survey collects.
  You can change the text on the survey form. You can also change the survey questions and the possible responses so that you can track the information that is most important to your organization.
  You can change the appearance and fields of the Customer Satisfaction Survey by editing the SD.CustomerSurvey project in Workflow Designer.

For more information about customizing forms and editing the Customer Satisfaction Survey, see the Symantec™ Workflow 7.5 User Guide.

See “About customizing forms” on page 505.
About the Customer Satisfaction Survey
Customizing the email in ServiceDesk

This chapter includes the following topics:

- Customizing the email actions for ServiceDesk processes
- About the contents of email notifications
- About configuring the email monitoring

Customizing the email actions for ServiceDesk processes

ServiceDesk can perform the following automatic email actions:

- Send email notifications at various stages of the Problem Management and Knowledge Management processes, based on one or more events that occur within these processes.
- Accept new incidents or updates to current incidents through inbound email.

These email capabilities are predefined and ready to use. However, you can customize them as needed.

All the actions that are listed in Process for customizing the email action for ServiceDesk processes table are optional and can be performed in any order.
Table 43-1 | Process for customizing the email actions for ServiceDesk processes

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the automatic email notifications.</td>
<td>The Problem Management and Knowledge Management processes can trigger several types of email notifications. You can customize the email notifications by editing the project for the appropriate process in Workflow Designer. See “About automatic email notifications” on page 377. For more information about editing the process projects, see the Symantec™ Workflow 7.5 User Guide.</td>
</tr>
<tr>
<td>Edit the automatic email contents.</td>
<td>The contents of the automatic email messages are predefined for each type of notification. You can customize any of these messages or add new ones. See “About the contents of email notifications” on page 512.</td>
</tr>
</tbody>
</table>
| Customize the email monitoring. | ServiceDesk monitors the appropriate inbox for all new, unread emails and processes them by creating incidents or routing them to the support team for classification. See “About the creation of incidents from emails” on page 163. You can customize the email monitoring as follows:  
  - The mailbox and other email settings are configured during the installation of the ServiceDesk application software. If necessary, you can change some of these settings on the portal Master Settings page.  
  - You can use the monitoring process as it is defined or you can customize it. For example, you can monitor multiple mailboxes, define the email contents to be processed, and change the assignee for the new incidents. See “About configuring the email monitoring” on page 513. |

About the contents of email notifications

ServiceDesk can send email notifications at various stages of the Problem Management and Knowledge Management processes. Email notifications can be sent based on one or more events that occur within these processes. See “About automatic email notifications” on page 377.

The contents of the email messages are predefined and ready to use. However, you can customize any of these messages. You can also edit the triggers of the emails or add notifications to additional processes.

ServiceDesk obtains the contents of the email messages from several sources.
Table 43-2 Sources for the contents of the email messages

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
</table>
| The Send Email component or adjacent text component within the Problem Management process | ■ The Problem Management process executes the Send Email component to generate the email messages within the process itself.  
 ■ The message text may be composed within the Send Email component or within adjacent text component.  
 ■ You can customize the default email messages by editing the message text within the Problem Management process in Workflow Designer. |
| The Send Email component or adjacent text component within the knowledge base submission process | ■ The knowledge base submission process executes the Send Email component to generate the email messages within the process itself.  
 ■ The message text may be composed within the Send Email component or within adjacent text components.  
 ■ You can customize the default email messages by editing the message text within the knowledge base submission process in Workflow Designer. |

For more information about configuring the content for email or editing processes and Projects, see the Symantec™ Workflow 7.5 User Guide.

These automatic email notifications are different from the process notifications that result from the events that occur on specific items within the Process Manager portal. For example, the process notifications can be sent when a document or a knowledge base entry is added, edited, or deleted.

See “About process notifications” on page 378.

About configuring the email monitoring

ServiceDesk can accept new incidents or updates to current incidents through inbound email. ServiceDesk monitors the appropriate inbox for all new, unread emails and processes them by creating incidents or routing them to the support team for classification. This email process relies on an automatically-generated reply code to link the email correspondence to an incident. The support workers do not have to check an Inbox because the email correspondence is added to the incident’s history.

By default, the email monitoring process can also add the contents of the email responses to a process ticket. The recipient of the email can send a reply that contains the requested information. The monitoring process reads the reply code
that is associated with the email. The process adds the email contents to the appropriate process history and creates a task for the process worker.

See “About the creation of incidents from emails” on page 163.

The mailbox and other email settings are configured during the installation of the ServiceDesk application software. If necessary, you can change these settings on the Application Properties page, under the Service Desk Settings link. The Application Properties page is available from the Admin menu.

See “Commands on the Admin menu” on page 523.

The default monitoring process is ready to use. However, you can customize it in several ways to meet your organization’s requirements.

Table 43-3 Suggestions for customizing the email monitoring

<table>
<thead>
<tr>
<th>Customization</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples of how you might customize the email monitoring process are as follows:</td>
<td>Edit the SD.Email.Monitor project in Workflow Designer.</td>
</tr>
<tr>
<td>■ Configure the process to monitor multiple mailboxes.</td>
<td></td>
</tr>
<tr>
<td>■ Add or change the words or phrases in the subject line that trigger the creation of an incident.</td>
<td></td>
</tr>
<tr>
<td>■ Create an incident rule that defines the words or phrases in the message body that can populate values in the incident.</td>
<td></td>
</tr>
<tr>
<td>■ Use a notification rule to automatically create an email if additional information is needed from the original sender.</td>
<td></td>
</tr>
<tr>
<td>Create templates for the users who submit incident through email so ServiceDesk can capture or evaluate specific information.</td>
<td>You can create an email template in your email client, and then set up incident rules in the SD.Email.Monitor project to evaluate the template content. For example, if you include a Location field in the email template, the incoming email messages can be routed to the correct location.</td>
</tr>
<tr>
<td>Many organizations perform this customization.</td>
<td></td>
</tr>
</tbody>
</table>

For more information about configuring email and customizing projects, see the Symantec™ Workflow 7.5 User Guide.
Distributing the ServiceDesk documentation

This chapter includes the following topics:

- Making the ServiceDesk documentation available to users
- Configuring the Help link for ServiceDesk documentation
- Linking to the ServiceDesk documentation from a Links Web part
- Displaying the ServiceDesk documentation in a File Browser Web part
- Adding the ServiceDesk documentation to Document Management

Making the ServiceDesk documentation available to users

Each organization has specific requirements for providing documentation to their process workers and the users of the Process Manager portal. Therefore, the ServiceDesk documentation is not installed with ServiceDesk. We recommend that you download these guides and make them available to your users as needed.

To avoid the distribution of outdated documentation, you must update the documentation files when updates are available. The updated documentation files are not installed with the software updates. When you plan how to distribute the documentation to your ServiceDesk users, consider the ease of updating the documents in the future.
## Table 44-1: Process for making the ServiceDesk documentation available to users

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Download the documentation to a shared network drive or other location.</td>
<td>Download any of the following documents:</td>
</tr>
</tbody>
</table>
|        |                                                                                                  | ■ Symantec™ ServiceDesk 7.5 Implementation Guide  
This guide is for the administrator who installs and configures ServiceDesk.  
■ Symantec™ ServiceDesk 7.5 User Guide  
This guide is for the process workers.  
The ServiceDesk release notes and other documentation resources contain the links to the location for downloading the documentation files. |
| Step 2 | Make the documentation available to the users.                                                   | You can provide access to the documentation files in whatever way you decide is best.  
Some of the options that are available in ServiceDesk are as follows:  
■ Edit the Help link that appears at the lower left of the Process Manager portal window. Set the link to target the location of the documentation files.  
The default target for the Help link is the ServiceDesk Product Support page on the Symantec Website.  
See “Configuring the Help link for ServiceDesk documentation” on page 517.  
■ Add the documentation files to a document management category and add a category browser Web part to access them.  
See “Adding the ServiceDesk documentation to Document Management” on page 520.  
■ Add a file browser Web part that enables browsing to the documents.  
See “Displaying the ServiceDesk documentation in a File Browser Web part” on page 519.  
■ Add the Links Web part that provides links to the documents.  
See “Linking to the ServiceDesk documentation from a Links Web part” on page 517.  
We do not recommend that you deliver copies of the documentation to individual users. The more copies of the documentation that you distribute, the harder it becomes to update all of them. |
| Step 3 | Tell the users how to access the documentation.                                                   | Use the method that is best for your organization.  
One option is to create a Bulletin Board message that users can view in the Process Manager portal.  
See “About the Bulletin Board” on page 309.                                                                                                   |
Configuring the Help link for ServiceDesk documentation

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by configuring the Help link that appears in the Process Manager portal to link to the location of the documentation files.

The default target for the Help link is the ServiceDesk Product Support page on the Symantec Website. Other options are available for providing access to the documentation from within the Process Manager portal.

See “Making the ServiceDesk documentation available to users” on page 515.

Caution: To avoid the distribution of outdated documentation, you must update the documentation files when updates are available. The documentation files are not installed with the software updates.

To configure the Help link for ServiceDesk documentation

1. In the Process Manager portal, click Admin > Portal > Master Settings.
2. On the Master Settings page, expand the Process Manager Settings section.
3. In Help Link Url, type the fully qualified path to the location of the documentation files in the following format:

   http://www.<domain>.com/<folder>

4. Click Save.

Linking to the ServiceDesk documentation from a Links Web part

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by adding a Links Web part in the Process Manager portal to display links to the location of the documentation files.

You can set permissions on the portal page that you add the Web part to. The permissions settings ensure that only the appropriate users can access the documentation.
Other options are available for providing access to the documentation from within the Process Manager portal. See “Making the ServiceDesk documentation available to users” on page 515.

**Caution:** To avoid the distribution of outdated documentation, you must update the documentation files when updates are available. The documentation files are not installed with the software updates.

### Table 44-2  Process for linking to the ServiceDesk documentation from a Links Web part

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Ensure that the documentation files are in the correct folder.</td>
<td>If you downloaded the documentation files to a location that is not accessible to all the users, move the files to an appropriate shared location.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add a Links Web part to a portal page that the target users can access.</td>
<td>The portal page that you select should be accessible to the target users only. For example, add a link to the Symantec™ ServiceDesk 7.5 Implementation Guide on a portal page that only the administrators can access. The Links option is in the Catalog Zone pop-up under the UI section. See “Adding a Web part to a Process Manager portal page” on page 85.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Edit the Web part to specify the target URL.</td>
<td>In the Editor Zone pop-up, under Property Grid, in URL, you must specify the fully-qualified path or URL where the documentation is located. See “Editing or deleting a Web part on a Process Manager portal page” on page 86.</td>
</tr>
</tbody>
</table>
Table 44-2  Process for linking to the ServiceDesk documentation from a Links Web part (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 4 | Make additional edits to the Web part. | In the Editor Zone pop-up, we recommend that you select the following options:  
- **Show open in new window control**  
  This option is in the Links Editor section.  
- **Title**  
  The text that you type here appears in the Web part title bar. For example, you might type ServiceDesk Documentation.  
  This option is in the Appearance section.  
You can edit other attributes of the Web part as needed. |

Displaying the ServiceDesk documentation in a File Browser Web part

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by adding a File Browser Web part in the Process Manager portal to display the folder that contains the documentation files.

The File Browser Web part displays a folder tree that starts with a parent folder that you specify. The users can navigate to the child folder that contains the documentation.

You can set permissions on the portal page that you add the Web part to. The permissions settings ensure that only the appropriate users can access the documentation. You can also set permissions on the documentation folder.

Other options are available for providing access to the documentation from within the Process Manager portal.

See “Making the ServiceDesk documentation available to users” on page 515.

**Caution:** To avoid the distribution of outdated documentation, you must update the documentation files in the Document Management system when updates are available. The documentation files are not installed with the application updates.
### Table 44-3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Ensure that the documentation files are in a folder that the target users can access.</td>
<td>If you downloaded the documentation files to a location that is not accessible to all the users, move the files to an appropriate shared location. Be sure to place the documentation files in their own folder, under a parent folder that contains no other subfolders. The FileBrowser Web part displays all the subfolders of the parent folder.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add a FileBrowser Web part to a portal page that the target users can access.</td>
<td>The portal page that you select should be accessible to the target users only. For example, add a link to the Symantec™ ServiceDesk 7.5 Implementation Guide on a portal page that only the administrators can access. The FileBrowser option is in the CatalogZone pop-up under the UI section. See “Adding a Web part to a Process Manager portal page” on page 85.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Edit the Web part to specify the target folder.</td>
<td>In the Editor Zone, under Property Grid, in Folder, you must specify the parent folder of the folder that contains the documentation files. Be sure to include the full path to the parent folder. The File Browser Web part cannot display any files in the parent folder. Therefore, do not specify the documentation folder as the parent. See “Editing or deleting a Web part on a Process Manager portal page” on page 86.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Make other edits as needed.</td>
<td>You can edit other attributes of the Web part as needed. For example, you might change the title of the Web part to Browse ServiceDesk Documentation. The Title option is in the Editor Zone pop-up under the Appearance section.</td>
</tr>
</tbody>
</table>

### Adding the ServiceDesk documentation to Document Management

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by adding the documentation files to a document category and providing access to those files from a category browser Web part.

You can set permissions on the category or on the document files so that only the appropriate users can access the documentation.
Other options are available for providing access to the documentation from within the Process Manager portal.

See “Making the ServiceDesk documentation available to users” on page 515.

**Caution:** To avoid the distribution of outdated documentation, you must update the documentation files in the Document Management system when updates are available. The documentation files are not installed with the Server software updates.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | (Optional) Create a new documents category. | You can dedicate an entire category to the documentation. For example, you might name the category ServiceDesk Documentation.  
See “Adding a document category” on page 348.  
Alternatively, you can add the documentation files to an existing category. |
| Step 2 | (Optional) Set permissions on the category. | You can set permissions at the category level if all the documents in that category are intended for the same users.  
See “Setting permissions for a document category” on page 351.  
Alternatively, you can set permissions on the individual documents. |
| Step 3 | Add one or more documentation files to the category. | Add the documentation files from their download location.  
See “Adding a document to the Document Management system” on page 355. |
| Step 4 | (Optional) Set permissions on the documents. | If the category contains multiple documents for different types of users, you can set permissions on the individual documents. For example, you can set permissions on the ServiceDesk Implementation Guide so that only administrators can view it.  
We recommend that you do not allow anyone to edit the documentation files.  
See “Setting permissions for a document” on page 359. |
| Step 5 | Add a category browser Web part to a portal page that the target users can access. | The category browser Web part displays the document categories and lets the user select the category and view the documents in that category.  
The CategoryBrowserWebPart option is in the CatalogZone pop-up under the Documents section.  
See “Adding a Web part to a Process Manager portal page” on page 85. |
### Table 44-4

Process for adding the ServiceDesk documentation to Document Management *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 6 | (Optional) Edit the Web part.              | You can edit the Web part as needed. For example, you might change the title of the Web part to ServiceDesk Documentation. The **Title** option is in the **Editor Zone** pop-up under the **Appearance** section.  
See “Editing or deleting a Web part on a Process Manager portal page” on page 86. |
Performing administrative tasks

This chapter includes the following topics:

- Commands on the Admin menu
- About application properties
- About incident close codes
- Adding and deleting incident close codes
- About the Process Manager portal master settings
- Editing the Process Manager portal master settings
- Master Settings: Process Manager Active Directory Settings section
- Creating user relationship types

Commands on the Admin menu

The Admin menu provides access to all the administrative functions that are available in ServiceDesk. Only an administrator or other user who has the appropriate permissions can access this menu.

The Admin menu consists of all the options that are available on the Admin page in the Process Manager portal.

See “Admin page” on page 57.
<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Application Properties</td>
<td>Lets you add, edit, and delete application properties. Typically, you define application properties as part of the installation configuration process, but you can also work with them from the Admin area. Application properties are a type of profile. Instead of hard-coding the values that you use in workflow components, you can define application properties to represent those values. You can use the properties in multiple workflow components. See “About application properties” on page 528.</td>
</tr>
<tr>
<td>Data</td>
<td>Lists/Profiles</td>
<td>Lets you add, edit, and delete profile definitions. Profiles let you categorize data by adding customizable fields, which you can use for further sorting of data. For example, you can set up profile values of “hardware” and “OS” for incidents. When users enter incidents in ServiceDesk, they can specify the hardware type and operating systems that are involved in the incident. When technicians analyze the data from multiple incidents, they can see patterns emerge. These patterns may reveal that they have serious problems with a certain hardware and OS combination, which needs further investigation.</td>
</tr>
<tr>
<td>Data</td>
<td>Document Type</td>
<td>Lets you add, edit, and delete document types. The document type defines the file format of a document that is imported to the Document Management system. The users who import documents can specify the document type. However, users can import files of types other than those that are defined. See “About Document Management” on page 346.</td>
</tr>
<tr>
<td>Data</td>
<td>Document Category Type</td>
<td>Lets you add, edit, and delete document category types. The document category type provides an additional means of grouping and organizing the document categories. You can sort the category display on the Documents page by document category type instead of alphabetically. See “About Document Management” on page 346.</td>
</tr>
</tbody>
</table>
## Commands on the Admin menu (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Hierarchy Data Service</td>
<td>Lets you add, edit, and delete incident categories and hierarchy items. ServiceDesk uses categories to classify incidents. You can use additional levels of classification items to further identify the incidents. The main categories and the additional classification items are referred to as the data hierarchy. See “About Incident Management classifications and the data hierarchy” on page 499.</td>
</tr>
<tr>
<td>Data</td>
<td>User Relationship Type</td>
<td>Lets you add, edit, and delete user relationship types. User relationship types define the relationships that users can have to other users and to groups. User relationship types can reflect that one user is the manager of another, or that a user is a member of a group. You can base incident assignment on relationships. For example, an incident is assigned to the support group. If the incident is not resolved after two days, it is assigned to the most senior person in that group. The assignment process only needs to know of the relationship to use for assignment, not the specific users. Therefore, if the most senior support worker changes, the assignments follow automatically.</td>
</tr>
<tr>
<td>Data</td>
<td>Profile Reference Type</td>
<td>Lets you add or edit a profile reference type. This option is available only if Workflow Solution is installed. You might want to call support for assistance if you plan to change or add profile reference types. Profiles let you define data. When you set up a profile, you set up the pieces of data that you want to see in different ServiceDesk items. ServiceDesk items include articles, schedules, or documents. For example, if you work with mortgage applications, you might want to know the property address, assessed value, and other information on the properties. Setting up profile reference types lets you define the property-specific data that you want to see.</td>
</tr>
<tr>
<td>Data</td>
<td>Process Type Actions</td>
<td>Lets you add, edit, and delete Process Type Actions on the Process View pages for Incident and Change Management. Process Type Actions are the links that let you perform other processes from the incident and the change request tickets’ Process View page. See “About Process Type Actions on the Process View pages” on page 106.</td>
</tr>
<tr>
<td>Command</td>
<td>Subcommand</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data</td>
<td>Business Hours</td>
<td>Lets you add, edit, and delete business hours configurations. You can set up your business hours and holidays based on your business locations and SLA policy. You can use these business hours and holidays to set up routing rules so that incidents are routed to specific service queues during business hours. You can also set up routing rules so that incidents are routed to specific queues during non-business hours, weekends, and holidays.</td>
</tr>
<tr>
<td></td>
<td>Master Settings</td>
<td>Lets you configure the master settings for the Process Manager portal, which determine the behavior of the ServiceDesk application software and portal. See “About the Process Manager portal master settings” on page 530.</td>
</tr>
<tr>
<td></td>
<td>Manage Pages</td>
<td>Lets you manage all the pages in the Process Manager portal. You can import, edit, delete, export, and move pages up and down the menu list. You can also add root pages and subpages, and make a root page a subpage. The Process Manager portal is a Web-based interface that provides access to the ServiceDesk application software. Most of the work in ServiceDesk is performed in a portal page or in a page that is accessed from a portal page. See “About the Process Manager portal” on page 52.</td>
</tr>
<tr>
<td></td>
<td>Plugin Upload</td>
<td>Lets you upload plugins, web parts, resources, or pages. For example, you can create a workflow project that you can upload as a plugin. You can create a workflow for the Document Management process, which requires users to go through several steps before a document is approved. You can load that workflow project into the Process Manager portal as a plugin.</td>
</tr>
<tr>
<td></td>
<td>Web Parts Catalog</td>
<td>Lets you add new Web parts to the catalog, and edit and delete existing Web parts.</td>
</tr>
<tr>
<td></td>
<td>Not applicable</td>
<td>Lets you manage the Service Catalog items. You can set the permissions on which ServiceDesk users, groups, and organizational units have access to the specific forms. You can also edit, rename, create, and delete Service Catalog items and categories, and modify Service Catalog item attributes such as the form size.</td>
</tr>
</tbody>
</table>
### Table 45-1: Commands on the Admin menu (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Accounts</td>
<td>Lets you manage the various ServiceDesk user, group, permission, and organization accounts. This command has the following subcommands:</td>
</tr>
</tbody>
</table>
|                       |                     | ■ Manage Users
|                       |                     |  Lets you add, edit, and delete users. You can also manage groups, organizations, and permissions for users, merge users, and set user relationships. In addition, you can set the Users password, enable or disable the user, add credit cards, transactions, and key value pairs for the user. |
|                       |                     | ■ List Permissions
|                       |                     |  Lets you add, edit, and delete permissions and view the users and groups that are assigned a certain permission.                                                                                          |
|                       |                     | ■ List Groups
|                       |                     |  Lets you add, edit, and delete groups, add users to groups, add permissions to groups, and remove users from groups.                                                                                    |
|                       |                     | ■ List Organizations
|                       |                     |  Lets you add, edit, and delete organizations, add users and permissions to organizations, and remove users from organizations.                                                                           |
| Users                 | AD Users            | Lets you view the current list of users in Active Directory and select users to update.                                                                                                                     |
| Users                 | Manage Delegations  | Lets you add and delete delegations for users.                                                                                                                                                               |
| Active Directory      | Sync Profiles       | Lets you add and manage the Active Directory sync profiles that you can create in ServiceDesk. See “Managing Active Directory sync profiles” on page 483.                                                         |
| Active Directory      | Sync Profile Schedule | Lets you configure schedules for automatically synchronizing your profiles with Active Directory. Lets you configure schedules for full syncs and for update syncs. For example, you can schedule a full sync to occur weekly and an update sync to occur daily. |
| Reports               | Report Schedule List | Lets you configure the schedules that automatically execute and email reports. See “Creating a report schedule” on page 414.                                                                                |
| Manage KB Synonyms    | Not applicable      | Lets you add, edit, and delete knowledge base synonyms.                                                                                                                                                     |
### Table 45-1  Commands on the Admin menu (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Automation</td>
<td>Not applicable</td>
<td>Lets you configure automation rules for any workflow-based application, which includes service automation library. Automation rules let the administrator configure the Incident Management and the Change Management processes.</td>
</tr>
</tbody>
</table>

---

### About application properties

ServiceDesk contains a set of default application properties named `ServiceDeskSettings`, which the components in Workflow Designer and Workflow Solution can use. The application properties are also referred to as profile properties in the Workflow products.

A best practice in the Workflow products is to reference the application properties instead of hard-coding values. If you need to change certain values, change them on the Application Properties page in ServiceDesk.

For example, instead of hard-coding the group “Support” in a component, you can use the application property for that group instead, as follows:

```
[ProfileProperties]service_desk_settings_group_support
```

When changes are made to the application property, the changes are automatically reflected in Workflow. Some of the values that you might change are the priority, impact, urgency, or URLs for processes.

For example, you can link to a page in your organization’s intranet from multiple ServiceDesk processes by defining an application property for the page’s URL. When you add that property to ServiceDesk forms, the intranet link appears on the pages that result from those forms.

The Application Properties page is available on the Admin menu.

See “Commands on the Admin menu” on page 523.

---

### About incident close codes

When an incident is closed, the support technician must provide a close code to indicate the nature of the resolution.

ServiceDesk contains a set of predefined close codes that are ready to use. If necessary, you can delete or add to the default close codes. You can edit the incident close codes in the Process Manage portal on the Applications Properties page.
Close codes let you select a code that indicates the nature of the resolution. The default close codes are as follows:

- Advice Given
- Change Required
- Completed Success
- Monitoring Required
- No Fault Found
- Other
- Review Documentation
- Training Required
- Other

See “Adding and deleting incident close codes” on page 529.

**Adding and deleting incident close codes**

ServiceDesk contains a set of predefined close codes that are used when an incident is resolved. If necessary, you can delete or add to the default close codes.

See “About incident close codes” on page 528.

Deleting a close code does not affect any process tickets that contain that close code. The tickets retain the close code, which is visible as usual when you view the tickets. Any reports that refer to a deleted close code still work.

**To add or delete incident close codes**

1. In the Process Manager portal, click **Admin > Data > Application Properties**.
2. On the **Applications Properties** page, under **Application Properties Profiles**, click **ServiceDeskSettings**.
3. At the far right of the **ServiceDeskSettings** title bar, click the **Actions** symbol (orange lightning), and then click **Edit Values**.
4. In the **Edit Profile Definition Instance** dialog box, scroll down to **CloseCodes**, and under the list of close codes, click **Edit**.
In the dialog box that appears, take any of the following actions:

To add a close code: In the box at the bottom of the dialog box, type the new close code, and then click Add.

To delete a close code: Click the Delete symbol (a red X) to the right of the close code.

When you finish editing the close codes, click Save.

In the Edit Profile Definition Instance dialog box, click Save.

About the Process Manager portal master settings

The Process Manager portal master settings determine the behavior of the ServiceDesk application software and portal.

The Process Manager portal master settings are established during the installation of the ServiceDesk application software. You can use the default settings or you can edit them as necessary. We recommend that you review the settings to familiarize yourself with them and then customize them for your organization.

See “Editing the Process Manager portal master settings” on page 530.

Examples of the types of settings that you might change are as follows:

- Settings under the Account Management section
  - PasswordExpireMonths, RegisterFailEmailaddress, and SecurityQuestion

- Settings under the Workflow Settings section
  - WorkflowTaskDueDate and WorkflowTaskLateDate

Do not change the settings for URLs or disable check boxes without fully understanding the ramifications. Few organizations need to change that type of information.

The portal master settings are arranged in sections. Expand each section to see the settings that appear there.

Editing the Process Manager portal master settings

The Process Manager portal master settings determine the behavior of the ServiceDesk application software and portal.
Although default master settings are established during the installation of the ServiceDesk application software, you can edit them to customize them for your organization.

See “About the Process Manager portal master settings” on page 530.

Do not change the settings for URLs or disable check boxes without fully understanding the ramifications. Few organizations need to change that type of information.

To edit the Process Manager portal master settings

1 In the Process Manager portal, click Admin > Portal > Master Settings.
2 On the Process Manager Settings page, expand the section that contains the settings that you want to edit.
3 Change the settings as necessary.
4 Continue to expand and edit additional sections as needed.
5 When you finish reviewing and editing the settings, at the lower right of the page, click Save.

Master Settings: Process Manager Active Directory Settings section

This section lets you edit the method for authenticating the users who log on to the Process Manager portal. If you use Active Directory authentication, you can also configure the interval for running the AD synchronization and performing other AD-related functions.

See “About ServiceDesk authentication” on page 450.

This section appears on the Process Manager Settings page.

See “About the Process Manager portal master settings” on page 530.

Table 45-2 Options in the Process Manager Active Directory Settings section

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory Authentication</strong></td>
<td>Lets you specify whether to use Active Directory for creating and authenticating the users who log on to the Process Manager portal.</td>
</tr>
<tr>
<td><strong>Convert Native Users to Active Directory User</strong></td>
<td>Lets you specify whether to convert native users to Active Directory users for authenticating the users who log on to the Process Manager portal.</td>
</tr>
</tbody>
</table>
### Table 45-2

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process AD Changes Using Workflow</td>
<td>This option is not available from the Process Manager portal because it does not apply to ServiceDesk.</td>
</tr>
<tr>
<td>Ignore AD Users (Comma separated)</td>
<td>Lets you specify any Active Directory users that should not be imported to ServiceDesk. You can type one or more user names and separate them with commas.</td>
</tr>
</tbody>
</table>

If you need to add, edit, and maintain the Active Directory server connections, you can do so from Workflow Explorer.

See “Managing Active Directory server connections” on page 469.

After you add and Active Directory server connection, you can add sync profiles. You can use these sync profiles to target the entire domain, organizational units and groups on the AD server, or for specific LDAP queries.

See “Managing Active Directory sync profiles” on page 483.

### Creating user relationship types

You can customize ServiceDesk so that process tickets can be assigned based on relationships. For example, if an incident is not completed in time, it can escalate from the original worker to that worker’s supervisor. The relationships can be between users, groups, permissions, or organizational units.

**To create a user relationship type**

1. In the Process Manager portal, click **Admin > Data > User Relationship Type**.
2. Click the **Add Relationship Type** symbol (green plus sign).
3. In the **Add Relationship Type** dialog box, type the name for the relationship.
4. In the **Relates To** drop-down list, select the type of relationship.
   - The relationship can relate to users, groups, permissions, or organizational units.
5. Click **Save**.
Default permissions in ServiceDesk

This appendix includes the following topics:

- Default ServiceDesk permissions by category
- Default ServiceDesk user groups

Default ServiceDesk permissions by category

ServiceDesk contains the default permissions that determine what screens users can access and what actions they can perform in the Process Manager portal.

Administrators and users with the appropriate permissions can view all the default permissions in the Process Manager portal. They can also edit the permission information.

See “Viewing the list of ServiceDesk permissions” on page 457.

On the List Permissions page, the Browse Permissions section lists the permission categories. The categories organize the permissions by function. When you click a category, the permissions for that category appear at the right of the page.

When you assign a permission to a user, group, service queue, or other entity, the permission name is displayed as a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.
<table>
<thead>
<tr>
<th>Permission category</th>
<th>Permission name</th>
<th>Permission granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>CompanyAdministration</td>
<td>Add or remove users to or from the organizational unit to which the user belongs.</td>
</tr>
<tr>
<td>Account</td>
<td>CompanyAdministration.PasswordReset</td>
<td>Reset passwords for users in the organizational unit to which the user belongs.</td>
</tr>
<tr>
<td>Account</td>
<td>ManageDelegations</td>
<td>Manage the delegations for others users.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>Access</td>
<td>Access everything in the Users area of the Admin module.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>Group.Create</td>
<td>Create a new group.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>Group.Modify</td>
<td>Modify an existing group.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>Permission.Create</td>
<td>Create a new permission.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>Permission.Modify</td>
<td>Modify an existing permission.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>Retrieve.Reference.Name</td>
<td>See reference names. This permission is used in a UserMan method that is called GetReferenceName which is then used in Components.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>User.CanResetPassword</td>
<td>Reset another user’s password.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>User.Create</td>
<td>Create new users.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>User.FetchInfo</td>
<td>Retrieve a user’ information.</td>
</tr>
<tr>
<td>AccountManagement</td>
<td>User.Modify</td>
<td>Modify an existing user.</td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td>Application permissions are related to the enterprise repository, and any applications permissions can be safely ignored.</td>
</tr>
<tr>
<td>Articles</td>
<td>Access</td>
<td>Access the knowledge base.</td>
</tr>
<tr>
<td>Articles</td>
<td>CanAddArticle</td>
<td>Add or update knowledge base articles.</td>
</tr>
<tr>
<td>Articles</td>
<td>CanAddCategory</td>
<td>Add categories.</td>
</tr>
<tr>
<td>Permission category</td>
<td>Permission name</td>
<td>Permission granted</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Articles</td>
<td>CanDeleteArticle</td>
<td>Delete knowledge base articles.</td>
</tr>
<tr>
<td>Articles</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>Discussions</td>
<td>Access</td>
<td>Access the threaded discussions module.</td>
</tr>
<tr>
<td>Discussions</td>
<td>Administrator</td>
<td>Remove and edit posts. The user with this administrative permission is the discussion moderator.</td>
</tr>
<tr>
<td>Discussions</td>
<td>Create</td>
<td>Create discussions.</td>
</tr>
<tr>
<td>Discussions</td>
<td>GroupManagement</td>
<td>Create and manage discussion threads on the <strong>Discussions</strong> page.</td>
</tr>
<tr>
<td>Discussions</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>DocumentManagement</td>
<td>Access</td>
<td>Access the document management module.</td>
</tr>
<tr>
<td>DocumentManagement</td>
<td>CanAddRootCategory</td>
<td>Add root categories to the document management module.</td>
</tr>
<tr>
<td>DocumentManagement</td>
<td>CanCheckoutDocuments</td>
<td>Check out documents from the document management module.</td>
</tr>
<tr>
<td>DocumentManagement</td>
<td>CanEditDocumentTypes</td>
<td>Edit the document types that are allowed in the document management module.</td>
</tr>
<tr>
<td>DocumentManagement</td>
<td>CanPostDocumentsForOther</td>
<td>Can add documents on behalf of other users.</td>
</tr>
<tr>
<td>DocumentManagement</td>
<td>CanViewCategoryHistory</td>
<td>View the category history in the document management module.</td>
</tr>
<tr>
<td>DocumentManagement</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>Permission category</td>
<td>Permission name</td>
<td>Permission granted</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>ProcessManager</td>
<td>User.Interface.Beta</td>
<td>Access pre-release versions of the beta portal pages. Even with this permission, a user might not see beta pages.</td>
</tr>
<tr>
<td>Forms</td>
<td>Access</td>
<td>Access the Service Catalog module.</td>
</tr>
<tr>
<td>Forms</td>
<td>Create</td>
<td>Create new forms.</td>
</tr>
<tr>
<td>Forms</td>
<td>Delete</td>
<td>Delete existing forms.</td>
</tr>
<tr>
<td>Forms</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>Access</td>
<td>Access the Hierarchy Data Service.</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>Portal</td>
<td>Admin</td>
<td>Perform most portal actions, such as creating portal pages, deleting portal pages, and editing portal pages.</td>
</tr>
<tr>
<td>Portal</td>
<td>CanAddPages</td>
<td>Create new portal pages.</td>
</tr>
<tr>
<td>Portal</td>
<td>PersonalCustomization</td>
<td>Customize a portal page. Other users cannot see these customizations. Customization is allowed only on the pages for which customization has been enabled.</td>
</tr>
<tr>
<td>Portal</td>
<td>SuperAdmin</td>
<td>Access all portal functions. This permission lets you make changes to the Process Manager portal to ensure that it functions properly. For example, if a user with the Portal.Admin permission accidentally denies their own access to a portal area, the Superadmin user can reset that permission.</td>
</tr>
<tr>
<td>ProcessData</td>
<td>Access</td>
<td>Access the reports module.</td>
</tr>
</tbody>
</table>
## Table A-1  Default ServiceDesk permissions by category (continued)

<table>
<thead>
<tr>
<th>Permission category</th>
<th>Permission name</th>
<th>Permission granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProcessData</td>
<td>CanViewFullProcessViewPage</td>
<td>View the entire process view page. This permission does not override other permissions. To see the full process view page, a user needs this permission and permission to view all of the parts on the page.</td>
</tr>
<tr>
<td>ProcessData</td>
<td>DefineFilters</td>
<td>Define filters for reports.</td>
</tr>
<tr>
<td>ProcessData</td>
<td>Reports</td>
<td>View a particular report.</td>
</tr>
<tr>
<td>ProcessData</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>ProcessData</td>
<td>ViewAll</td>
<td>View all the processes. This permission is a super administrator privilege for processes.</td>
</tr>
<tr>
<td>ProcessData</td>
<td>WriteReports</td>
<td>Create reports.</td>
</tr>
<tr>
<td>Profile</td>
<td>Access</td>
<td>Access the Profiles module.</td>
</tr>
<tr>
<td>Profile</td>
<td>CanViewTree</td>
<td>View the profile tree.</td>
</tr>
<tr>
<td>Profile</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>Reports</td>
<td>Access</td>
<td>Access the reporting module.</td>
</tr>
<tr>
<td>Reports</td>
<td>Access.ReplicationSchedule</td>
<td>Access the replication schedule.</td>
</tr>
<tr>
<td>Reports</td>
<td>OLAP.Create</td>
<td>Create OLAP reports.</td>
</tr>
<tr>
<td>Reports</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>Reports</td>
<td>ViewRDD</td>
<td>View a report as RSS.</td>
</tr>
<tr>
<td>Schedules</td>
<td>Access</td>
<td>Access the schedules module.</td>
</tr>
<tr>
<td>Schedules</td>
<td>CanCreate</td>
<td>Create schedules.</td>
</tr>
<tr>
<td>Schedules</td>
<td>CanDelete</td>
<td>Delete schedules.</td>
</tr>
<tr>
<td>Permission category</td>
<td>Permission name</td>
<td>Permission granted</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Schedules</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
<tr>
<td>ServiceDesk</td>
<td>CanViewAllIncidents</td>
<td>View all incidents in ServiceDesk.</td>
</tr>
<tr>
<td>ServiceDesk</td>
<td>CanViewChangeSchedules</td>
<td>View the change schedules and release schedules.</td>
</tr>
<tr>
<td>ServiceDesk</td>
<td>CanViewProblemManagementTickets</td>
<td>View all the problem tickets in ServiceDesk.</td>
</tr>
<tr>
<td>ServiceDesk</td>
<td>Incident.CanSelectAssignment</td>
<td>Select a specific person to assign a task to.</td>
</tr>
<tr>
<td>UserLicenseLevel</td>
<td>ProcessManager</td>
<td>Access the Process Manager portal.</td>
</tr>
<tr>
<td>UserLicenseLevel</td>
<td>ServiceDesk</td>
<td>Access ServiceDesk.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>Access</td>
<td>Access the Workflow tasks.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>Add</td>
<td>Add Workflow tasks.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>AllowBreakLeases</td>
<td>Break a leased task.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>CanCloseAnyTask</td>
<td>Close any task, including the tasks that are not assigned to the user who has this permission. This permission is generally granted to administrators only.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>CanCompleteAnyTask</td>
<td>Complete any task, including the tasks that are not assigned to the user who has this permission.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>CanManageAttributes</td>
<td>Maintain task attributes.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>CanRemoveTask</td>
<td>Remove any task, including the tasks that are not assigned to the user who has this permission.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>CanSetupDefaultProfile</td>
<td>Set up the default profile.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>Modify</td>
<td>Modify any task, including the tasks that are not assigned to the user who has this permission.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>ShowInMenu</td>
<td>View this module on the tab bar or menu bar in the Process Manager portal.</td>
</tr>
</tbody>
</table>
Table A-1  Default ServiceDesk permissions by category (continued)

<table>
<thead>
<tr>
<th>Permission category</th>
<th>Permission name</th>
<th>Permission granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>WorkflowTasksManagement</td>
<td>ViewAllTasks</td>
<td>View all the tasks in ServiceDesk, including the tasks that are not assigned to the user who has this permission.</td>
</tr>
<tr>
<td>WorkflowTasksManagement</td>
<td>ViewUnassignedTasks</td>
<td>View all the unassigned tasks in ServiceDesk, including the tasks that are not assigned to the user who has this permission.</td>
</tr>
</tbody>
</table>

Default ServiceDesk user groups

The ServiceDesk provides default user groups. Each group has predefined permissions that the users inherit when you make them members of the group.

See “About group-level permissions” on page 449.

Administrators and users with the appropriate permissions can view all the default permissions in the Process Manager portal. They can also edit the permission information.

See “Adding or removing permissions for groups” on page 456.

Table A-2  Default ServiceDesk user groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>Contains the users who administer ServiceDesk.</td>
</tr>
<tr>
<td></td>
<td>The Administrators group is granted all available permissions and can access all the tabs in the Process Manager portal.</td>
</tr>
<tr>
<td>All Users</td>
<td>Contains all ServiceDesk users with valid accounts.</td>
</tr>
<tr>
<td></td>
<td>All users can create requests, view and confirm their resolved incidents, access the knowledge base, and perform other common tasks. They can also perform other actions, which depend on what other groups the users belongs to.</td>
</tr>
<tr>
<td></td>
<td>See “Default permissions for the All Users group” on page 541.</td>
</tr>
<tr>
<td>Application Users</td>
<td>See “Default permissions for the Application Users group” on page 542.</td>
</tr>
<tr>
<td>Group</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change Approvers</td>
<td>Contains the users who can approve changes. They are typically members of the change approval board (CAB). They can advise the change manager in the assessment, prioritization, and scheduling of changes. Change approvers can create incidents and problems, request changes, approve changes, and view and work tasks. They can also run reports, and submit knowledge base articles. See “Default permissions for the Change Approvers group” on page 544.</td>
</tr>
<tr>
<td>Change Manager</td>
<td>Contains the users who orchestrate changes by assigning roles to change implementers. Change Managers have the final sign-off on changes. Change managers can create incidents and problems, request changes, approve changes, and view and work tasks, including the tasks that are assigned to others. They can also view all tickets, run reports, and submit knowledge base articles. See “Default permissions for the Change Manager group” on page 545.</td>
</tr>
<tr>
<td>KB Approvers</td>
<td>Contains the users who are assigned to approve knowledge base articles. KB (knowledge base) approvers can create incidents and problems, request changes, and work their assigned tasks. They can also view all tickets and edit the knowledge base entries. See “Default permissions for the KB Approvers group” on page 547.</td>
</tr>
<tr>
<td>KB Editors</td>
<td>Contains the users who are assigned to review and edit knowledge base articles. KB editors can create incidents and problems, request changes, and work their assigned tasks. They can also view all tickets and edit the knowledge base entries. See “Default permissions for the KB Editors group” on page 549.</td>
</tr>
<tr>
<td>Problem Analysts</td>
<td>Contains the users who are assigned to work on problems. Problem analysts can create incidents and problems, request changes, and view and work tasks, including the tasks that are assigned to others. They can also view all tickets, run reports, and submit knowledge base articles. See “Default permissions for the Problem Analysts group” on page 550.</td>
</tr>
<tr>
<td>Problem Reviewers</td>
<td>Contains the users that are one level higher than Problem Analysts. These users have approval rights for problems, and review and implement problem resolution proposals submitted by Problem Analysts. Problem Reviewers can create incidents and problems, request changes, work tasks (including those assigned to others), view tickets, submit knowledge base articles, and run reports. See “Default permissions for the Problem Reviewers group” on page 552.</td>
</tr>
</tbody>
</table>
## Default permissions for the All Users group

By default, the All Users group can access the following tabs in the Process Manager portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Knowledge Base**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the All Users group are as follows:

- AccountManagement.User.FetchInfo
- Application.Access
- Articles.Access
Default permissions for the Application Users group

By default, the Application Users group can access the following tabs in the Process Manager portal:

- Home
- Submit Request
- My Task List
Knowledge Base

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the Application Users group are as follows:

- AccountManagement.User.FetchInfo
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- Forms.Access
- ProcessData.Access
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- ProcessManager.ShowNotifications
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access
- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
WorkflowTaskManagement.Access

See “Default ServiceDesk user groups” on page 539.

Default permissions for the Change Approvers group

By default, the Change Approvers group can access the following tabs in the Process Manager portal:

- Home
- Submit Request
- My Task List
- Tickets
- Technician Dashboard
- Knowledge Base
- Documents
- Reports

Administrators and users with the appropriate permissions can view and edit the group permissions.

See “Viewing the permissions for a group” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the Change Implementers group are as follows:

- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
Default permissions for the Change Manager group

By default, the Change Manager group can access the following tabs in the Process Manager portal:

- Home
Administrators and users with the appropriate permissions can view and edit the group permissions.

See “Viewing the permissions for a group” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the Change Manager group are as follows:

- AccountManagement.Access
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
Default permissions for the KB Approvers group

By default, the KB Approvers group can access the following tabs in the Process Manager portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Knowledge Base**
- **Documents**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See “**Viewing the permissions for a group**” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “**Default ServiceDesk permissions by category**” on page 533.
The default permissions for the KB Approvers group are as follows:

- Articles.Access
- Articles.CanAddArticle
- Articles.CanDeleteArticle
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanAddRootCategory
- DocumentManagement.CanCheckoutDocuments
- DocumentManagement.CanEditDocumentTypes
- DocumentManagement.CanPromoteDocumentVersions
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.CanViewHiddenCategories
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access
By default, the KB Editors group can access the following tabs in the Process Manager portal:

- Home
- Submit Request
- My Task List
- Tickets
- Knowledge Base
- Documents

Administrators and users with the appropriate permissions can view and edit the group permissions.

See “Viewing the permissions for a group” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the KB Editors group are as follows:

- Articles.Access
- Articles.CanAddArticle
- Articles.CanDeleteArticle
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
Default permissions for the Problem Analysts group

By default, the Problem Analyst group can access the following tabs in the Process Manager portal:

- **Home**
- **Submit Request**
Administrators and users with the appropriate permissions can view and edit the group permissions.

See “Viewing the permissions for a group” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the Problem Analyst group are as follows:

- AccountManagement.Access
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
ProcessData.WriteReports
Profile.Access
Profile.CanViewTree
Reports.Access
Reports.OLAP.Create
Reports.ShowInMenu
Schedules.Access
Schedules.ShowInMenu
ServiceDesk.CanViewAllIncidents
UserLicenseLevel.ServiceDesk
WorkflowTaskManagement.Access

See “Default ServiceDesk user groups” on page 539.

Default permissions for the Problem Reviewers group

By default, the Problem Reviewer group can access the following tabs in the Process Manager portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Supervisor Dashboard**
- **Knowledge Base**
- **Documents**
- **Reports**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See “Viewing the permissions for a group” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.
The default permissions for the Problem Reviewer group are as follows:

- AccountManagement.Access
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Reports.ShowInMenu
- Schedules.Access
- Schedules.ShowInMenu
- ServiceDesk.CanViewAllIncidents
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See “Default ServiceDesk user groups” on page 539.
Default permissions for the Service Managers group

By default, the Service Managers group can access the following tabs in the Process Manager portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Supervisor Dashboard**
- **Knowledge Base**
- **Documents**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See “Viewing the permissions for a group” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the Service Managers group are as follows:

- **AccountManagement.Access**
- **AccountManagement.User.FetchInfo**
- **Applications.DirectoryService.DefaultAccess**
- **Articles.Access**
- **Articles.ShowInMenu**
- **Discussions.Access**
- **Discussions.Create**
- **Discussions.GroupManagement**
- **Discussions.ShowInMenu**
- **DocumentManagement.Access**
- **DocumentManagement.CanViewCategoryHistory**
- **DocumentManagement.CanViewDocumentHistory**
- **DocumentManagement.ShowInMenu**
Default permissions in ServiceDesk

Default ServiceDesk user groups

By default, the Support group can access the following tabs in the Process Manager portal:

- [Home]
- [Submit Request]
- [My Task List]
- [Tickets]

See “Default ServiceDesk user groups” on page 539.
Administrators and users with the appropriate permissions can view and edit the group permissions.

See “Viewing the permissions for a group” on page 457.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See “Default ServiceDesk permissions by category” on page 533.

The default permissions for the Support group are as follows:

- AccountManagement.Access
- AccountManagement.User.FetchInfo
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
■ ProcessData.WriteReports
■ Profile.Access
■ Profile.CanViewTree
■ Reports.Access
■ Reports.OLAP.Create
■ Reports.ShowInMenu
■ Schedules.Access
■ ServiceDesk.Pages.FullIncidentView
■ ServiceDesk.Pages.Search
■ ServiceDesk.Pages.TechDashboard
■ ServiceDesk.Pages.Tickets
■ ServiceDesk.Reports.Run.Change
■ ServiceDesk.Reports.Run.Incident
■ ServiceDesk.Reports.Run.Problem
■ ServiceDesk.Services.Items.AdvancedIncident
■ WorkflowTaskManagement.Access
■ WorkflowTaskManagement.ViewUnassignedTasks

See “Default ServiceDesk user groups” on page 539.
Default permissions in ServiceDesk

Default ServiceDesk user groups
Default categories in ServiceDesk

This appendix includes the following topics:

- Default categories for incidents and default classifications for problems

Default categories for incidents and default classifications for problems

ServiceDesk uses categories to classify incidents and route them to the appropriate incident technician or group queue. The person that creates the incident can select a category for that incident. The category also helps sort incidents for reports. ServiceDesk also uses classifications to classify problems. During the initial problem analysis, the problem analyst can select a classification for the problem.

ServiceDesk contains predefined incident categories and problem classifications, which can be used immediately or edited to meet your organization’s requirements.

<table>
<thead>
<tr>
<th>Main category or classification</th>
<th>Category or classification level 2</th>
<th>Category or classification level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Desktop</td>
<td>■ Backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Disk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Office</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ PC Personality</td>
</tr>
<tr>
<td>Main category or classification</td>
<td>Category or classification level 2</td>
<td>Category or classification level 3</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Hardware</td>
<td>Drive</td>
<td>N/A</td>
</tr>
<tr>
<td>Hardware</td>
<td>Handheld</td>
<td>Can’t Sync</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>Hardware</td>
<td>Keyboard</td>
<td>N/A</td>
</tr>
<tr>
<td>Hardware</td>
<td>Monitor</td>
<td>N/A</td>
</tr>
<tr>
<td>Hardware</td>
<td>Mouse</td>
<td>N/A</td>
</tr>
<tr>
<td>Hardware</td>
<td>Notebook</td>
<td>Backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Docking Station</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fax</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Machine Discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>Hardware</td>
<td>Phone</td>
<td>No Dial Tone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reset Voice Mail Pin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voice Mail Not Working</td>
</tr>
<tr>
<td>Hardware</td>
<td>Printer</td>
<td>Jammed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Out of Toner</td>
</tr>
<tr>
<td>Hardware</td>
<td>Server</td>
<td>CPU or Blade</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>Main category or classification</td>
<td>Category or classification level 2</td>
<td>Category or classification level 3</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>How To</td>
<td>■ Access Email</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>■ Access the Web</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Install Printer Drivers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Other</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Recover Deleted Files</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Use Handheld</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ View Email Attachment</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>■ Can't Browse Web Site</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>■ Other</td>
<td></td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Network</td>
<td>■ Can't Access Some Resources</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>■ No Connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Other</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Can't Send Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Email Won't Run</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Not Receiving Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Other</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>■ Deployment Failure</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>■ Migration Failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Operating System</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Other</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Sw Delivery Failure</td>
<td></td>
</tr>
</tbody>
</table>
Default categories in ServiceDesk

Default categories for incidents and default classifications for problems
ServiceDesk reporting data dictionary

This appendix includes the following topics:

- ServiceDesk reporting data dictionary

ServiceDesk reporting data dictionary

All ServiceDesk reportable data is stored in the Process Manager database. The Process Manager database holds data that is required for general Process Manager database operations. This instruction provides information about the tables that commonly hold reported data and the relationship of these tables to each other.

<table>
<thead>
<tr>
<th>Tables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item Base Tables</td>
<td>These tables contain base data about an item.</td>
</tr>
<tr>
<td>Item Detail Tables</td>
<td>These tables contain additional details for Item Base Tables.</td>
</tr>
<tr>
<td>Process Data Tables</td>
<td>These tables contain process data for ServiceDesk or custom processes.</td>
</tr>
<tr>
<td></td>
<td>These tables are expressed as ProcessProfiles in the Process Manager portal.</td>
</tr>
<tr>
<td>Reference / Relationship Tables</td>
<td>These tables are used to manage the relationship between records without adding additional detail fields.</td>
</tr>
</tbody>
</table>

Several common keys are used to link records across these different tables. Depending on the table, the key fields in the table may have different names than their key values. Use these key field types to link the various tables.
### Table C-2  Main types of key fields in the tables

<table>
<thead>
<tr>
<th>Key field</th>
<th>Description</th>
</tr>
</thead>
</table>
| SessionID   | ■ Sometimes called the WorkflowTrackingID.  
  ■ This field is a GUID that is unique to each instance of a Workflow or ServiceDesk process. |
| ProcessID   | ■ A sequential number  
  ■ This field is the TicketID for a ServiceDesk process and the ReportID for a custom Workflow process.  
  ■ For example, IM-00003 is the TicketID number for an incident in the Incident Management process in ServiceDesk. |
| UserID      | ■ Generally, the GUID ID for the user  
  Does not apply to the default admin and guest user accounts.  
  ■ If the user comes from Active Directory, the UserID is the same UserID GUID from Active Directory. |
| UserPrimaryEmail | ■ The primary email address for the user on record. |
| TaskID      | ■ A GUID that is unique to each task.  
  ■ A single SessionID can have many tasks, but a task can only report to a single SessionID. |
| GroupID     | ■ A GUID ID for a Process Manager group.  
  ■ Tasks can be assigned to either users or groups. |

### Table C-3  ServiceDesk Reporting data dictionary

<table>
<thead>
<tr>
<th>Table name</th>
<th>Table type</th>
<th>Field name</th>
<th>Field type</th>
<th>Key field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReportProcess</td>
<td>Item Base</td>
<td>ReportProcessID</td>
<td>nvarchar</td>
<td>ProcessID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LogonUserIdentity</td>
<td>nvarchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AnonymousID</td>
<td>nvarchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Browser</td>
<td>nvarchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description</td>
<td>nvarchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DocumentCategoryID</td>
<td>nvarchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>InputData</td>
<td>ntext</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IsAuthenticated</td>
<td>nvarchar</td>
<td>UserID</td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------</td>
<td>-----------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>IsLocal</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IsSecure</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LanguagePreference</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LastElapsedTime</td>
<td>bigint</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModelInWhichComponentWasRun</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PercentComplete</td>
<td>tinyint</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PriorityColor</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PriorityName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProcessEnded</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProcessName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProcessStarted</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProcessTitle</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProcessViewerPageID</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProjectName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ReferralURL</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ReportLogProcessID</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Result</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ResultAnnotation</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ResultData</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ResultIDData</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ScheduledComplete</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServiceID</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UrlOfProcess</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table C-3  ServiceDesk Reporting data dictionary (continued)

<table>
<thead>
<tr>
<th>Table name</th>
<th>Table type</th>
<th>Field name</th>
<th>Field type</th>
<th>Key field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReportProcessComment</td>
<td>Item Detail</td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UserName</td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comment</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CommentBrief</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ComponentID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DatePosted</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExecutionOrder</td>
<td>bigint</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ModelName</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ProcessViewMessage</td>
<td>tinyint</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReportProcessCommentID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ViewLevel</td>
<td>tinyint</td>
<td></td>
</tr>
<tr>
<td>ReportProcessContact</td>
<td>Item Detail</td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReferenceID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ContactNotes</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ContactType</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DateContactAdded</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IsPrimary</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReferenceType</td>
<td>tinyint</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReportProcessContactID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ReportProcessHistory</td>
<td>Item Detail</td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UserName</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ComponentExecutedMessage</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>-------------------------------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>ComponentExecuted</td>
<td></td>
<td>Name</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ComponentID</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ComponentType</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ExecutionOrder</td>
<td></td>
<td></td>
<td>bigint</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td></td>
<td></td>
<td>uniqueidentifier</td>
<td></td>
</tr>
<tr>
<td>MessageBrief</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>MessageType</td>
<td></td>
<td></td>
<td>tinyint</td>
<td></td>
</tr>
<tr>
<td>ModelInWhich</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ComponentWasRun</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ProjectName</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>TimeOfExecution</td>
<td></td>
<td></td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td>UrlOfProcess</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ViewLevel</td>
<td></td>
<td></td>
<td>tinyint</td>
<td></td>
</tr>
<tr>
<td>ReportProcessStatus</td>
<td>Item Detail</td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td>History</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UserName</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td>ComponentID</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>DatePosted</td>
<td></td>
<td></td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td>ExecutionOrder</td>
<td></td>
<td></td>
<td>bigint</td>
<td></td>
</tr>
<tr>
<td>IncludeStatusChange</td>
<td></td>
<td>IncludeStatusChange</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td>InCalculation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModelName</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ReportProcessStatus</td>
<td></td>
<td>ReportProcessStatus</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>HistoryID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>StatusMessage</td>
<td></td>
<td></td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>ReportProcessTiming</td>
<td>Item Detail</td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UserID</td>
<td>nvarchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DatePosted</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExecutionOrder</td>
<td>bigint</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReportProcessTimingID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SpentOn</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TimeSpent</td>
<td>bigint</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Item Base</td>
<td>WFTaskNumberPrefix</td>
<td>nvarchar</td>
<td>ProcessID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TrackingID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TaskID</td>
<td>nvarchar</td>
<td>TaskID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CompletedBy</td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AssignedDate</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AutoDelete</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AutoDeleteDate</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CanBeCompleted</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CompletedOn</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreatedBy</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DoNotShowInTaskList</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DueDate</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FormHeight</td>
<td>int</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FormWidth</td>
<td>int</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IgnoreLeased</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IsCompleted</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>----------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LateDate</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LeasedBy</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LeasedUntil</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Originator</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Priority</td>
<td>tinyint</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RespondDisplayFormat</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TaskNumber</td>
<td>int</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TaskTypeId</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UrlOfProcess</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UrlOfResponseService</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WFTaskNumber</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>TaskAssignment</td>
<td>Item Detail</td>
<td>ReferenceType</td>
<td>tinyint</td>
<td>1 = User 2 = Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TaskID</td>
<td>nvarchar</td>
<td>TaskID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReferenceID</td>
<td>nvarchar</td>
<td>UserID or GroupID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AssignedDate</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AssignFromDate</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AssignToDate</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TaskAssignmentID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>TaskResponse</td>
<td>Item Detail</td>
<td>TaskID</td>
<td>nvarchar</td>
<td>TaskID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IsMobileType</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TaskResponseID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Title</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>User</td>
<td>Item Base</td>
<td>Manager</td>
<td>nchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UserID</td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PrimaryEmail</td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AccountActive</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AccountExpires</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ActiveDirectoryGuid</td>
<td>uniqueidentifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Address1</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Address2</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADLoginName</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BlankPasswordAllowed</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CanChangePassword</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>City</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ContactOwnerID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Country</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreatedBy</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreatedOn</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DefaultShow</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SecondaryMenu</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DisplayName</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DynamicallyTimeZone</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EmployeeID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FirstName</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>HomePage</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------</td>
<td>-------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Initials</td>
<td>nchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IsActiveDirectoryUser</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IsContact</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IsLocked</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LastLoggedInTime</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LastName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MenuRenderer</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MenuStyle</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MiddleInitial</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModifiedOn</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MustChangePassword</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NickName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office</td>
<td>nchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OrganizationTitle</td>
<td>nchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OrganizationUnit</td>
<td>nchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>binary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PasswordExpireDate</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PasswordHint</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PasswordNeverExpires</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PerUserSalt</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salutation</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Answer</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>----------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SecurityQuestion</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SelectTimeZone</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ShowNotifications</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ShowSecondaryMenu</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theme</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USNChanged</td>
<td>bigint</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebPage</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zip</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UserID</td>
<td>nvarchar</td>
<td>User ID</td>
<td></td>
<td>UserID</td>
</tr>
<tr>
<td>AddressLine1</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AddressLine2</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AddressType</td>
<td>tinyint</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>City</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CreatedBy</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CreatedOn</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModifiedOn</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UserAddressID</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zip</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UserID</td>
<td>nvarchar</td>
<td>User ID</td>
<td></td>
<td>User D</td>
</tr>
<tr>
<td>UserEmailAddress</td>
<td>Item Detail</td>
<td>UserID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreatedBy</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreatedOn</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EmailAddress</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ModifiedBy</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ModifiedOn</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SendNotifications Here</td>
<td>bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UserEmailAddressID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ReportProcessReference</td>
<td>Reference</td>
<td>ReferenceID</td>
<td>nvarchar</td>
<td>ExternalID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SessionID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReferenceType</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReportProcessReferenceID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SystemName</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Url</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ReportProcessRelationship</td>
<td>Reference</td>
<td>ChildProcessID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IsSessionJoin</td>
<td>bit</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ParentProcessID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReportProcessRelationshipID</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>CMAssignment</td>
<td>Process Data - CM</td>
<td>TicketNumber</td>
<td>nvarchar</td>
<td>ProcessID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CMChangeTicketID</td>
<td>varchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WorkflowTrackingID</td>
<td>nvarchar</td>
<td>SessionID</td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
<td>----------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>TaskID</td>
<td>nvarchar</td>
<td>TaskID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignee</td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AssignmentType</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CloseCode</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMAssignment_id</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LastComments</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TaskDescription</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TaskIsClosed</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TaskTitle</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM CabVote</td>
<td>Process Data - CM</td>
<td>CMChangeTicketId</td>
<td>varchar</td>
<td>ProcessID</td>
</tr>
<tr>
<td>TicketNumber</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkflowTrackingId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TaskId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CabMemberUserId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM Cab Vote id</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoteComments</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoteStatus</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM Change Ticket</td>
<td>Process Data - CM</td>
<td>AssignedCabId</td>
<td>varchar</td>
<td>CabID</td>
</tr>
<tr>
<td>ProcessId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM Change Ticket_id</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SessionId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ImplementationPlan</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DevelopedBy</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementer</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table C-3  ServiceDesk Reporting data dictionary (continued)
<table>
<thead>
<tr>
<th>Table name</th>
<th>Table type</th>
<th>Field name</th>
<th>Field type</th>
<th>Key field type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
<td>UserPrimaryEmail</td>
<td></td>
</tr>
<tr>
<td>Requestedby</td>
<td>nvarchar</td>
<td>UserPrimaryEmail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ActualCompletion DateTime</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ActualStartDate Time</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AssignedCab Id_type</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AssignedCabName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackoutPlan AssignedOn</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackoutPlan AssignedTo</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackoutPlan CompletedOn</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackoutPlanDetails</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackoutPlan DevelopedBy</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackoutPlanStatus</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BusinessJustification</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CabApprovalStatus</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ChangeType</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CloseCode</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CostOfImplementing</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CostOfNotImplementing</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DenialReason</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DocumentCategoryId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ImplementationPlan AssignedOn</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>ImplementationPlan</td>
<td>nvarchar</td>
<td>AssignedTo</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ImplementationPlan</td>
<td>datetime</td>
<td>CompletedOn</td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td>ImplementationPlan</td>
<td>ntext</td>
<td>Details</td>
<td>ntext</td>
<td></td>
</tr>
<tr>
<td>ImplementationPlan</td>
<td>nvarchar</td>
<td>Status</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>InitialRouting</td>
<td>nvarchar</td>
<td>GroupName</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>LocationId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LocationName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PlannedCompletionDateTime</td>
<td>datetime</td>
<td></td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td>PlannedStartDateTime</td>
<td>datetime</td>
<td></td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ReportProcessId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequestChannel</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequestDescription</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequestTitle</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequiredCompletionDate</td>
<td>datetime</td>
<td></td>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td>RiskAssessment</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskScore</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ScheduleEntryId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TemplateName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TestingPlanAssignedOn</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TestingPlanAssignedTo</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------</td>
<td>----------------------------</td>
<td>------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>TestingPlanCompletedOn</td>
<td>nvarchar</td>
<td>Testing Plan Completed On</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>Testing Plan Details</td>
<td>nvarchar</td>
<td>Testing Plan Details</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>TestingPlanDevelopedBy</td>
<td>nvarchar</td>
<td>Testing Plan Developed By</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>TestingPlanStatus</td>
<td>nvarchar</td>
<td>Testing Plan Status</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>TicketStatus</td>
<td>nvarchar</td>
<td>Ticket Status</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>Urgency</td>
<td>nvarchar</td>
<td>Urgency</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ImIncidentTicket</td>
<td>Process Data - IM</td>
<td>Currently Assigned</td>
<td>varchar</td>
<td>ImServiceQueueID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QueueId</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ProcessId</td>
<td>varchar</td>
<td>ProcessID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReportProcessId</td>
<td>varchar</td>
<td>ProcessID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SessionId</td>
<td>varchar</td>
<td>SessionID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AffectedUserId</td>
<td>varchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SubmittedById</td>
<td>varchar</td>
<td>UserID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AffectedUser</td>
<td>varchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Owner</td>
<td>varchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ResolvedBy</td>
<td>varchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SubmittedBy</td>
<td>varchar</td>
<td>UserPrimaryEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AffectedDepartment</td>
<td>varchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AffectedDepartmentId</td>
<td>varchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AffectedLocation</td>
<td>varchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AffectedLocationId</td>
<td>varchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AffectedUserID</td>
<td>varchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AppliedTemplateName</td>
<td>varchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Classification</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>HardwareManufacturer</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Classification</td>
<td>nvarchar</td>
<td>HardwareType</td>
<td>nvarchar</td>
<td></td>
</tr>
<tr>
<td>ClassificationOS</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClassificationSoftwareManufacturer</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClassificationSoftwareType</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClassificationSystemType</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CloseCode</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CurrentlyAssignedQueueId_type</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CurrentlyAssignedQueueName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DocumentCategoryId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ImIncidentTicket_id</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IncidentDescription</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IncidentGrouping</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IncidentName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IncidentType</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequestChannel</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequiredResolutionDateTime</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resolution</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ResolutionDate</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ResolvedImmediately</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>TemplateName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TicketStatus</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Urgency</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkResolveTaskId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ImServiceQueue</td>
<td>Process Data - IM</td>
<td>ImServiceQueue_id</td>
<td>varchar</td>
<td>ImServiceQueue_id</td>
</tr>
<tr>
<td>LocationId</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LocationName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QueueDescription</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QueueName</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProcessID</td>
<td>Process Data - PM</td>
<td>process_id</td>
<td>nvarchar</td>
<td>ProcessID</td>
</tr>
<tr>
<td>ProblemManagement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>change_ticket_tracking_id</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td>SessionID</td>
</tr>
<tr>
<td>session_id</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td>SessionID</td>
</tr>
<tr>
<td>tracking_id</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td>SessionID</td>
</tr>
<tr>
<td>action_to_date</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>category</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>changes_wait_id</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_created</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>due_date</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>impact</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>implementation_date</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k_bwait_id</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>next_step</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>priority</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table name</td>
<td>Table type</td>
<td>Field name</td>
<td>Field type</td>
<td>Key field type</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------</td>
<td>-----------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>resolution_date</td>
<td>datetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>resolutionorWorkaround</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>resolved</td>
<td>bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rfc</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rootCause</td>
<td>ntext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServiceDeskProblemManagement_id</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sla_id</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sla_id_type</td>
<td>varchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>task_id</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>title</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>urgency</td>
<td>nvarchar</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Add Advanced Document dialog box 357
adding an automation rule to a ruleset Incident Management 214
Process Type Actions to the Change Management Process View page 107
to the Incident Management Process View page 107
Admin menu. See Admin page
Admin page about 57
commands 523
advanced customizations ServiceDesk 430 Workflow Designer 430
advanced document 355
advanced incident about 151
all users default permissions 541
application properties about 528
application users default permissions 542
article in knowledge base 329
See also knowledge base item creating 328
defining content 329
viewing 339
Active Directory sync profile (continued)
settings 492
Active Directory sync profiles configuring 467
management 483
Active Directory synchronization about 466
all sync profiles 496
effect on user accounts 466
status check 497
update synchronization 496
AD. See Active Directory
Active Directory authentication about 450
Active Directory network share requesting 123
Active Directory password reset requesting 121
Active Directory self service catalog about 121
Active Directory server connection, testing 476
settings 477
testing connection 476
Active Directory server connection adding 470
deleting connection 475
editing settings 473
Active Directory server connections management 469
Active Directory sync profile full synchronization 495
about change request rulesets 231
about configuring Service Level Agreement (SLA) late date 436
actions about 104
automation rules Incident Management 211
Active Directory authentication method, selecting 475
groups added to ServiceDesk 451
master settings 531
sync profile, deleting 492
sync profile schedule, deleting 482
sync profile schedule, editing 481
sync profile schedules, adding 479
sync profile schedules, managing 478
sync profile, adding 486
sync profile, editing 489
synchronization methods 493
users added to ServiceDesk 451, 460
Active Directory authentication about 450
Active Directory network share requesting 123
Active Directory password reset requesting 121
Active Directory self service catalog about 121
Active Directory server connection, testing 476
settings 477
testing connection 476
Active Directory server connection adding 470
deleting connection 475
editing settings 473
Active Directory server connections management 469
Active Directory sync profile full synchronization 495
attach file 144
authentication for ServiceDesk. See ServiceDesk authentication
authentication method
   Active Directory, selecting 475
automation rules 528
   about
      Incident Management 202
B
blacklist user email 166
Bulletin Board
   about 309
bulletin board message 330
   See also knowledge base item
      creating 328
      defining content 330
      viewing 339
business hours 526
   configuration 438
C
CAB
   authorizing change request 255
Calendar page
   about 57
      viewing 300
canceling a vote
   on a change plan 255
capture screen 115
   from incident 145
   icons 117
cascading closure
   about 38
   from problem ticket 265
category 326
   See also knowledge base category
document. See document category
knowledge base. See knowledge base category
problem. See problem category
report. See report category
change approver
   default permissions 544
Change Management
   about 220
      creating email templates 234
      deleting email templates 239
      editing email templates 236
   (continued)
      process 221
      user roles 239
Change Management process
   Closed state 225
   Planned state 222
   Received state 223
   Reviewed state 224
change manager
   default permissions 545
change plan
   canceling a vote on 255
   initiating a vote on 253
   monitoring a vote on 254
change request
   approving 256
   authorizing 255
   CAB authorization 255
   creating 242
   creating from incident 176
   from problem 278
   fulfilling 257
   reassigning 289
   sources 241
Change request rulesets
   configuring 232
change request rulesets
   about 231
change request ticket
   closing 257
   sending email 375
change template
   about 243
   creating 244
   deleting 246
   editing 245
   using 247
changes
   viewing by resource 45
child reports 402
CI. See configuration item
classification
   Incident Management. See Incident Management classification
classification of incidents. See Incident Management classification
classification of problems
   changing 276
   defaults 559
classification of problems  (continued)
   selecting 275
classify email for incidents 165
clone
   user 460
close codes
   about 528
   adding 529
   defaults 529
   deleting 529
CMDB
   about 39
components
   Process Automation rules
      Incident Management 203
   components of ServiceDesk 35
conditions
   automation rules
      Incident Management 206
configuration
   ServiceDesk 422
configuration item
   about 39
Configuration Management Database. See CMDB
configurations
   additional
      ServiceDesk 428
configuring
   Data Mapping Routing Tables 440
   Help link 517
   Impact/Urgency Matrix 440
   new automation rules
      Incident Management 214
   Routing Tables 440
context-sensitive help 31
core processes
   ServiceDesk 24
Create Subtasks page 181
creating
   service queues 189
   subtask template
      from incident’s Process View page 183
creating email templates 195, 234
   See also Change Management
   See also Incident Management
Customer Satisfaction Survey
   about 508
   customizing 508
   submitting 149
customization
   portal page lists 88
   portal pages 82
   request list 88
   task list 88
   tickets list 88
customize report 406
customized
   form 505
   Process Manager portal page 80

D
data event rulesets
   about 203
data from Helpdesk Solution 6.x. See Helpdesk Solution 6.x
data hierarchy 499
   See also Incident Management classification
   about 499
   defaults 559
Data Mapping
   about configuring Routing Tables 440
   configuring
      Routing Tables 440
default portal page 80
delegation of tickets
   deleting 294
   managing 527
   performing 293, 295
deleting
   email templates 200, 239
   Process Type Actions
      from the Change Management Process View page 112
      from the Incident Management Process View page 112
   service queues 192
deleting email templates 200, 239
   See also Change Management
   See also Incident Management
discussion
   about 381
   adding 382
   adding thread 383
deleting 58
   filtering 58
   participating 384
   posting 384
   problem-related 269
discussion  (continued)
    rating 384
    rating levels 382
Discussions page 58

document
    actions 365
    adding 355
    adding to category 362
    advanced 355
    attaching to process ticket 287
    deleting 363
    displaying 368
    downloading 369
    downloading compressed 369
    editing data 360
    emailing 369
    history 371
    new version 360
    options 365
    permissions 359
    previewing 368
    promoting version 361
    searching for 367
    sending 369
    simple 355
    viewing 368
    viewing versions 370

document category 347
    See also document subcategory
        about 347
        adding 348
        defining 349
        deleting 351
        editing 350
        history 352
        permissions 351

Document Management
    about 346
    in processes 347

document subcategory
    about 347
    adding 348
    defining 349

documentation 31
    adding to Document Management 520
    from File Browser Web part 519
    from Help link 517
    from Links Web part 517
    making available 515

Documents page
    about 59

E

Edit AD connection settings
    dialog box 477

editing
    Process Type Actions 110
    service queues 191

editing email templates 197, 236
    See also Change Management
    See also Incident Management

email
    blacklisting sender 166
    creating incident.  See incidents from email
    customizing 511
    sending from a ticket's Process View page 375
    submitting incident 141

email classification 166

email monitoring 163
    See also incidents from email
    about 163
    configuring 513

email notification
    event-driven 378

email notifications
    automatic 377
    contents 512
    incidents 133
    knowledge base 311
    problem tickets 267
    process-driven 377

email templates
    creating 195, 234
    editing 197, 236

escalation
    about 201

Examination and Analysis page 275

expected document message 353

export portal page 73

F

FAQ 332
    See also knowledge base item
    creating 328
    defining content 332
    viewing 339

feedback for incident.  See incident feedback
file
  attaching to incident 144
  attaching to process ticket 287
filter report 406
fine tuning reports
  in the Process Manager portal 393
fix
  proposal 276
  reviewing 277
form
  customizing 505
  editing 507
  permissions 508
frequently asked question. See FAQ
FSC page 57
  See also Calendar page
  See also Schedule page
G
group
  about 449
  adding users 455
  creating 452
  customizing permissions 456
  default groups 539
  defining 453
  definition 449
  deleting 454
  editing 454
  from Active Directory 451
  permissions. See group permissions
group permissions
  about 449
  copying between groups 456
  customizing 456
  from Active Directory 451
  viewing 457
H
help
  context-sensitive 31
Helpdesk Solution 6.x
  about data migration 444
hierarchy
  see data hierarchy 499
holidays
  adding 438
Home page
  about 61
I
ID for process ticket. See process ID
impact of incident
  about 432
  defaults 433
implementation of change plan
  scheduling 249
import portal page 74
inbound email
  monitoring 163
incident
  actions 134
  adding to problem ticket 273
  advanced 151
  attaching files 144
  capturing screen image 115, 145
  closing 148
  closing multiple incidents 176
  confirming resolution 147
  creating 139
  creating change request 176
  creating for user
    advanced form 153
  creating from template 154
  creating problem ticket 174
  defining 142
  defining advanced 155
  email notifications 133
  feedback 148
  finding 147
  Process View page 134
  reassigning 289
  reopening 149
  reporting 139
  resolution 158
  resolving from advanced form 169
  resolving from tasks 170
Smart Tasks 137
  sources 133
  status 131
submitting 139
submitting by email 141
submitting for user
  advanced form 153
template. See incident template
incident categories
  default 559
incident classification
  adding 500
  deleting 501
incident classifications
  exporting 502
  importing 502
incident escalation. See escalation
incident feedback
  about 147
incident ID. See process ID
incident impact. See impact of incident
Incident Management
  about 127
  automation rules components 203
  creating email templates 195
  deleting email templates 200
  editing email templates 197
  process 128
  user roles 132
Incident Management classifications 499
  See also data hierarchy
  about 499
incident priority. See priority
Incident Response page 171
incident routing. See routing incidents
incident subtask. See subtask
incident template
  about 152
  creating 159
incident ticket
  sending email 375
incident tickets
  reassigning to a service queue 296
incident tickets reassignment to service queue
  performing 296
incident timeout
  about 147
incident urgency. See urgency of incident incidents
  viewing by resource 45
incidents from email
  about 163
  classifying 165
  evaluating 165
  priority 167
  submitting 141

initiating a vote
  on a change plan 253

K
KB approver 315
  default permissions 547
KB editor 315
  default permissions 549
key features
  ServiceDesk 26
knowledge base
  actions 340
  notifications 311
  options 340
  permissions 312
  searching 339
  types of items 309
knowledge base approver 315
  default permissions 547
knowledge base category 325
  See also knowledge base subcategory
  about 325
  adding 326
  adding subcategory 326
  permissions 312
knowledge base editor 315
  default permissions 549
knowledge base item
  actions 340
  changing category 327
  creating 328
  options 340
  sources 315
  viewing 339
knowledge base items
  ratings 307
Knowledge Base page
  about 62
knowledge base request
  accepting 318
  final review 320
  process 313
  rejecting 318
  sources 315
  status 310
  submitting 317
knowledge base subcategory
  about 325
Knowledge Management 307
See also knowledge base
about 307
process 313
Knowledge Management process. See user roles

L
lease tasks 283
breaking lease 284
levels for SLA
defaults 437
licensing for ServiceDesk 40
lists/profiles 524

M
manage delegations 527
manage pages 526
master settings
about 530
editing 530
migrating data
about
to ServiceDesk 430
from ServiceDesk 7.0 MR2 444
from ServiceDesk 7.1 SP1 443
from ServiceDesk 7.1 SP2 442
migration from Helpdesk Solution 6.x
about 444
MIME type
RDP 428
modules
ServiceDesk 24
monitoring a vote
on a change plan 254
monitoring email. See email monitoring
multiple tickets
performing actions on 286
My Task List page 63
See also task list
about 63

N
native authentication
about 450
New AD Connections Profile
dialog box 477
notification email (continued)
contents 512
event-driven 378
process-driven 377

O
optimizing reports
for viewing on the Reports page 393
on a Process Manager portal page 393
organization
creating 458
definition 449
organizational unit. See organization

P
password
changing 119
permissions
about 448
copying between groups 456
defaults by category 533
group. See group permissions
knowledge base 312
report 392
report category 400
setting 113
viewing 457
viewing for groups 457
pick 114
plugin upload 526
portal. See Process Manager portal
portal page
about 52
customizing contents 80
managing 526
portal page list
customization options 89
customizing 88
report, changing 91
post
about 382
adding to discussion 384
deleting 58
postponed incident
reopening 173
postponing an incident
scheduling for later 172
priority
  about 432
defaults 433
how it is calculated 434
incident email 167

problem
  reporting 270
status 265

problem analyst 266
default permissions 550

problem category
  customization 431
selecting 275

problem classification
  changing 276
selecting 275

problem classifications
  default 559

Problem Management
  about 262

Problem Management process
  about 263
user roles 266

problem reviewer 266
default permissions 552

problem ticket
  actions 269
  adding incidents 273
creating 270
creating from incident 174
defining 271
discussion 269
email notifications 267
entering analysis results 274
fix 276
Process View page 267
reassigning 289
reviewing fix 277
reviewing workaround 277
reworking 279
sources 266
workaround 276
working 274

problems
  viewing by resource 45

process
  Change Management 221
Incident Management 128
Problem Management 263

Process Actions
  about 106

Process Automation rules
  components
    Incident Management 203

process event rulesets
  about 203

process ID
  about 37

Process Manager
  portal page. See portal page

Process Manager Active Directory Settings 531

Process Manager authentication. See ServiceDesk authentication

Process Manager database
  reportable data 563

Process Manager portal
  about 52
logging on 53
pages. See portal page portal. See Process Manager portal

Process Manager portal page
  adding Web parts 85
customizing by administrator 82
customizing by user 82
default 54, 80
deleting 75
deleting Web parts 86
disabling 76
editing Web parts 86
enabling 76
enabling user customization 81
exporting 73
importing 74
opening page 80
rearranging the sequence 74
sharing 87
user’s home 80

process notification email
  about 378

process notifications
  bulletin board 331
FAQ 332
knowledge base article 329
wiki article 334

process ticket
  attaching file 287
delegating 293, 295
process tickets
  cascading closure 38
  relationships 38
process time
  about 285
  posting 285
Process Type Actions
  about 106
  adding to Process View pages 107
  editing 110
  removing from Process View pages 112
process type actions 525
Process View page
  Change Management's 101
  Incident Management's 94
  Problem Management's 98
Process View pages
  about 93
  incidents 134
  problem tickets 267
profile
  managing 524
profile reference type 525

Q
Quick Search page
  about 64

R
ratings for knowledge base items 307
reassign tickets 289
relationship type
  about 525
  creating 532
Release Notes 31
remote control through RDP 428
removing
  Process Type Actions
    from the Change Management Process View page 112
    from the Incident Management Process View page 112
reopening
  postponed incident 173
report
  about 390
  actions 391
  adding to category 401
report (continued)
  adding to portal page 397
  adding to schedule 415
  changing 411
  child 402
  copying 395
  creating email schedule 414
  creating standard 403
  customizing 406
  deleting 398
  emailing 413
  exporting definition 396
  filtering 406
  importing 397
  layout grid 406
  options 391
  permissions 392
  print view 392
  sorting 406
  viewing 390
  Web Service access 407
report category 398
  See also report subcategory about 398
  adding 398
  adding reports 401
  adding subcategory 399
  deleting 399
  importing 401
  permissions 400
report data 404
report subcategory
  about 398
  adding 399
reporting
  data dictionary 563
Reports page
  about 65
request for knowledge base. See knowledge base request
request list
  customizing 88
requesting
  a change 242
requesting a password reset 121
  See also Active Directory password reset
requesting access to network share 123
  See also Active Directory network share
resolve incident
  from advanced form 169
  from tasks 170
roles
  Change Management 239
  Incident Management 132
  Knowledge Management 314
  Problem Management 266
routing incidents
  about 201
routing rules 528
Routing Tables
  about configuring Data Mapping 440
ruleset
  automation rules
    Incident Management 204

S
schedule
  adding 302
  adding entry 303
  creating 302
  defining 302
  searching 301
  viewing 300
schedule entry
  adding 303
  defining 304
  searching 301
Schedule page
  page 57
scheduling
  about 299
  implementation of change plan 249
scheduling an incident
  postponing 172
screen capture
  from incident 145
  icons 117
screen capture utility
  capturing an image 115
search
  incident 147
  schedule entry 301
security 448
Service Catalog
  about 442
service item
  about 442
Service Level Agreement (SLA)
  creating 435
  default levels 437
  editing 435
Service Level Agreement (SLA) late date
  about configuring 436
service manager
  default permissions 554
service queues
  creating 189
  deleting 192
  editing 191
ServiceDesk
  about 23
  components 35
  configuration. See ServiceDesk configuration
  configuring 423
  core processes 24
  how it works 26
  key features 26
  licenses 40
  modules 24
  settings. See ServiceDesk settings
  solution. See ServiceDesk solution software
  what you can do with it 24
ServiceDesk authentication
  about 450
  mixed mode 450
ServiceDesk configuration
  about 422
  prerequisites 423
  what to configure 423
ServiceDesk portal
  master settings. See master settings
ServiceDesk portal page 54
  See also Process Manager portal page
ServiceDesk settings
ServiceDesk Solution
  console page 44
ServiceDesk solution software
  about 43
  accessing console page 44
share portal page 87
simple document 355
Site Actions 83
SLA. See Service Level Agreement (SLA)
SLA late date. See Service Level Agreement (SLA)
late date
Smart Tasks
  incident  137
smart tasks
  about  104
sort report  406
status
  incident  131
  knowledge base request  310
  problem  265
Submit Problem page  175
Submit Request page  66
  See also request list
  about  66
subtask
  about  179
  creating  180
  creating from template  181
  template. See subtask template
subtask template
  about  180
  creating from incident's Process View page  183
subtask templates
  creating  184
  deleting  186
  editing  185
Support II
  default permissions  555
sync profile
  Active Directory, adding  486
  Active Directory, deleting  492
  Active Directory, editing  489
sync profile schedule
  Active Directory, editing  481
sync profile schedules
  Active Directory, adding  479
  Active Directory, deleting  482
  Active Directory, managing  478
synchronization methods
  Active Directory  493
synchronization of Active Directory. See Active Directory synchronization

T
  tables
    in the Process Manager database  563
    key fields in  563
task
  breaking lease  284
  leasing  283
task (continued)
  restricting access  283
task list
  customizing  88
  Technician Dashboard page
    about  67
    options for changing  68
template
  incident. See incident template
  subtask. See subtask template
thread
  about  382
  adding  383
  deleting  58
ticket
  ID. See process ID
tickets
  performing actions on multiple  286
tickets list
  customizing  88
  Tickets page  69
  See also tickets list
  about  69
U
  upload plugin  526
urgency of incident
  about  432
  defaults  433
user
  adding  458
  adding to group  455
  cloning  460
  creating  458
  definition  448
  disabling  462
  editing  461
  enabling  462
  from Active Directory  451, 460
  picking  114
user accounts  527
user relationship type
  about  525
  creating  532
V
  voting
    on a change request  255
W
Web part
  adding to portal page 85
  deleting from portal page 86
  editing on portal page 86
wiki article 333
  See also knowledge base item
  adding entry 335
  adding links 335
  creating 328
  defining content 333
  link syntax 336
  viewing 339
workaround
  proposal 276
  reviewing 277
Workflow page
  about 71