TOC

Management Center Overview .................................................................................................................. 29

Web Console Overview .............................................................................................................................. 31
  Dashboard .................................................................................................................................................. 32
  Network ................................................................................................................................................... 32
  Configuration .......................................................................................................................................... 33
  Jobs ......................................................................................................................................................... 33
  Reports ................................................................................................................................................... 33
  Administration ......................................................................................................................................... 34
    Example ............................................................................................................................................... 34

Log into the Web Console ............................................................................................................................. 36

Navigate the Web Console ............................................................................................................................. 37

Required Ports, Protocols, and Services ........................................................................................................ 38
  Inbound Connections to Management Center .......................................................................................... 38
  Outbound Connections from Management Center .................................................................................. 38
  Required IP Addresses and URLs .............................................................................................................. 39

Verify Web Console Access ........................................................................................................................... 41

Move Items .................................................................................................................................................. 42

Encrypt Sensitive System Data ....................................................................................................................... 43
  Potential Data Loss .................................................................................................................................... 44

Management Center Solutions ....................................................................................................................... 45

Manage Devices ......................................................................................................................................... 47
  Add and Monitor Devices ............................................................................................................................ 48
  Add a Device ............................................................................................................................................. 50
  Add a Device Group .................................................................................................................................. 56
  Set the Device Polling Interval ..................................................................................................................... 57
  Monitor Device Health ................................................................................................................................. 58
    Metrics ................................................................................................................................................... 62
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve Device Errors</td>
<td>63</td>
</tr>
<tr>
<td>Add Multiple Devices at Once</td>
<td>64</td>
</tr>
<tr>
<td>Import Devices Using a CSV File</td>
<td>64</td>
</tr>
<tr>
<td>Determine Your Next Step</td>
<td>65</td>
</tr>
<tr>
<td>Edit a Device</td>
<td>66</td>
</tr>
<tr>
<td>Procedure</td>
<td>66</td>
</tr>
<tr>
<td>View Effective Policy for Each Slot on the Device</td>
<td>66</td>
</tr>
<tr>
<td>Determine Your Next Step</td>
<td>67</td>
</tr>
<tr>
<td>Edit a Device Group</td>
<td>68</td>
</tr>
<tr>
<td>Launch a Device Console</td>
<td>69</td>
</tr>
<tr>
<td>View Device License Information</td>
<td>69</td>
</tr>
<tr>
<td>Upgrade System Images on Managed Devices</td>
<td>69</td>
</tr>
<tr>
<td>Restrictions</td>
<td>70</td>
</tr>
<tr>
<td>Install System Image</td>
<td>70</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>73</td>
</tr>
<tr>
<td>Receive Error Notifications</td>
<td>73</td>
</tr>
<tr>
<td>Alert Notifications</td>
<td>73</td>
</tr>
<tr>
<td>Configure Alerts for Device Errors</td>
<td>74</td>
</tr>
<tr>
<td>About Alerting</td>
<td>74</td>
</tr>
<tr>
<td>Enable Alerting</td>
<td>74</td>
</tr>
<tr>
<td>View Alerts</td>
<td>75</td>
</tr>
<tr>
<td>Configure SNMP Alerts</td>
<td>75</td>
</tr>
<tr>
<td>Restrictions</td>
<td>75</td>
</tr>
<tr>
<td>Configure SMTP Alerts</td>
<td>76</td>
</tr>
<tr>
<td>Manage Alerts</td>
<td>77</td>
</tr>
<tr>
<td>Back Up Device Configurations</td>
<td>89</td>
</tr>
<tr>
<td>Next Steps</td>
<td>91</td>
</tr>
<tr>
<td>Regularly Back Up a Group of Devices</td>
<td>91</td>
</tr>
<tr>
<td>Use Device Information for Backup Job Image Metadata</td>
<td>93</td>
</tr>
</tbody>
</table>
Configure WAF Application Objects ................................................................. 145

WAF Policy Use ............................................................................................... 145

Analyze and Refine WAF Policy (Mitigate False Positives) ................................ 150

WAF Policy Use ............................................................................................... 151

Analyze and Refine WAF Policy Workflow ...................................................... 151

Manage WAF Security Policy ............................................................................ 152

WAF Policy Use ............................................................................................... 152

**Distribute Configurations to Devices** ................................................................ 156

Create and Distribute Configurations Using Scripts .......................................... 157

*Compare Versions of the Script* .................................................................... 160

*Customize Object Filters* ............................................................................. 161

*Execute Scripts* ............................................................................................. 162

*Filter by Attributes and Keyword Search* ...................................................... 167

Search by Keyword .......................................................................................... 167

Procedure ......................................................................................................... 168

Can quotes be used in a search? ...................................................................... 168

How do you search for whole words? ............................................................... 168

How do you search for partial words? ............................................................... 168

Example Searches .......................................................................................... 168

IPv4 127.0.0.1 ................................................................................................. 168

IPv6 "0:0:0:0:0:1" .......................................................................................... 168

Hostnames ........................................................................................................ 168

What if the search finds no match? .................................................................. 168

What if the search succeeds in finding matches? ............................................ 168

How do you clear the search results? ............................................................. 168

*Import Script from a Device* ......................................................................... 169

Determine Your Next Step ............................................................................... 170

*Manage Attributes* ....................................................................................... 171

View and Sort the Following Attributes Lists ................................................... 171

*Restore a Version of Script* ........................................................................... 172
View Script Information ........................................................................................................173

Apply Logical Expressions to Scripts and Policy .................................................................174
  Supported Expressions ........................................................................................................174
  Examples ..............................................................................................................................175
  Define simple if else logic flow .........................................................................................175
  Define advanced if else logic flow with foreach .............................................................175

Use Substitution Variables in Policies and Scripts ............................................................176
  Use in Shared Policy ..........................................................................................................176
    Syntax ..............................................................................................................................176
    Examples ........................................................................................................................177
  Supported Variables ..........................................................................................................177
  Specify a Default Substitution Value ..............................................................................179
    Syntax ..............................................................................................................................179
    Example ........................................................................................................................179
  Use Regular Expressions ...............................................................................................179
    Syntax ..............................................................................................................................179
    Example ........................................................................................................................179

Organize Scripts by Attribute ..........................................................................................180

Create and Distribute Policy ..............................................................................................183

Use Content Policy Language (CPL) to Create Policy ......................................................187
  Working with CPL Policy Fragments ...............................................................................188
  Determine Your Next Step ...............................................................................................188

Create a CPL Policy Object ...............................................................................................189
  Determine Your Next Step ...............................................................................................189

Add or Edit CPL Policy Sections ......................................................................................191

Refine Existing CPL Policy ..............................................................................................193

Manage CPL Policies ..........................................................................................................195

Work with CPL Policy Sections ........................................................................................196

Layout Modes ....................................................................................................................196

Single Pane Layout ..........................................................................................................196
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modular Layout</td>
<td>196</td>
</tr>
<tr>
<td>Navigate sections</td>
<td>197</td>
</tr>
<tr>
<td>Collapse a section</td>
<td>197</td>
</tr>
<tr>
<td>Collapse all sections</td>
<td>198</td>
</tr>
<tr>
<td>Move sections</td>
<td>198</td>
</tr>
<tr>
<td>Find a Policy Section</td>
<td>199</td>
</tr>
<tr>
<td>If the search finds no match</td>
<td>199</td>
</tr>
<tr>
<td>If the search finds matches</td>
<td>199</td>
</tr>
<tr>
<td>Clear the search results</td>
<td>199</td>
</tr>
<tr>
<td>Manage Attributes</td>
<td>200</td>
</tr>
<tr>
<td>View and Sort the Following Attributes Lists</td>
<td>200</td>
</tr>
<tr>
<td>Change the Order in which Policy Rules are Evaluated</td>
<td>201</td>
</tr>
<tr>
<td>Use Substitution Variables in Policies and Scripts</td>
<td>202</td>
</tr>
<tr>
<td>Use in Shared Policy</td>
<td>202</td>
</tr>
<tr>
<td>Syntax</td>
<td>203</td>
</tr>
<tr>
<td>Examples</td>
<td>203</td>
</tr>
<tr>
<td>Supported Variables</td>
<td>203</td>
</tr>
<tr>
<td>Specify a Default Substitution Value</td>
<td>205</td>
</tr>
<tr>
<td>Syntax</td>
<td>205</td>
</tr>
<tr>
<td>Example</td>
<td>205</td>
</tr>
<tr>
<td>Use Regular Expressions</td>
<td>205</td>
</tr>
<tr>
<td>Syntax</td>
<td>205</td>
</tr>
<tr>
<td>Example</td>
<td>205</td>
</tr>
<tr>
<td>Launch Visual Policy Manager</td>
<td>207</td>
</tr>
<tr>
<td>VPM Requirements</td>
<td>207</td>
</tr>
<tr>
<td>Launch the VPM</td>
<td>207</td>
</tr>
<tr>
<td>Set Up and Enable Java in Your Browser</td>
<td>209</td>
</tr>
<tr>
<td>Launch Visual Policy Manager</td>
<td>210</td>
</tr>
<tr>
<td>VPM Requirements</td>
<td>210</td>
</tr>
<tr>
<td>Launch the VPM</td>
<td>210</td>
</tr>
</tbody>
</table>
Select Reference Device for VPM Policy ................................................................. 212
Determine Your Next Step ...................................................................................... 213
View VPM Policy Source ....................................................................................... 213
Restrict Access Only to a Specific Object Included in a VPM Layer ......................... 214

Create Shared Objects .......................................................................................... 221
  Create a CPL Policy Fragment .............................................................................. 223
  Create URL List (URL Policy Exceptions) ........................................................... 224
  Enabling and Disabling URLs ............................................................................. 226
  URL List Example ............................................................................................... 227
  Step One - Create the URL List Object .............................................................. 227
  Step Two - Add Allowed URLs .......................................................................... 228
  Step Three - Add the URL List to the ASUP Policy ............................................ 228

Manage URL and Category List Triggers ............................................................... 230
  URL List Triggers .............................................................................................. 230
  Category List Triggers ....................................................................................... 230

Include a Shared Policy Object in CPL or VPM Policy ........................................... 232

Work with Categories ............................................................................................ 237
  Create Category Lists ........................................................................................ 237
  Category List Example ....................................................................................... 240
  Step One - Create the Category List Object ....................................................... 241
  Step Two - Select Categories that Should be Denied ......................................... 241
  Step Three - Add the Category List to the ASUP Policy .................................... 243
  Use Category List Templates ............................................................................. 247
  Create Custom Categories ................................................................................. 250

Enabling and Disabling URLs .............................................................................. 253
  Custom Category Example ................................................................................. 253
  Step One - Create the Category Object .............................................................. 254
  Step Two - Add URLs ........................................................................................ 254
  Step Three - Add the Category to the ASUP Policy .......................................... 255

Create a Local Content Filter Database ................................................................ 255
Supported Local Category Syntax ............................................................................................................ 257
Local Category Limitations ...................................................................................................................... 257
Define and Manage Local Categories ...................................................................................................... 257
Optional Step - Import Categories .......................................................................................................... 257
Edit a Category ........................................................................................................................................ 258
View Database Versions .......................................................................................................................... 258
Compare Database Versions .................................................................................................................... 258
Record the Local Database Direct URL ................................................................................................... 259
Local Database URL Protocol Note .......................................................................................................... 259
Manual Deployment - SSL Visibility ......................................................................................................... 260
Manual Deployment - ProxySG and Advanced Secure Gateway ............................................................... 261
(Optional) Scripted Configuration - ProxySG and Advanced Secure Gateway ....................................... 261
Create SSL Visibility List Policy ............................................................................................................ 261
Create SSL Visibility URL List Policy ..................................................................................................... 269
Create SSL Visibility IP Address List ...................................................................................................... 277
Enabling and Disabling IP Addresses ..................................................................................................... 279

Deploy Tenant Policy ............................................................................................................................. 280
Manage Tenants ....................................................................................................................................... 282
WAF Policy Use ....................................................................................................................................... 282
Create a VPM Tenant Policy Object ......................................................................................................... 286
Determine Your Next Step ......................................................................................................................... 286
Import VPM Tenant Policy from Source Device ....................................................................................... 287
Determine Your Next Step ......................................................................................................................... 289
Deploy Tenant Policy ................................................................................................................................ 290

Apply a Single Policy to Both On-Premises and Cloud Users .................................................................. 291
Prerequisites ............................................................................................................................................. 291
SSL Requirements .................................................................................................................................... 292
Solution Steps .......................................................................................................................................... 292
Add a Universal VPM Policy Object ........................................................................................................ 292
Transform Existing VPM Policy into Universal VPM Policy .................................................................... 293
Refine and Validate Universal VPM Policy ................................................................. 294
VPM Requirements ................................................................................................. 294
Procedure ................................................................................................................. 295
Deploy Universal CPL Policy .................................................................................. 297
   Analyze the CPL Universal Policy ......................................................................... 297
   Select Reference Device for Universal CPL Policy .................................................. 299
Determine Your Next Step ....................................................................................... 300
Install or Import Policy ............................................................................................ 300
   Preview Policy Before Installing It ........................................................................ 300
   Install Policy ......................................................................................................... 302
      Policy Installation Methods ............................................................................... 302
   Install: .................................................................................................................... 302
   Install to All... ....................................................................................................... 306
   Install to Target ..................................................................................................... 306
   Install Multiple Policies ....................................................................................... 307
Import Policy or Shared Objects ............................................................................. 308
   Universal VPM Policy Considerations ................................................................. 313
      Import from Device ............................................................................................. 313
   Determine Your Next Step .................................................................................... 314
Import External Policy ............................................................................................ 315
Prerequisites ............................................................................................................ 315
Procedure ................................................................................................................. 315
View Policy .............................................................................................................. 316
   View Policy Versions ............................................................................................ 316
   View Existing Policy Information ......................................................................... 319
   View Deployed Policy for each Device Slot ......................................................... 323
   View Devices Associated with Policy ..................................................................... 324
Configure Policy ....................................................................................................... 325
Add or Remove Devices Associated with Policy ...................................................... 326
   Add Targets .......................................................................................................... 326
Remove Targets ................................................................. 328
Determine Your Next Step .................................................... 328
Check Consistency between Policy and Devices ....................... 329
Determine Your Next Step .................................................... 330
Compare Different Versions of the Same Policy ......................... 331
Compare the Device Policy Version with Current Policy Version .... 332
Determine Your Next Step .................................................... 333
Export Policy or Shared Objects to Local Disk ......................... 333
Restore a Version of Policy .................................................. 335
Use Specific Attribute Values to Control Access to Policy .......... 335
Procedure ........................................................................... 335

Create Shared Objects ............................................................. 336

Permissions Reference ......................................................... 338
Reference: Permissions Interdependencies ............................... 339
Reference: Permissions Filters Object and Attributes .................. 348
Reference: Understanding Job Permissions ............................... 352

User runs a job immediately after configuring it or manually using Run Now .............................................. 352
User configures a job scheduled in the future ............................ 352

Configure Users, Roles, and Attributes .................................. 353
Manage Management Center Users ........................................ 354

Add Users and Grant Permissions ......................................... 354
Add Local Users ................................................................... 357
Add Users from an Existing Directory or Service ...................... 359

Authenticate Users Against LDAP ......................................... 360
Authenticate Users Against Active Directory LDAP ................. 363
Authenticate Users Against RADIUS ...................................... 365

Authenticate Users with SSL Mutual Authentication ............... 366

Note .................................................................................... 369

Use Certificate Subject Alternative Name Data for Certificate Validation ....................................................... 370
Management Center Configuration & Management

View, Edit, or Delete User Accounts .................................................................372
  View User Information ..........................................................372
  View User Permissions .........................................................372
  Edit User ...........................................................................372
  Delete a User ...................................................................373
Change and Reset Passwords .................................................................374
  Change Your Password ......................................................375
  Reset Password .................................................................376
  Automate Password Reset Process ....................................376
  Manually Reset a User’s Web Console Password .............378
  Expire a User’s Web Console Password ..........................378
  Reset or Restore Admin Account Passwords ..................380
Manage User Groups .......................................................................381
  Add User Groups .................................................................381
  Edit a User Group .................................................................383
  View Group Permissions and Roles .................................383
  View Group Members ............................................................383
  Delete a User Group ...............................................................384
Manage User Sessions ..................................................................385
Define Roles ..................................................................................386
  About Roles ......................................................................386
  Procedure ..........................................................................386
Duplicate an Existing Role .............................................................388
Edit an Existing Role ..................................................................388
Grant Permissions .........................................................................390
Update Access When a User’s Job Changes ..............................392
  Update a User’s Roles ..........................................................392
Filter Devices or Device Groups in a Permission .........................393
Reference: Permissions Filters Object and Attributes ..............393
Restrict Access to Reporter Reports ..............................................396
Configure SMTP Alerts .............................................................................................................. 424
Configure SNMP Alerts .............................................................................................................. 425
Restrictions ................................................................................................................................. 425
Customize the Audit Log ............................................................................................................ 427

Create and Manage Jobs ............................................................................................................. 429
Add a Job ...................................................................................................................................... 430
Job Operations .............................................................................................................................. 432
Job Scheduling Options .................................................................................................................. 436
Monitor Jobs .................................................................................................................................. 438
Edit a Job ....................................................................................................................................... 439
View Current Jobs .......................................................................................................................... 440
Cancel a Currently Running Job ...................................................................................................... 441
View and Manage Job History ......................................................................................................... 442
View and Filter Job Progress ........................................................................................................... 442

Management Center Reports ....................................................................................................... 444
Statistics Monitoring Reports ........................................................................................................ 444
Reporter Reports ............................................................................................................................ 444
View Consolidated Reports ............................................................................................................. 444
Integrate Reporter into Management Center .................................................................................. 446
Add a Device .................................................................................................................................. 447
View a Reporter Report .................................................................................................................... 453
Customize Reporter Report Options ............................................................................................... 459
Add Report Filters .......................................................................................................................... 459
Filter Examples .................................................................................................................................. 461
Change the Report Grouping ........................................................................................................... 461
Change the number of items displayed per page .............................................................................. 462
Change the grouping of the report (that is, change the focus of the report) ..................................... 462
Create a two-level report .................................................................................................................. 463
Reference: Report Descriptions ................................................................. 465
Create Custom Report Groups .............................................................. 474
Create a Custom Report ................................................................. 476
Edit Custom Reports ......................................................................... 483
Additional Information ....................................................................... 485
Search for Specific Report Data (Search and Forensic Report) ................. 485
Reporter Graph Types and Views ....................................................... 489
Set Time Zone for Reporter Reports .................................................. 490
Determine Why A Reporter Database Does Not Display ......................... 491
View Statistics Monitoring Reports .................................................... 492
Reference: Statistics Monitoring Reports in Management Center ............... 493
Modify Options for Statistics Monitoring Reports ................................... 496
Change the Scope of a Statistics Monitoring Report .............................. 498
Filter on Devices or Device Groups .................................................... 499
Zoom In and Out on Reports ............................................................ 499
Statistics Monitoring Graph Types ..................................................... 499
Display a Full Report ......................................................................... 500
Determine Your Next Step .................................................................. 500
View Statistics Monitoring Reports .................................................... 501
Reference: Statistics Monitoring Reports in Management Center ............... 502
Modify Options for Statistics Monitoring Reports ................................... 505
Change the Scope of a Statistics Monitoring Report .............................. 507
Filter on Devices or Device Groups .................................................... 508
Zoom In and Out on Reports ............................................................ 508
Display a Full Report ......................................................................... 508
Determine Your Next Step .................................................................. 509
Statistics Monitoring Graph Types ..................................................... 509
Work with Reports ........................................................................... 510
Customize Report Widgets ............................................................... 511
Collapse Report Widgets .................................................................. 511
Move Report Widgets ................................................................. 511
Remove Report Widgets ............................................................ 511
Add Reports .............................................................................. 511
Close a Report ........................................................................... 511
Close the Active Report ............................................................ 511
Close a Report on Another Widget ............................................. 511
Modify Display of Table Data ..................................................... 511
View Raw Report Data ............................................................... 514
Reports: Save as PDF ................................................................. 514

Manage Dashboards ................................................................... 515

Notes ......................................................................................... 515

Dashboards and Widgets ........................................................... 517
    Add a Widget to the Current Dashboard .................................... 517
Add the Bookmarked Devices Widget ........................................... 518
Edit or Duplicate Dashboards ..................................................... 519
    Home ................................................................................. 519
    Statistics Monitoring Dashboard ............................................. 519
Change the Dashboard Layout or Refresh Rate ............................. 519

Administrate Management Center .............................................. 521

Configure General System Settings ......................................... 521
    Set Bandwidth Cost for Reports ............................................ 523
    Set the Device Polling Interval ............................................. 523
    Set the Number of Backup Slots .......................................... 523
    View Audit Log ..................................................................... 524
    Specify Explicit Proxy Settings ............................................ 525
    Configure Diagnostics Logging ............................................ 526
    Configure Housekeeping Settings ....................................... 527
    Configure Mail Settings ........................................................ 528
    Configure the SNMP Agent Password ................................... 529
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Consent Banner</strong></td>
<td>529</td>
</tr>
<tr>
<td>Procedure</td>
<td>530</td>
</tr>
<tr>
<td>Editor Example</td>
<td>531</td>
</tr>
<tr>
<td><strong>Configure Hardware Monitor Settings</strong></td>
<td>532</td>
</tr>
<tr>
<td>Upload Files to Management Center</td>
<td>532</td>
</tr>
<tr>
<td>Migrate Device Metadata from Director as Management Center Scripts</td>
<td>536</td>
</tr>
<tr>
<td>Determine Your Next Step</td>
<td>543</td>
</tr>
<tr>
<td><strong>Upgrade/Downgrade System Images</strong></td>
<td>544</td>
</tr>
<tr>
<td>Restrictions</td>
<td>544</td>
</tr>
<tr>
<td><strong>Back Up the Management Center Configuration</strong></td>
<td>546</td>
</tr>
<tr>
<td>Backup Requirements</td>
<td>547</td>
</tr>
<tr>
<td>Back Up Management Center</td>
<td>547</td>
</tr>
<tr>
<td>Back Up Management Center Using the CLI</td>
<td>547</td>
</tr>
<tr>
<td><strong>Encrypt Sensitive System Data</strong></td>
<td>548</td>
</tr>
<tr>
<td>Potential Data Loss</td>
<td>548</td>
</tr>
<tr>
<td><strong>Restore a Management Center Backup Configuration</strong></td>
<td>549</td>
</tr>
<tr>
<td>Restore Management Center Backup</td>
<td>549</td>
</tr>
<tr>
<td><strong>Configure Management Center Failover</strong></td>
<td>550</td>
</tr>
<tr>
<td>Replicated Data</td>
<td>550</td>
</tr>
<tr>
<td>Configuration Limitations</td>
<td>551</td>
</tr>
<tr>
<td>Device Limitations</td>
<td>551</td>
</tr>
<tr>
<td>Failover Prerequisites</td>
<td>551</td>
</tr>
<tr>
<td>Configure Failover</td>
<td>551</td>
</tr>
<tr>
<td>Switch to Secondary When the Primary is Unresponsive</td>
<td>554</td>
</tr>
<tr>
<td>Disable Failover</td>
<td>555</td>
</tr>
<tr>
<td><strong>Update the Management Center License</strong></td>
<td>556</td>
</tr>
<tr>
<td><strong>Verify License Components from the Web Console</strong></td>
<td>557</td>
</tr>
<tr>
<td><strong>Troubleshoot and Resolve Issues</strong></td>
<td>558</td>
</tr>
<tr>
<td>Audit Transactions</td>
<td>559</td>
</tr>
</tbody>
</table>
Understand Transaction Types .............................................................................................. 561
Customize the Audit Log ........................................................................................................ 562
Configure Housekeeping Settings .......................................................................................... 564
Configure Diagnostics Logging ............................................................................................. 564
Required Ports, Protocols, and Services .................................................................................. 567
  Inbound Connections to Management Center ........................................................................ 567
  Outbound Connections from Management Center ............................................................... 567
  Required IP Addresses and URLs ........................................................................................ 568
Determine Which Version You are Using ................................................................................. 569
  Build Information Fields ..................................................................................................... 570
Automate Password Reset Process ........................................................................................ 570
Prevent Licensing Issues on a Virtual Appliance ..................................................................... 572
  Duplicate Serial Numbers .................................................................................................. 572
  Expiring Licenses .............................................................................................................. 572
Stop or Restart Services .......................................................................................................... 572
  Stop Management Center Services .................................................................................... 572
  Restart Services .................................................................................................................. 573
Test Network Connectivity ..................................................................................................... 573
Upload System Diagnostics ..................................................................................................... 574
View Hardware Diagnostics and Memory Resources .............................................................. 574
Problems and Errors ............................................................................................................. 576
  Read Messages and Alerts ................................................................................................... 577
  "Could not enable statistics collection due to unexpected server failure" when activating a device .......................................................................................................................... 577
  "Import batch contains duplicate device name violation" when importing multiple devices ................................................................................................................................. 578
  "Local Changes Detected" error when installing policy ...................................................... 578
  User has "access denied" error when running a job .............................................................. 578
  "Multi-tenant policy support is not enabled for this device" when installing policy .......... 578
Review Open Source Attributions ............................................................................................ 579
Tips and Use Cases .................................................................................................................. 581
Organize Scripts by Attribute ................................................................. 581
Restrict Access Only to a Specific Object Included in a VPM Layer ............... 584
Management Center REST API ............................................................. 592
  Limitations ................................................................................. 592
  Documentation ....................................................................... 592
  Troubleshooting ................................................................... 592
CLI Command Reference .................................................................. 593
  Access the Management Center CLI ........................................... 594
  CLI URL Syntax ...................................................................... 595
  Notes ..................................................................................... 595
  Standard Mode Commands .......................................................... 596
    > enable ........................................................................... 596
      Syntax ............................................................................ 596
      Example ......................................................................... 596
    > exit ............................................................................... 596
      Syntax ............................................................................ 596
      Example ......................................................................... 596
    > help ............................................................................. 597
      Syntax ............................................................................ 597
      Example ......................................................................... 597
    > ping ............................................................................... 597
      Syntax ............................................................................ 597
      Example ......................................................................... 598
    > show ............................................................................. 598
      Syntax ............................................................................ 598
      Subcommands ................................................................... 598
        Example ....................................................................... 598
        Example ....................................................................... 599
        Example: ...................................................................... 599
Example .......................................................................................................................... 600
Example .......................................................................................................................... 600
> tracepath ...................................................................................................................... 600
Syntax .............................................................................................................................. 600
Example .......................................................................................................................... 600

Privileged Mode Commands .............................................................................................. 602

# appliance-name ........................................................................................................... 603
Syntax .............................................................................................................................. 603
Subcommands .................................................................................................................. 603
Notes .................................................................................................................................. 603
Example of changing the appliance name to MC_One: ..................................................... 604

# backup .......................................................................................................................... 604
Syntax .............................................................................................................................. 604
Subcommands .................................................................................................................. 604
Transfer Configuration and Data to Another Appliance .................................................... 605
Example .......................................................................................................................... 605

# clock ............................................................................................................................... 606
Syntax .............................................................................................................................. 606
Subcommands .................................................................................................................. 606
Examples ......................................................................................................................... 606

# diagnostic-systems ........................................................................................................ 607
Syntax .............................................................................................................................. 607
Subcommands .................................................................................................................. 607

# disable ........................................................................................................................... 607
Syntax .............................................................................................................................. 607
Example .......................................................................................................................... 608

# exit .................................................................................................................................. 608
Syntax .............................................................................................................................. 608
Example .......................................................................................................................... 608

# failover .......................................................................................................................... 608
# restore-defaults ................................................................. 616
  Syntax .................................................................................. 616
  Subcommands ........................................................................ 616
  Example ................................................................................. 616
# rsyslog-output ................................................................. 616
  Syntax .................................................................................. 617
  Subcommands ........................................................................ 617
  Examples ................................................................................ 617
# security ........................................................................... 617
  Syntax .................................................................................. 618
  Subcommands ........................................................................ 618
  Example ................................................................................. 622
# service ............................................................................. 622
  Perform Disk Maintenance ................................................... 623
  Syntax .................................................................................. 623
  Enable Verbose Logging ....................................................... 623
  Syntax .................................................................................. 623
  View Disk Usage ................................................................. 623
  Syntax .................................................................................. 623
  Purge VPM Cache ............................................................... 623
  Syntax .................................................................................. 623
  Rebuild Repository Index .................................................... 624
  Syntax .................................................................................. 624
  Start or Stop Service .......................................................... 624
  Upload Diagnostics Data ...................................................... 624
  Syntax .................................................................................. 624
  Subcommands ........................................................................ 624
# show ............................................................................... 625
  Syntax .................................................................................. 625
  Subcommands ........................................................................ 625
Example .......................................................................................................................... 625
Example .......................................................................................................................... 626
Example .......................................................................................................................... 626
Example .......................................................................................................................... 627
Example .......................................................................................................................... 627
# shutdown ..................................................................................................................... 627
  Syntax ............................................................................................................................ 627
  Example .......................................................................................................................... 627
# snmp ............................................................................................................................ 627
  Syntax ............................................................................................................................ 628
  Subcommands ................................................................................................................ 628
  Example .......................................................................................................................... 628
# static-route .................................................................................................................. 628
  Syntax ............................................................................................................................ 628
  Subcommands ................................................................................................................ 628
  Example of adding a static network route entry to nic0_0: ............................................. 629
# statistics-monitoring .................................................................................................... 629
  Syntax ............................................................................................................................ 629
  Subcommands ................................................................................................................ 629
  Example .......................................................................................................................... 629
# subscriptions ............................................................................................................... 629
  Syntax ............................................................................................................................ 630
  Subcommands ................................................................................................................ 630
  Example .......................................................................................................................... 630
# tracepath ....................................................................................................................... 630
  Syntax ............................................................................................................................ 630
  Example .......................................................................................................................... 631
# verify-hardware ............................................................................................................. 631
  Syntax ............................................................................................................................ 631
  Example .......................................................................................................................... 631
Management Center Configuration & Management

# timezone ........................................................................................................... 632

Syntax ......................................................................................................................... 632

Subcommands ............................................................................................................... 632

Examples ....................................................................................................................... 633
Copyright © 2017 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Blue Coat, and the Blue Coat logo are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

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. SYMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

www.symantec.com

8/24/2018
Management Center Overview

Management Center centrally manages and monitors the Symantec devices in your organization. You can organize devices into hierarchical groups, monitor device health, install policies to ProxySG devices, back up device configurations, and produce consolidated reports. In addition, you can control access to Management Center and devices by adding system users manually or authenticating through an existing directory or service, such as RADIUS.

The following table summarizes some of the features and benefits of using Management Center.

You can also view a list of Management Center solutions.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Center provides centralized management for up to 500 devices.</td>
<td>Eliminate the need to manage each remote device manually, reducing management costs.</td>
</tr>
<tr>
<td>Groups devices based on location, department, purpose, and other attributes that you specify.</td>
<td>Delegate administrative duties and deploy policies for specific groups. Enables administrators to assign attributes for managed devices that have different network.</td>
</tr>
<tr>
<td>Roles have greater flexibility, enabling user groups with the same permissions to access and manage policies and devices within their specific organization.</td>
<td>User Groups with the same permissions access, manage, and can report on devices within their management area without overlapping job duties and wasting time and resources. Apply roles to user groups that you need to have homogenous results (for example user groups that are in specific locations or have a specific job function).</td>
</tr>
<tr>
<td>Manages internal and external user accounts for Management Center.</td>
<td>Users only access the functional areas and perform tasks required for their jobs.</td>
</tr>
<tr>
<td>Facilitates creating and deploying policy to multiple devices simultaneously. Includes Visual Policy Manager and consistency checking between policies and devices</td>
<td>Ensure consistency amongst devices that have the same purpose or require standardized policy. Administrators can manage policy using the Visual Policy Manager on managed devices from within the Management Center web console.</td>
</tr>
<tr>
<td>Manage attributes for devices, device groups, policy and device scripts</td>
<td>Use attributes to define custom metadata for devices, device groups, policy and device scripts. Filter on attributes to refine searches for all objects.</td>
</tr>
<tr>
<td>Create, edit and execute scripts. Includes the ability to compare script versions and to import a script from a managed device</td>
<td>Administrators can create and edit scripts as well as execute scripts on managed devices. Variable replacement is supported, as well as the ability to check versions of a saved script and to import a script from a device.</td>
</tr>
<tr>
<td>Audit log records user and system event history</td>
<td>Be aware of all user actions in the system and support organizational accountability.</td>
</tr>
<tr>
<td>Feature</td>
<td>Benefit</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Reporting (Reports on device</td>
<td>Management Center provides centralized reporting for managed devices. Statistics Monitoring reports are included by default and include:</td>
</tr>
<tr>
<td>performance)</td>
<td>- Devices</td>
</tr>
<tr>
<td></td>
<td>- WAN Optimization Reports</td>
</tr>
<tr>
<td>Advanced Reporting (Reporter 10.x integration)</td>
<td>For advanced reporting features, you can add a Reporter Enterprise Server as a managed device. After adding Reporter, four groups of reports are available for viewing data:</td>
</tr>
<tr>
<td></td>
<td>- Security reports</td>
</tr>
<tr>
<td></td>
<td>- Web Application reports</td>
</tr>
<tr>
<td></td>
<td>- User Behavior reports</td>
</tr>
<tr>
<td></td>
<td>- Bandwidth Usage reports</td>
</tr>
<tr>
<td></td>
<td>Advanced Reporting provides visibility and a control point between employees of your organization and the cloud services and SaaS applications that users access (e.g., Box, Dropbox, Google Drive, Office 365, Salesforce, Facebook, etc.). Using full Reporter integration enables the discovery of all of the web applications in use, enabling you maximum visibility into all risky users, web sites and potential threats. See how trends of risky users and sites affect your company over time.</td>
</tr>
<tr>
<td>Storing device backups on an external server</td>
<td>Enables administrators to export backups to external servers using any of the following 4 protocols: FTP, HTTP, HTTPS, or SCP</td>
</tr>
<tr>
<td>Job scheduling to automate repetitive tasks</td>
<td>Administrators can set up jobs to automate tasks that recur or are otherwise inefficient to perform manually. Additional permissions are required to perform some jobs.</td>
</tr>
<tr>
<td>Hardware appliance support</td>
<td>Hardware diagnostics information is available in the web console, such as System Metrics, Storage Usage, Temperature, Voltage, RPM and other sensors. From the CLI you can run hardware diagnostics, power off the appliance and restore the appliance to factory defaults.</td>
</tr>
</tbody>
</table>
Web Console Overview

The web console is the user interface for Management Center.

Depending on a user’s permissions, not all of the tabs may be visible to a particular user. See "Reference: Permissions Interdependencies" on page 339 for more information.

Banner

The banner is the area at the top of the Management Center web console; look for the title Management Center. The banner is visible regardless of which tab or menu item you select. It provides you with a view of device health status and alert messages, access to your profile, global settings, and more. The following are options in the banner, from left to right (excluding the title):

- **Task Menu** contains device management operations.
- **Device Status Totals** indicate the number of devices and colors indicate device health. See the table below for web console color details.
Management Center Configuration & Management

- **Messages** display when you or other users complete certain tasks in Management Center. See "Read Messages and Alerts" on page 577.

- **System Menu** contains the following options:
  - **Profile** displays your user profile in Management Center. See Update Your Web Console Profile, Password and Security Question.
  - **Log out** of the system.
  - **Support** links to https://support.symantec.com.
  - **Documentation** links to the Management Center documentation on Symantec Product Documentation.
  - **About** displays the Management Center version and links to legal notices, including the EULA.

**Tabs**

Management Center divides functionality into tabs.

**Dashboard**

When you log in to Management Center, the web console displays the Home dashboard by default. From here, you can "Manage Dashboards" on page 515 and customize the data that you want to monitor for managed devices. See "Change the Dashboard Layout or Refresh Rate" on page 519,"Dashboards and Widgets" on page 517, and "Add the Bookmarked Devices Widget" on page 518.

**Network**

Network displays all managed devices in your hierarchy. For each device, you can view device overview information (such as platform, OS and serial number), device health, system metrics, and the backups for each device.
Configuration

ProxySG configurations can be updated using Policy or Scripts. To create and manage policy or create and execute scripts, see "Distribute Configurations to Devices" on page 156.

Jobs

The Jobs tab enables you to create and run jobs, view the progress of any currently running job, and provides a way to schedule recurring jobs. You can also see the entire job history for each device. "Create and Manage Jobs" on page 429.

Reports

Management Center provides centralized reporting for managed devices. Statistics Monitoring includes reports on the following categories:

- Devices
- WAN Optimization (requires a Proxy or MACH5 Edition license)

For advanced reporting features, you can add a Reporter Enterprise Server as a managed device. After adding Reporter, four groups of reports are available for viewing data about ProxySG devices:

- Security reports
- Web Application reports
Management Center Configuration & Management

- User Behavior reports
- Bandwidth Usage reports
- Log Detail

Administration

These settings enable you to add users, assign roles, and perform other administrative tasks. The tabs include Auditing, Settings, Users, Groups, Roles, Attributes, Hardware Diagnostics, Logs, User Session, and License.

About Color-Coded Status Indicators

Colors represent the status of significant events in several areas in the web console:

- **Alert colors**
  In alerts that pop up in the web console and are listed in the Messages list, colors indicate the severity level of the event. If you have unread alerts, the Messages label in the banner displays the status of the message with the highest severity level. For example, if you have an unread Message-level alert and an unread Error alert, the Messages label displays a red Error status. See "Read Messages and Alerts" on page 577 for more information.

- **Banner**
  On the web console banner, the Device Status Totals icons represent not only health status but the number of each devices. Click a number to view the devices in the Network tab.

- **Dashboard**
  Colors in the Device Health and Top Problem widgets indicate a device's health status. Select any part of the display color in the Device Health widget to display the devices in the Network tab.

- **Example**

![Device Health Widget](image)

- **Network**
From the **Network** tab, a device’s color indicates its health status. The colors of groups and hierarchies indicate the health status of the devices with the highest-severity status. See "Monitor Device Health" on page 58.

- **Jobs**

When viewing a currently running job, the status of the job is displayed. If you are viewing the Job History, all jobs are displayed with the completed job status. "View Current Jobs" on page 440.

The following table lists the statuses in Management Center, the colors associated with them, and descriptions of each status.

<table>
<thead>
<tr>
<th>Status</th>
<th>Color</th>
<th>How it applies to devices</th>
<th>How it applies to alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>red</td>
<td>A component on the device is failing, or is far outside normal parameters, and requires immediate attention. The job has not completed or has completed with errors. Red is also used for jobs that are running with errors. See &quot;View Current Jobs&quot; on page 440.</td>
<td>An error occurred, preventing an event from completing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> The ProxySG appliance’s Subscription Communication Status metric is in critical state.</td>
<td><strong>Example:</strong> During the device registration process, the connection test failed.</td>
</tr>
<tr>
<td>Warning</td>
<td>yellow</td>
<td>A component on the device is outside normal operating parameters and might require attention. Yellow is also used to show that an attribute on a device is in a warning state. See &quot;Monitor Device Health&quot; on page 58.</td>
<td>An error might occur if you do not take preventative action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> The ProxySG appliance’s SGOS Base License Expiration is in warning state.</td>
<td><strong>Example:</strong> The Management Center license will expire in 15 days or fewer. If you do not renew the license within 15 days, Error alerts display.</td>
</tr>
<tr>
<td>OK (device)</td>
<td>green</td>
<td>Components on the device are operating within normal parameters. The job has completed successfully. See &quot;View and Manage Job History&quot; on page 442.</td>
<td>A task was completed or a change was made.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> The monitored device has no health warnings or errors.</td>
<td><strong>Example:</strong> A user account was added.</td>
</tr>
<tr>
<td>Inactive</td>
<td>gray</td>
<td>The device is pre-deployment or deactivated. See &quot;About Pre-Deployed and Deactivated Devices&quot; on page 109 for information.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>
Log into the Web Console

Log into Management Center web console using a supported browser. For a list of supported browsers, refer to the Management Center Release Notes.

TLS 1.0 and TLS 1.1 are disabled on Management Center. To securely connect to the Management Center web interface using Internet Explorer 10 or later, you must enable TLS 1.1 and 1.2 on the browser. In the browser, select Internet Options > Advanced, and enable Use TLS 1.1 and Use TLS 1.2.

1. In the web browser, enter one of the following URLs:
   - http://IP_address:8080
   - https://IP_address:8082
   The browser displays the login screen.

   When enabled, the consent banner page displays before the login screen. If the user recognizes both the text and image, the user confirms that the system will be used for the purpose shown, by clicking Accept. "Configure Consent Banner" on page 529.

2. Enter your username and password, and click log in.

   The default username/password is admin/admin. To restore the default admin password, see “Reset or Restore Admin Account Passwords” on page 380.

3. You can request a password reset. Click Reset Password. For more information, see "Reset Password" on page 376. For added access control, administrators should enable password reset settings for users with the correct permissions. See "Automate Password Reset Process" on page 570.

4. Upon successful login, Management Center displays the main Dashboard.

   See "Web Console Overview" on page 31 and "Dashboards and Widgets" on page 517.
Navigate the Web Console

Refer to the following for an overview of navigational tools in the web console interface.

Tabs

The web console organizes information on tabs in two key areas at the top of the screen. The functional grouping of tabs that include the Dashboards, Network, Configuration, Jobs, Reports, and Administration tabs are organized for managing devices from Management Center.

- Functional areas in the web console are divided into tabs at the top of the screen, under the banner. Click a tab label to perform specific tasks. For example, click Network to manage your devices.
- In Dashboards, you can see the Home and Statistics Monitoring dashboards. To close a report, click the X on the tab.

The Administration tab has numerous sections that are specific to managing Management Center itself:

- Auditing
- Settings
- Users
- Groups
- Roles
- Hardware Attributes
- Logs
- Users Sessions
- License

Split Screens

In some areas of the web console, split bars divide screens into panes:

- From the Network tab, you can manage all devices in your network. The screens are divided into a left pane and a right pane with a filters pane on the right. The top pane displays the filters and a search field if the Details drop-down list has Details (rather than Tiles) selected.

If a split bar has an arrow on it, you can click the arrow to collapse or expand the split screen.

You can also move a split bar to resize panes: hover over the split bar until the pointer changes to divider. Then, drag the bar to a new location.

Information on Multiple Pages

In the following areas of the web console, items display on multiple pages if more than 50 items exist:

- Logs in Auditing
- Policy and Script Objects in Configuration
- Device search results in Network

Use the following features of the navigation bar at the bottom of a page to navigate pages:
Management Center Configuration & Management

- Click < > to move back or forward one page at a time.
- Click << >> to go to the first page or the last page of results.
- Enter a page number in the Page field.

The right side of the navigation bar indicates which items are displayed and the total number of items in the list:

### Required Ports, Protocols, and Services

Management Center uses the following ports while operating. Ensure that you allow these ports when setting up Management Center.

#### Inbound Connections to Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>8080</td>
<td>TCP</td>
<td>No</td>
<td>User’s client</td>
<td>Management Center web console</td>
</tr>
<tr>
<td></td>
<td>8082</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>User’s client</td>
<td>Management Center CLI</td>
</tr>
<tr>
<td>SSL</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>User’s client</td>
<td>Management Center API</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9009</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Starting with Management Center 1.7, Port 9009 is disabled unless HTTP is enabled via the security http enable command.</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9010</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics over HTTPS</td>
</tr>
</tbody>
</table>

#### Outbound Connections from Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>10389</td>
<td>TCP</td>
<td>Yes</td>
<td>LDAP server</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>389</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>636</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>10389</td>
<td>TCP</td>
<td>Yes</td>
<td>Active Directory server</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>389</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>636</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>1812</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Authentication</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1813</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Accounting</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>TCP</td>
<td>Yes</td>
<td>SMTP server</td>
<td>SMTP alerts</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>162</td>
<td>UDP</td>
<td>Yes</td>
<td>Trap receiver</td>
<td>SNMP traps</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Configurable?</td>
<td>Destination</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>--------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTP Proxy</td>
<td>8080</td>
<td>TCP</td>
<td>Yes</td>
<td>HTTP Proxy</td>
<td>Updates</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
<td>UDP/TCP</td>
<td>No</td>
<td>NTP server list</td>
<td>Time sync to customer-configured NTP time server</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Symantec</td>
<td><a href="https://support.symantec.com">https://support.symantec.com</a> License activation, Web Application Protection (WAP) subscription, the latest release information and documentation</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP/TCP</td>
<td>No</td>
<td>DNS server</td>
<td>FQDN lookups</td>
</tr>
<tr>
<td>MA</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Malware Analysis</td>
<td>Health monitoring and backup</td>
</tr>
<tr>
<td>PacketShaper</td>
<td>80/443</td>
<td>TCP</td>
<td>No</td>
<td>PacketShaper</td>
<td>Health Monitoring (unencrypted/encrypted)</td>
</tr>
<tr>
<td>Reporter</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Reporter</td>
<td>Reporter API (unencrypted/encrypted)</td>
</tr>
<tr>
<td>ProxySG</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance monitoring and management</td>
</tr>
<tr>
<td>Management Center</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>Management Center</td>
<td>Management Center communication with failover partner</td>
</tr>
<tr>
<td>VPM</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>Visual Policy Manager</td>
</tr>
<tr>
<td>CA</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Content Analysis</td>
<td>Health Monitoring (unencrypted/encrypted)</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9009</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics. Starting with Management Center 1.7, Port 9009 is disabled unless HTTP is enabled via the security http enalbe command.</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9010</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics over HTTPS</td>
</tr>
<tr>
<td>SSL Visibility</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>SSL Visibility</td>
<td>Health monitoring and configuration synch</td>
</tr>
</tbody>
</table>

**Required IP Addresses and URLs**

Ensure connectivity from Management Center to the following URLs.
<table>
<thead>
<tr>
<th>URL</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>199.116.168.195</td>
<td>TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>validation.es.bluecoat.com/phs.cgi</td>
<td>HTTPS</td>
<td>443</td>
<td>Validates the license every 5 minutes. After successful validation, validation occurs every hour.</td>
</tr>
<tr>
<td>bto-services.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Validates the license.</td>
</tr>
<tr>
<td>device-services.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>services.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>abrca.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Symantec CA.</td>
</tr>
<tr>
<td>appliance.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Trust package downloads.</td>
</tr>
<tr>
<td>subscription.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Subscription services.</td>
</tr>
<tr>
<td>upload.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Upload diagnostic reports to Symantec support.</td>
</tr>
<tr>
<td>sgapi.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Universal VPM policy.</td>
</tr>
</tbody>
</table>
Verify Web Console Access

After you install a new license or update an existing license, verify that you can access the web console. Refer to the Release Notes for a list of supported browsers.

TLS 1.0 and TLS 1.1 are disabled on Management Center. To securely connect to the Management Center web interface using Internet Explorer 10 or later, you must enable TLS 1.1 and 1.2 on the browser. In the browser, select Internet Options > Advanced, and enable Use TLS 1.1 and Use TLS 1.2.

1. Open a web browser.
2. In the address bar, enter the URL.
   
   https://ip_address:8082

   You cannot change the port number.

   The web browser displays the login screen.

   If the web console does not load, run the # license view CLI command to determine if the license was installed and is valid.
Move Items

To complete some tasks in the web console, you move items from one area or container to another. For example, you move items to add devices to groups, associate devices with policy, remove users from groups, and remove roles from users.

The following example shows the Edit User dialog, where you can add or remove roles to a user:

![Edit User dialog]

If the list of items is long, you can scroll down to locate the item to move. You can also search using the search field above it.

The web console allows several ways to move items:

Drag an item from one area to another. How to drag items

For example, to add a role to a user, select the role under Available Roles. Click and hold; the pointer turns into a hand cursor. Drag the role to Assigned Roles. The dialog displays a green line under Assigned Roles and the pointer turns into a pointer cursor, indicating that the role can be moved there.
Release the mouse button to move the role.

Drag a selected device to a device group. Associate Devices with Device Groups.

1. Click the **Network** tab. In the left pane, click **Unassigned Devices**. Unassigned devices display on the right pane. See "Ensure Devices Belong to Device Groups" on page 118.
2. Select the saved device.
3. To assign the device to a group, select the device and drag it into the device group into the tree on the left.
4. Drop the device into the device group. Confirm the move. Click **OK**.

---

**Encrypt Sensitive System Data**

In 1.6 and later, each Management Center appliance (hardware or virtual) has a unique encryption key that is used to encrypt data in the system. The administrator generates this key in the **Administration > Data Protection** page. When the key is generated, a recovery key is also generated in case you later need to restore the encryption key. Make sure to save the recovery key in a safe place.
Potential Data Loss

- As part of this process, you should keep the recovery key in a safe place in the event that you need to restore the encryption key later. DO NOT LOSE THE KEY. If you lose the key, you will not be able to recover your encrypted data.
- You should not recover a key unless you are certain that you need to. If you use the Restore previous key feature and the current data in the database was not encrypted with that key, that data will not be able to be decrypted and you will have to reenter all of the device passwords.
- If the current passwords for the device were not encrypted with the previous key, you will not be able to access the information with the current passwords. You will need to reenter the device passwords before accessing the backup information.

New Management Center Appliance Recommendations

Upon receiving a new appliance, you should do the following:

1. Select Administration > Data Protection.
2. Click Generate Key.
   
   A new encryption key is created and a recovery key is displayed.
3. Record the recovery key and secure it in a safe location.
4. Click Restart System.
5. Configure the appliance.
6. Run a Management Center backup. See "Back Up the Management Center Configuration" on page 546.

This process ensures that you can restore your configuration as necessary.

Upgrade Recommendations

If you are upgrading Management Center, Symantec recommends regenerating a new key and then taking a new backup. Doing so will ensure that you have the latest protection schemes and a valid backup that can be restored to the device if necessary.

1. Select Administration > Data Protection.
2. Click Generate Key.
   
   A new encryption key is created and a recovery key is displayed.
3. Record the recovery key and secure it in a safe location.
4. Click Restart System.
5. Run a Management Center backup. See "Back Up the Management Center Configuration" on page 546.

This process ensures that you will be able to restore the previous configuration if the upgrade has issues.
Management Center Solutions

What do you want to do in Management Center? See the following topics for assistance.

"Update the Management Center License" on page 556
"Add and Monitor Devices" on page 48
"Create and Manage Jobs" on page 429
"Add Users and Grant Permissions" on page 354
"Monitor Device Health " on page 58
"Manage Dashboards" on page 515

Create Web Application Firewall Policy

Implement Universal Policy

"Integrate Reporter into Management Center" on page 446
"View Consolidated Reports" on page 444

Modify Table Data

"Migrate Device Metadata from Director as Management Center Scripts" on page 536
"View Audit Log" on page 524

Define Management Center Settings

"Authenticate Users with SSL Mutual Authentication" on page 366
"Upload Files to Management Center" on page 532
"Regularly Back Up a Group of Devices" on page 91
"Back Up the Management Center Configuration" on page 546
Management Center Configuration & Management

Manage Devices

Refer to the following topics for assistance.

"Add a Device" on page 447
"Add a Device Group" on page 56
"Add Multiple Devices at Once" on page 64
"Edit a Device" on page 66
"Edit a Device Group" on page 68
"Launch a Device Console" on page 69
"Back Up Device Configurations" on page 89
"Use Device Information for Backup Job Image Metadata" on page 93
"View Device Backups" on page 95
"Restore Device Backups" on page 100
"Export Device Backups" on page 98
Import Device Backups
"Set the Number of Backup Slots" on page 523
"Monitor Device Health and Statistics" on page 103
"Stop Managing a Device" on page 108
"About Pre-Deployed and Deactivated Devices" on page 109
"Restart a Device" on page 109
"Synchronize Devices" on page 110
"Configure Hierarchy for Devices and Device Groups" on page 113
"Search for Managed Devices" on page 116
"Perform an Operation on a Managed Device" on page 117
"Ensure Devices Belong to Device Groups" on page 118
"Monitor Device Health" on page 58
Verify Device Details
"View System Metrics" on page 121
"RMA a Device" on page 123
"Put Device in Read-Only Mode" on page 125
Add Device Group Attributes
Add and Monitor Devices

The Network dashboard (left pane > Network) presents data about managed devices and enables you to perform operations on them. Before you can view appliance data, you must add the device to Management Center. To import multiple devices, see "Add Multiple Devices at Once" on page 64 or "Migrate Device Metadata from Director as Management Center Scripts" on page 536.

To run operations on managed devices, see "Perform an Operation on a Managed Device" on page 117.

You can manage up to 500 devices in Management Center.

Create Hierarchy and Group Views

You require a way to administer and monitor devices in your network, which might comprise a complex organizational or geographical scheme. In Management Center, you can manage the devices in your network within a hierarchical structure.

Management Center comes with a predefined structure for device management, as follows:

- Location (Hierarchy)
  - World (Group)
    - France, Canada, Germany, and others (Subgroups)
Management Center Configuration & Management

- Organization (Hierarchy)
  - Company (Group)
    - Finance, Sales, Legal, and others (Subgroups)

You can use these predefined hierarchies and groups, but if you must organize the devices in your network using different criteria, you can create your own hierarchies and groups. Then, create device groups and subgroups to logically represent the structure of your network.
Add a Device

Before you can manage and monitor your devices, you must add them to Management Center. Devices that can be added to and managed by Management Center include the following:

- Advanced Secure Gateway (credential authentication or public key)
- Content Analysis
- Malware Analysis
- PacketShaper
- ProxySG (credential authentication or public key)
- Reporter
- Security Analytics
- SSL Visibility
- Web Security Service

Configure how often devices are polled. See "Set the Device Polling Interval" on page 523.

About Public Key or Credential Authentication for ProxySG or Advanced Secure Gateway

When adding a device, you must specify how Management Center will connect to it. Management Center can connect to a device using the following methods:

- **Credential authentication**: Management Center uses the device's credentials to connect. Credential authentication is considered less secure because the device's credentials are stored in Management Center. Therefore, it is recommended that you use public key authentication.

  Management Center always uses credential authentication when importing devices from Director.

- **Public key authentication**: Management Center inserts a copy of its public key onto the device. The device then "trusts" Management Center connections. This authentication method is considered more secure because device credentials are not stored on Management Center.

  Management Center does not remove its public key from devices that are deleted and no longer managed. You can manually delete the key using the following CLI command on the ProxySG or Advanced Secure Gateway:

  # (config ssh-console) delete director-client-key key-id

About Host Key Validation

Host key validation is a feature of the SSH protocol. It is designed to prevent devices from impersonating legitimate servers in an attempt to steal credentials and data (man-in-the-middle attack). To prevent this, each device has a unique host key that can be used to establish a host's identity. If a device supports it, Symantec recommends that you enable host key validation because the method can warn you of a man-in-the-middle attack. In that case, Management Center notes that host verification failed and prompts you to verify the SSH host fingerprint.

You can verify the host fingerprint using one of the following methods:
Enter the following command from a terminal that has a trusted network path to the device:

```bash
# ssh keygen -lf <(ssh-keyscan device_ip 2>/dev/null)
```

The system displays the host key.

Do the following from the device's serial connection:

a. Enter the following command:

```bash
# (config ssh-console) view host-public-key sshv2
```

b. Copy the output to a file, for example, /tmp/hostkey.

c. Enter the following command from a system running OpenSSH 7.2:

```bash
# ssh-keygen -l -e sha256 -f /tmp/hostkey
```

The system displays the host key.

### Add a ProxySG or Advanced Secure Gateway using Credential Authentication

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the Add Device wizard.
4. Select the device type.
5. Specify the **Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
   - Specify whether to collect statistics for the device. See "View Statistics Monitoring Reports" on page 501.
6. In **Connection**, click **Credentials**. Set the following:
   - The IP address or hostname of the device.
   - The SSH port.
   - The username and password you use to authenticate to the device.
   - Your enable password for administrator actions.
   - Confirm whether to **Enable host key validation** (recommended).
7. Click **Connect**. Management Center attempts to connect to the device using the information you entered.
8. If you enabled host key validation, verify the SSH Host Fingerprint and click **Accept**.
9. Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

10. Verify or change the **Device Name**.
12. Click **Save**.
The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

**Add a ProxySG or Advanced Secure Gateway using Public Key Authentication**

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click Add Device. The system displays the Add Device wizard.
4. Select the device type.
5. Specify the Modes:
   - Select Existing device if the device is already installed, or Unavailable (pre-deployment) if the device is not available yet. See “About Pre-Deployed and Deactivated Devices” on page 109 for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See “Put Device in Read-Only Mode” on page 125 for more information.
   - Specify whether to collect statistics for the device. See “View Statistics Monitoring Reports” on page 501.
6. In Connection, click Public Key. Set the following:
   - The IP address or hostname of the device.
   - The SSH port.
   - Your enable password for administrator actions.
   - Confirm whether to Enable host key validation (recommended).
7. Click Connect. Management Center attempts to connect to the device using the information you entered.
8. If you enabled host key validation, verify the SSH Host Fingerprint and click Accept.
9. Enter the username and password you use to authenticate to the device. You must do this so that Management Center can install its public key onto the ProxySG appliance. The credentials are not saved.

   Management Center attempts to connect to the appliance. If the connection is established, the system displays Successful.

   If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

10. Verify or change the Device Name.
11. Optional—Input any applicable attributes. See “Add Attributes” on page 401.
12. Click Save.

   The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

**Add a Reporter**

Symantec recommends that you create a new non-administrator Reporter role before adding Reporter to Management Center. If you choose to add a Reporter using the default Admin role, you must specify the role as "_admin."

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click Add Device. The system displays the Add Device wizard.
4. Select the device type.
5. Specify the Modes:
   - Select Existing device if the device is already installed, or Unavailable (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
6. In Connection, specify the following:
   - The IP address or hostname of the device.
   - The protocol and port (HTTP or HTTPS).
   - The username and password you use to authenticate to the device.
   - The Reporter role. Specify the role assigned to this user in Reporter. If this is an admin account, input _admin.
7. Click Connect. Management Center attempts to connect to the device using the information you entered.
   Management Center attempts to connect to the appliance. If the connection is established, the system displays Successful.
   
   If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

8. Verify or change the Device Name.
10. Click Save.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility

If you upgrade an SSL Visibility appliance from 3.x to 4.x, you must delete the 3.x device from Management Center and then add it back as a 4.x device.

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click Add Device. The system displays the Add Device wizard.
4. Select the device type.
5. For SSL Visibility only, select the version 3.8.3+ or 4+.
6. Specify the Modes:
   - Select Existing device if the device is already installed, or Unavailable (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
7. In Connection, specify the following:
   - The IP address or hostname of the device.
   - The protocol and port (HTTP or HTTPS).
The username and password you use to authenticate to the device.

8. Click **Connect**. Management Center attempts to connect to the device using the information you entered.

Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.

![Warning](image1)

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

9. Verify or change the **Device Name**.
11. Click **Save**.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

### Add a Security Analytics

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the Add Device wizard.
4. Select **Security Analytics**.
5. Specify the **Device Management Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
6. In **Connection Details**, specify the following:
   - The IP address or hostname of the device.
   - The port (the default is HTTPS 443).
   - The username you use to authenticate to the device.
   - In the **Password** field, enter the Security Analytics device API key.
7. Click **Connect**. Management Center attempts to connect to the device using the information you entered.

Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.

![Warning](image2)

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

8. Verify or change the **Device Name**.
10. Click **Save**.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

### Add Web Security Service (WSS)

...
Management Center Configuration & Management

Note: As of November 2017, all connections from Management Center to WSS use the same username, \textit{mc-register} and a unique token that identifies your WSS account as unique. This token associates your connection with the appropriate WSS account.

1. Select the \textbf{Network} tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click \textbf{Add Device}. The system displays the \textbf{Add Device} wizard.
4. Select the device type.
5. Specify the \textbf{Modes}:
   - Select \textbf{Existing device} if the device is already installed, or \textbf{Unavailable} (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select \textbf{Read/Write} or \textbf{Read Only}.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
6. Open another browser, and log in to the WSS portal at \url{https://portal.threatpulse.com}.
   a. Click the \textbf{Solutions} menu and select \textbf{Service}.
   b. Click \textbf{Account Maintenance} and select \textbf{Integrations}.
   c. Click \textbf{New Integration}. The portal displays the \textbf{New Integration} wizard.
   d. Set the \textbf{Expiry Type} as appropriate for your purposes. If you select \textbf{Never}, the token can be used indefinitely.
   e. Copy the contents of the \textbf{Token} field and click \textbf{Save}.
7. Switch back to Management Center and do the following:
   a. Select the \textbf{Cloud Network} to connect to, Production or Pre-Production.
      
      \textbf{If you are participating in a beta program, click Analyze in Pre-Production.}
      
      b. Click \textbf{Connect}.
      c. Enter \textit{mc-register} as the username and paste the integration token from the portal as the password.
      d. Click \textbf{Register}. After successfully connecting, the system populates the \textbf{Name} fields.
      
      \textbf{After connecting to the WSS, Management Center deletes the credentials. They are not saved. For failover, this has special implications.}
      
      \textbf{If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.}
7. Verify or change the \textbf{Device Name}.
8. Optional—Input any applicable Name. See "Add Attributes" on page 401.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>&quot;Ensure Devices Belong to Device Groups&quot; on page 118</td>
</tr>
<tr>
<td>Check information specific to the selected device.</td>
<td>&quot;Monitor Device Health &quot; on page 58</td>
</tr>
<tr>
<td>Check device metrics.</td>
<td>&quot;View System Metrics&quot; on page 121</td>
</tr>
</tbody>
</table>
Add a Device Group

A device group is a folder in the device organizational structure that exists below the hierarchy level and contains devices or sub-folders.

1. Select the Network tab. In the left pane, select the hierarchy in which you want to create the device group.
2. (If applicable) Browse to the folder in which you want to create the device group. Select Add Group.
3. On the Add Group: Basic Info dialog, enter a name and a description. An asterisk denotes fields that are mandatory.
4. Select a parent group from the Parent Group drop-down list. An asterisk denotes fields that are mandatory. Click Next.
5. On the Add Group: Attributes dialog, use the up/down arrows to specify Bandwidth Cost. Bandwidth Cost is a multiplier and is thus not expressed in a specific currency unit. For example, you can enter a value to represent on average how you pay per gigabit for data usage on your network. "Set Bandwidth Cost for Reports" on page 523.
6. (Optional) Specify your Primary Contact for the device group, as well as the Location device group and the sub-group.
7. Click Next. The Add Group wizard displays the Add Group: Membership.

8. Select devices from the Available Devices list and add them to the Associated Devices list.
9. Click Finish. The new device group is displayed under the network tab. If you cannot see the new device group, select Unassigned Devices and "Ensure Devices Belong to Device Groups" on page 118 or "Configure Hierarchy for Devices and Device Groups" on page 113.

You can define attributes for a particular a device, device groups policy and script objects. See "Manage Attributes" on page 400.
Set the Device Polling Interval

You can specify the frequency with which Management Center looks for updates on managed devices. Specify an appropriate interval to ensure that device health statuses display accurately. The default interval is 10 seconds.

1. In the web console banner, select the Administration tab and select Settings.
2. Select General on the left. General fields display on the right.
3. Select Device Polling Interval (sec).
4. Enter a value in seconds.
5. Do one of the following:
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server.
   - Click Activate to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.
Monitor Device Health

Management Center collects health status information on device components including system resources, license validity, and user-defined health checks, and displays the aggregate health status in several areas.

Device health is always represented by status colors: **Error** (red), **Warning** (yellow), and **OK** (green). A device’s health status is determined by system-defined thresholds on the device: if a service or other monitored component exceeds a threshold, the device goes into a Warning or Error state.

If you cannot get the device out of the **Error** state, regardless of what you try, you may need to RMA the device. See "Perform an Operation on a Managed Device" on page 117.

A gray status color indicates an absence of health status and represents an **inactive** device. Some jobs and operations cannot occur on inactive or pre-deployed devices.

See "About Color-Coded Status Indicators" on page 34 for more information on status colors in various areas of the web console.

---

For more information on monitoring health status on the ProxySG appliance, refer to the *SGOS Administration Guide*.

---

View Device Health Status on the Dashboard

The Dashboard displays overall health status information in widgets. Two widgets display by default, but you can close them by clicking the X in the top right corner.

The **Device Health** widget gives an overall picture of the health of monitored devices in a circle graph.

---

Click a status icon below the chart to see the devices that have that status.

The **Top Problem Devices** widget lists the devices that are consistently displaying with errors or warnings.
For example, if you click on the first SG300 Series device, the Device Overview displays the health status as red with the specific errors and warnings for each device value.

If you have removed a widget from the Dashboard, you can display it again. See "Change the Dashboard Layout or Refresh Rate" on page 519 for instructions.

View Health Status in the Banner

In the web console banner, look for the device status icons.

Click a status icon to see the devices that have that status. These totals are the same as the device status totals that display under the Device Health widget on the Dashboard; because these are in the banner, they are visible to you no matter which tab you are working on.

View Device Health Status

1. Select the Network tab.
2. Select the device whose health you want to view. Overview, System Metrics, Dashboard, Health Checks and Backup tabs display at the bottom of the screen.
3. Click **Health Checks**. The web console displays information about the system resources for the selected device. Each device type provides unique health details. Consider the images below. The first is from a ProxySG appliance, while the second is from an SSL Visibility appliance.

To view the health of a device, select the device or group of devices. If the Health status section of the page is not visible, click the up arrow at the bottom of the page to display it.

![Health Checks for ProxySG appliance](image1)

![Health Checks for SSL Visibility appliance](image2)

**Note:** As of Management Center 1.11.1, SSL Visibility appliances running version 4.0 or later support health reporting for **License**, **Load**, **Network**, and **System** attributes with the Up/Down column. Earlier versions of SSL Visibility do not support this functionality.

### View Device Dashboards

A dynamically generated dashboard is available for device monitoring.

1. Select the **Network** tab.
2. Select the device whose health you want to view. **Overview**, **System Metrics**, **Dashboard**, **Health Checks** and **Backup** tabs display at the bottom of the screen.
3. Click **Dashboard**. The web console displays system status metrics. The content available will vary with the device:

*ProxySG/Advanced Secure Gateway Dashboard*
Content Analysis (CA) 2.1+ appliances include on-board Malware Analysis (MA). If the MA is licensed and enabled, the dashboard for CA 2.1 displays 7 additional panels for internal sandboxing data.
The Dashboard is not supported for Security Analytics devices in Central Manager (CMC) mode.

SSL Visibility Dashboard

SSL Visibility devices running version 3.x do not display dashboard information.

Metrics

The metrics may be displayed in one of several different ways:

- Counters: Displays a count for a specific time period.
  
  Examples: Object Count, Total Scan.

- State: Displays a text value.
  
  Examples: Condition - Green/Yellow/Red condition indicator.

- Series: Displays values over a period; this presentation may be in an area display, a bar, a column, a pie chart, or a donut chart.

  Examples: CPU, ICAP Scan.
Resolve Device Errors

See Resolve Device Errors for more information.
Add Multiple Devices at Once

To add multiple devices using a CSV file, you can use Management Center's template CSV file, or you can create your own. You can import multiple devices of various types, including:

- ProxySG appliances
- Advanced Secure Gateway (ASG) appliances
- Content Analysis appliances
- Malware Analysis appliances
- PacketShaper appliances
- SSL Visibility appliances
- Reporter

Import Devices Using a CSV File

Before importing devices, ensure that the device groups that you want to assign the devices to have been created on Management Center. See "Add a Device Group" on page 56 for more information.

1. From the web console, click **Network**.
2. Select **Operations > Import from File**.

3. Select the **Import devices from manually created CSV file**.
4. Click **Launch Import Wizard**. The web console displays the Import Devices wizard.
5. From the Select Device Type dialog, select the device type that you want to import. Click **Next**.
6. You can either Download CSV Template or **Select File** and browse to the location of the import file containing all of the devices. Click **Next**.

   If you download the CSV template, open it and add your devices to it. Refer to the following table for descriptions of the CSV file columns.
7. After the devices are uploaded, they are displayed in the **Import Devices: Assign Groups** dialog.
8. Select the devices to assign to a device group.

To add an imported device to a group using a CSV file, the group must already exist in Management Center. Therefore, ensure that you have created the desired groups before importing. You cannot create them using the CSV file.

9. After the devices have been selected, from **Device Group**, select the object selector. From the available device groups or hierarchies, select a device group. The selected device group is displayed when you select it. Click **OK**. To apply the imported devices to the device group, click **Apply**.

10. (Optional) Repeat Step 9 until all imported devices belong to a device group or hierarchy.
11. When you are finished assigning the imported devices to device groups, click **Finish**.

### Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>&quot;Ensure Devices Belong to Device Groups&quot; on page 118</td>
</tr>
<tr>
<td>View information about an imported device.</td>
<td>&quot;Verify Device Details&quot; on page 119</td>
</tr>
<tr>
<td>Edit device information.</td>
<td>&quot;Edit a Device&quot; on the facing page</td>
</tr>
<tr>
<td>Check device metrics.</td>
<td>&quot;View System Metrics&quot; on page 121</td>
</tr>
</tbody>
</table>
Edit a Device

You can edit device metadata, connection parameters, and the membership within a hierarchy and device group, and view the effective policy for each slot.

Procedure

1. Select the Network tab. (Optional) Browse to the hierarchy and folders/subfolders where the device you want to edit belongs. An asterisk denotes fields that are mandatory.
2. Select a Device.
3. Click Edit. Five tabs within the Edit Device wizard display editable fields:
   - Basic Info
   - Connection Parameters
   - Membership
   - Attributes
   - Policies
4. Click the Basic Info tab. Edit the device name and description and view the deployment status, model number, serial number, and OS version. See "About Pre-Deployed and Deactivated Devices" on page 109.
5. Click the Connection Parameters tab. The following fields are all required:
   - The IP address or hostname of the device
   - The username and password you use to authenticate to the device
   - The enable password for administrator actions.
   - The SSH port.
6. Click Test Connection. Management Center attempts to connect to the device using the information you edited.
7. Click the Membership tab. (Optional) Edit membership with the drop-down lists assigned to Hierarchy and the following:
   - Device Groups
   - Location
   - Organization
8. Click the Attributes tab. Mandatory attributes for the device are marked with a red asterisk (*). You can change the value on mandatory attributes, but you cannot delete "Mandatory Attributes" on page 403.
9. Select the Policies tab. The Edit Device displays the effective policy for each slot. The Policy Name mapped to each slot is displayed and the following assignments are displayed:
   - Direct assignment - The policy was installed directly to the slot.
   - Inherited from [Device Group Name] - The policy was inherited from device group that the device membership is from.

The Local, Central, and Forward slots display CPL policy only. See "Create a CPL Policy Object" on page 189 or see "Create a CPL Policy Fragment" on page 223

10. After you have completed editing the tabs for each device, click Save.

View Effective Policy for Each Slot on the Device

You can view the effective policy for each slot on the device from the Policies tab.
### Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>&quot;Ensure Devices Belong to Device Groups&quot; on page 118</td>
</tr>
<tr>
<td>View information about the device.</td>
<td>&quot;Verify Device Details&quot; on page 119</td>
</tr>
<tr>
<td>Choose Operations for a Device or Device Group.</td>
<td>&quot;Perform an Operation on a Managed Device&quot; on page 117</td>
</tr>
<tr>
<td>Edit device attributes.</td>
<td>&quot;Edit Attributes&quot; on page 404</td>
</tr>
<tr>
<td>Edit policy attributes.</td>
<td>&quot;Edit Attributes&quot; on page 404</td>
</tr>
</tbody>
</table>
Edit a Device Group

You can edit any device group, including the system’s predefined parent groups (the top-level folders in the Location and Organization hierarchies).

1. Select the Network tab.
2. In either Tiles view or Details view, browse to the parent folder of the group you want to modify.
3. Select the group and click Edit. The web console displays the Edit Group wizard.
4. Edit the information on each tab as required:
   - **Basic Info** - Change the device group name and description.
   - **Attributes** - Under System, change the statistics collection option and bandwidth cost. For information on the User-defined attributes, see “Filter Devices or Device Groups in a Permission” on page 393.
   - **Membership** - Add or remove devices.
5. Click Save.
Launch a Device Console

Management Center offers a central location from which you can open the console of any managed Symantec device so that you can log in to the device.

1. Select the Network tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. Select one of the following:
   - From the Operations drop-down list, click Launch Console.
   - or
   - At the bottom of the web console, make sure the Overview tab is selected and click Launch Console.
4. Log in to the device.

View Device License Information

Management Center allows you to monitor the health status of a device's license and its associated components. Devices are polled hourly for license changes.

Some unmonitored devices may show licensing information while others do not. If you disable statistics collection on a device that was previously monitored, it will show the last license data. Devices that were never monitored show no license data.

1. Select the Network tab.
2. Select the device group in the left pane.
3. Select the Licenses tab. The system displays the license information for all applicable devices in the group, including the licensed components, time to expiration, and the expiration date.
4. To review the license details for a specific device, click the + symbol next to the device's IP address.

   The system then displays the same details for each associated license and component.
5. Optional: Click Export Data to save the data to a .csv file.

Upgrade System Images on Managed Devices

You can install system images to the following devices:

- ProxySG appliance
- Advanced Secure Gateway
- Content Analysis
Management Center Configuration & Management

- Malware Analysis
- SSL Visibility

Restrictions
- Downgrading a Content Analysis 2.x appliance is not supported.
- Upgrading SSL Visibility appliances from 3.x to 4.x requires other tasks not documented here. If you upgrade an SSL Visibility appliance from 3.x to 4.x, you must delete the 3.x device from Management Center and then add it back as a 4.x device.
- Downgrading SSL Visibility appliances from 4.x to 3.x is not supported.

Install System Image

To install system images on managed devices, complete the following steps.

1. Ensure that the system image has been uploaded to Management Center and that it has been associated with the correct device type. See "Upload Files to Management Center" on page 532 for more information.
2. Select Jobs > Scheduled Jobs > New Job.
3. In the Basic Info dialog, enter a name for your job. An asterisk denotes fields that are mandatory.
4. Enter a description of the job. Good descriptions help to differentiate jobs when they have similar names. Click **Next**.
5. Select **Install System Image** from the **Operation** drop-down list.

6. Click the **System Image** field. The system displays the Select System Image dialog.
7. Select the system image and click **OK**.
8. Optional—Select **Restart device(s) after installation** to restart the target device after installation, which is required to load the installed image on some device types.
9. Select the Delivery method:

- **Upload image to targets**

  Choose this option to push the image to the target devices.

  If the target devices are connected to the Management Center using SSH public key connections, enable the **if credential not available, pull image from Management Center** check box. This option directs the target device to pull the image from Management Center in the event that SSH authentication to the device fails.

  Upload is supported for the Malware Analysis, SSL Visibility, Content Analysis, ProxySG, and Advanced Secure Gateway appliances.

  Do not alter the file names for Malware Analysis images when uploading them to the Management Center file server. This is required for successful installation of the image to the Malware Analysis when the appliance has downloaded the image but installation was scheduled for another time.

- **Download image from Management Center**

  Choose this option so that the target devices download the image from the Management Center file server. This method is supported only by Content Analysis, ProxySG, and Advanced Secure Gateway.

  - Optional (for download only)–Select **pull over secure connection**

    This option determines whether the device will use HTTP or HTTPS to download the image from the Management Center file server. Choose this option if Management Center has a certificate from a trusted certificate authority (CA). If Management Center uses a self-signed certificate that is not trusted (a common scenario), choosing this option may cause the download to fail.

    If you choose the non-secure option, HTTP must be enabled on Management Center. To enable HTTP, enter the following CLI commands:

    ```
    # en
    #security http enable
    ```

10. Click **Next**.
11. Select the target device(s) and click **Next**.
12. Select a job schedule and click **Finish**.
Troubleshooting

If the upgrade operation is not successful, check the following:

- Verify HTTP/HTTPS connectivity between Management Center and the target device(s).
- Verify that the image being installed is associated with the correct device type.
- Check Management Center and target device logs for errors.

Receive Error Notifications

Configure how you will be notified when errors occur in Management Center.

| Configure Alerts for Device Errors | ................................................................. | 74 |
| Configure SNMP Alerts             | ............................................................. | 75 |
| Configure SMTP Alerts             | ............................................................. | 76 |
| Manage Alerts                     | ....................................................................... | 77 |

Alert Notifications

<table>
<thead>
<tr>
<th>Description</th>
<th>Message Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware monitor warnings or critical errors.</td>
<td>&lt;monitor_name&gt; has exceeded &lt;level_name&gt; level of &lt;#&gt;%, current usage is &lt;#&gt;%.</td>
</tr>
<tr>
<td>Database disk quota warning.</td>
<td>Statistics Monitoring DB exceeded allowed disk quota. Collector to reject upload requests.</td>
</tr>
<tr>
<td>Critical repository messages.</td>
<td>Unable to create/start the repository, &lt;repository_name&gt;. The system is stopping.</td>
</tr>
<tr>
<td></td>
<td>Unable to initialize the &lt;repository_name&gt; repository.</td>
</tr>
<tr>
<td>Internal critical errors.</td>
<td>Subscription URLs are not installed.</td>
</tr>
<tr>
<td>Errors with auditing user actions.</td>
<td>Unable to write audit record, user: &lt;username&gt;, event: &lt;action&gt;.</td>
</tr>
<tr>
<td>Management Center license errors due to duplicate serial or server avoidance.</td>
<td>License error &lt;message_string&gt;:</td>
</tr>
<tr>
<td>Migration errors during an upgrade.</td>
<td>Migration step: &lt;step_name&gt; failed. Changes made by the step have been rolled back, but migration steps that have completed successfully have been retained. Subsequent steps have been canceled.</td>
</tr>
<tr>
<td>Statistics monitoring exceeds the disk quota.</td>
<td>Statistics Monitoring DB exceeded allowed disk quota. Collector to reject upload requests.</td>
</tr>
</tbody>
</table>
### Description

<table>
<thead>
<tr>
<th>Description</th>
<th>Message Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raise alert whenever a device's license (or any of its sub-components) are about to expire. The warning shows within 30 days of the expiration.</td>
<td>License component &lt;component_name&gt;, for device &lt;device_name&gt; has, or will, expire on &lt;date&gt;.</td>
</tr>
<tr>
<td>If a device license expires, the warning alert closes to open an error alert.</td>
<td>State changed from NEW to CLOSED. System closed alert because license expired.</td>
</tr>
<tr>
<td>If a device license, in the warning state, is renewed, the warning alert closes because of subscription renewal.</td>
<td>State changed from NEW to CLOSED. System closed alert because license was renewed.</td>
</tr>
<tr>
<td>If a device license, in the error state, is renewed, the error alert closes because of subscription renewal.</td>
<td>State changed from NEW to CLOSED. System closed alert because license was renewed.</td>
</tr>
</tbody>
</table>

### Configure Alerts for Device Errors

Use the settings on the Administration > Settings > Alerts page to enable alerts, configure alerting thresholds, and specify alert severity.

**About Alerting**

- An alert is raised when a device is in a **WARNING** or **ERROR** state.
- SMTP or SNMP messaging occurs only for alerts with the severity of **WARNING** or **ERROR**.
- An alert is only generated if the device stays above the specified alert threshold for longer than 60 seconds (about 100 seconds on average).
- The alert clears when the device returns to normal.
- The alert count will increment for each detection of the same alert. Multiple alerts are not sent.

**Enable Alerting**

1. Go to Administration > Settings > Alerts.
2. Select **Raise Alerts on Device Errors**. This is a global switch. If it is not enabled, no alerts are generated.
3. To enable or disable a specific alert, select **Enable alert**.

   ![Device Health Response Time](image)

   - **Device Health Response Time**
   - **Enable alert**:
   - Alert when device, to respond with health status, takes longer than (in seconds):
   - Alert with severity:

4. Examine the threshold for the alert and alter it if desired.
5. Specify the severity of the alert: **INFO, WARNING, or ERROR**.

   If you have configured **SNMP** or **SMTP alerting**, notifications are only sent for alerts with a severity of **WARNING** or **ERROR**.

6. Click **Save**.
7. Click **Activate** to restart the service.

**View Alerts**

To view and manage your alerts, see "Manage Alerts" on page 413.

**Configure SNMP Alerts**

By using the SNMP protocol, alerts can be sent by Management Center to other computers. An SNMP trap is sent each time an alert is generated by Management Center. These traps are sent in the Management Information Protocol (MIB) format.

The Simple Network Management Protocol (SNMP) itself does not define which variables a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs).

**Restrictions**

- SNMPv1 traps are not supported in Management Center 1.10.1.1 and later.
- Content Analysis 2.2 SNMP trap settings are not backed up and restored.

Configure SNMP settings for Management Center. If you want to enter a password for the SNMP traps, see "Configure the SNMP Agent Password" on page 529.

The MIBs are available on the [Downloads](#) page. Refer to the *Management Center Release Notes* for information on MIBs.

1. Select **Administration > Settings**.
2. Select **SNMP Alerts**. SNMP fields display on the right. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>What to send*</td>
<td>Specify OFF to turn off SNMP notifications or ERROR when errors occur with the SNMP traps.</td>
<td>OFF</td>
</tr>
<tr>
<td>SNMP Destination IP*</td>
<td>Specify an IP address for the listener.</td>
<td>Example: 192.0.2.0</td>
</tr>
<tr>
<td>SNMP Destination port*</td>
<td>Specify the port for the listener.</td>
<td>Example: 155</td>
</tr>
<tr>
<td>SNMP Version*</td>
<td>Specify the protocol version for the SNMP listener.</td>
<td>2</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Input Value/Format</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Community</td>
<td>A password that allows access to a device's statistics (transmitted in plaintext).</td>
<td>Enter the password. See &quot;Configure the SNMP Agent Password&quot; on page 529.</td>
</tr>
<tr>
<td>Engine ID</td>
<td>The unique SNMP engine ID based on the device IP. This engine ID is associated with the specific Management Center installation and displays in each SNMP packet to identify the source of the packet. Applies to SNMPv3 only.</td>
<td>Click <strong>generate</strong> to generate the engine ID.</td>
</tr>
<tr>
<td>Security</td>
<td>Use name used to access the management module. Applies to SNMPv3 only.</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Auth Protocol</td>
<td>The authentication protocol algorithm to use. SHA is the default. Applies to SNMPv3 only.</td>
<td>SHA</td>
</tr>
<tr>
<td>Auth Passphrase</td>
<td>Passphrase to use for authentication. Applies to SNMPv3 only.</td>
<td>Enter the passphrase.</td>
</tr>
<tr>
<td>Priv Protocol</td>
<td>The protocol to use for SNMP message privacy. AES is the default. Applies to SNMPv3 only.</td>
<td>AES</td>
</tr>
<tr>
<td>Priv Passphrase</td>
<td>Passphrase to use when encrypting messages. Applies to SNMPv3 only.</td>
<td>Enter the passphrase.</td>
</tr>
</tbody>
</table>

4. Perform one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server.
     If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

**Configure SMTP Alerts**

Configure the mail server for sending health monitoring notifications from Management Center and specify which administrators receive the alerts.

1. Select **Administration > Settings**.
2. Click **SMTP Alerts** on the left. SMTP fields display on the right. An asterisk denotes fields that are mandatory.
### Setting | Description | Input Value/Format
---|---|---
What to send* | Specify OFF to turn off e-mail notification or ERROR when errors occur with mail delivery. | OFF|ERROR
Mail Server* | The SMTP mail server to use for outgoing mail. | Example: smtp.organization.com
Send to address* | E-mail addresses to which alerts are sent. For example, enter administrators' e-mail addresses or a distribution list. | A comma-separated list of valid e-mail addresses.
From address* | The e-mail address from which e-mails are sent. | Example: bccm@organization.com

4. Perform one of the following:
- Click **Reset** to remove your current changes and revert to the default or last saved settings.
- Click **Save** to store the settings on the server. If you are unable to save your changes, make sure that all required settings are specified.
- Click **Activate** to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

### Manage Alerts

Management Center provides an area for administrators to store and manage various alerts. The settings on the *Administration > Alerts* page enable you to change the state of an alert, change the owner, provide feedback, or find a specific alert.

This is different from the message viewer. To view messages in the Recent Messages pane, see "Read Messages and Alerts" on page 577.

Go to the **Alerts** management page using one of the following methods:
- Select **Administration > Alerts**.
- Click the **Alert Notification** icon. This shows the number of open (or unresolved) alerts.

### Overview

The landing page shows the current alerts and the options available for management.

- **Sorting** options allow you to view the alerts based on various criteria.
  - **Severity** | **Priority** | **Message** | **Category** | **State** | **Received** | **Acknowledged** | **Owner**
- **Details and Filters Tabs** give quick information about the alert(s).
- **Navigation** options at the bottom allow you to go to specific pages.

- **Management** options allow you to take action on specific alert(s).

### Sorting Alerts

The primary element on the landing page is the list of available alerts. These can be sorted by different columns.

*Indicates columns that are NOT shown by default*

<table>
<thead>
<tr>
<th>Sort By</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Impact level of an alert on the affected category.</td>
</tr>
<tr>
<td>Priority</td>
<td>Importance level of resolving an alert.</td>
</tr>
<tr>
<td>Message</td>
<td>Current status of an alert. Alerts are either considered open or closed.</td>
</tr>
<tr>
<td>Count*</td>
<td>Number of times an issue is reported.</td>
</tr>
<tr>
<td>Source*</td>
<td>System reporting an alert. Note: This field is populated only if an external network is reporting an issue.</td>
</tr>
<tr>
<td>Category</td>
<td>Element affected by an alert.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of an alert.</td>
</tr>
<tr>
<td>Received</td>
<td>Date and time an issue is reported as an alert</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Received status of an alert.</td>
</tr>
<tr>
<td>Owner</td>
<td>Person currently responsible for an alert.</td>
</tr>
</tbody>
</table>

Sort and view the alerts with these options:

- Adjust the length of columns by hovering between two columns to get the adjustment cursor.

- To sort the list, you have two options:
  - Click on a column header. The first click sorts the list by that column in ascending order. A second click sorts it in descending order.
  - Hover over a column header, then select **Menu Arrow > Sort Ascending** or **Sort Descending**.

- To customize which columns show, hover over any column header, then select **Menu Arrow > Columns**.
To reset the columns back to the default columns and width, hover over any column header, then select Menu Arrow > Reset Columns.

Details and Filters Tabs

Get an overview of a specific alert or use filter options in order to find specific alerts.

If you need more space to view the alerts list, collapse this pane by clicking the arrow tab on the left of it. See Filters Panel for an example image.

Preview Details Panel

Gives a brief summary of the selected alert. If you need to view more details, such as the history of the alert, see Editing Alerts.

Select only one alert to preview the details.

Filters Panel

Find specific alerts with various filters. Once applied, the Filters tab shows how many active filters there are. Example: (Active 3).
**Apply/Clear**

Save or delete any filter changes selected.

**Customize**
Select the filters that show in the **Filter Panel**.

![Filter Panel]

**Time Range**
Select the time range you want to search in.

<table>
<thead>
<tr>
<th>Hour Options</th>
<th>Day Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 1 Hr</td>
<td>Last 24 Hrs</td>
</tr>
<tr>
<td>Last 12 Hrs</td>
<td>Last 3 Days</td>
</tr>
<tr>
<td>Last 24 Hrs</td>
<td>Last 7 Days</td>
</tr>
</tbody>
</table>

**State**
Select the alert current status(es).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>New or unworked issues.</td>
</tr>
<tr>
<td>Pending</td>
<td>Already known issue, but resolution hasn't started.</td>
</tr>
<tr>
<td>Assigned</td>
<td>Assigned to a specific user.</td>
</tr>
<tr>
<td>In Progress</td>
<td>A resolution has been started.</td>
</tr>
<tr>
<td>Resolved</td>
<td>The issue has been resolved.</td>
</tr>
<tr>
<td>Closed</td>
<td>The issue has been closed. This can be used whether or not the issue has been resolved.</td>
</tr>
</tbody>
</table>

**Acknowledge**
Select the receipt status(es).
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledge</td>
<td>Alert received by owner.</td>
</tr>
<tr>
<td>Unacknowledge</td>
<td>Alert not received by owner.</td>
</tr>
</tbody>
</table>

### Category
Select the element(s) affected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy specific.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Scripts, Shared Objects, Tenants, and Files.</td>
</tr>
<tr>
<td>License</td>
<td>Device license status.</td>
</tr>
<tr>
<td>Operational</td>
<td>Alerts related to the function of a device or Management Center.</td>
</tr>
<tr>
<td>System</td>
<td>Networks linked to Management Center, including files, software, hardware, and firmware.</td>
</tr>
<tr>
<td>Security</td>
<td>Security related alerts.</td>
</tr>
<tr>
<td>Other</td>
<td>For an issue not listed in any other category.</td>
</tr>
</tbody>
</table>

### Priority
Select the importance level of resolution.

<table>
<thead>
<tr>
<th>Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Urgent</td>
</tr>
</tbody>
</table>

### Owner
Select the current owner.

Alerts that are **not assigned** (in the **Owner** sorting column) will not show up if an owner is selected.

### Keyword Search
Next to the Preview/Filter pane is the keyword searching option. If you know keywords in the alerts you are looking for, enter them into the search box and click the magnifying glass or press Enter. To clear the search terms, click the (×) within the search box.

**Navigation**

Navigate between pages and set navigation options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginning</td>
<td>&lt;&lt;</td>
<td>Go to the first page.</td>
</tr>
<tr>
<td>Back</td>
<td></td>
<td>Go back a page.</td>
</tr>
<tr>
<td>Page Number</td>
<td>Page 1 of 1</td>
<td>Current page number and total page count. Type a number to go to a specific page.</td>
</tr>
<tr>
<td>Forward</td>
<td></td>
<td>Go forward a page.</td>
</tr>
<tr>
<td>End</td>
<td></td>
<td>Go to the last page.</td>
</tr>
<tr>
<td>Refresh</td>
<td></td>
<td>Refresh the list.</td>
</tr>
<tr>
<td>Page Size</td>
<td>Page Size 50</td>
<td>Number of alerts displayed per page.</td>
</tr>
</tbody>
</table>

**Alert Management**

Create, edit, delete, or acknowledge receipt of alert(s).

**Creating New Alerts**

Use Raise Alert to create a new alert.
Raise Alert

Message*
Enter in the message for the alert. *This field is required.

Severity
The impact level on the affected category. *Indicates default

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Severity Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info*</td>
<td>📦️</td>
<td>Low</td>
<td>Little or no impact.</td>
</tr>
<tr>
<td>Warning</td>
<td>🚨</td>
<td>Medium</td>
<td>Potential to cause errors.</td>
</tr>
</tbody>
</table>
Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Severity Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>🚨</td>
<td>High</td>
<td>Errors found.</td>
</tr>
<tr>
<td>Fatal</td>
<td>🆘</td>
<td>Critical</td>
<td>System failure.</td>
</tr>
</tbody>
</table>

**Priority**
The importance level of resolving the alert. *Indicates default

<table>
<thead>
<tr>
<th>Priority Level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Low*</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Urgent</td>
<td></td>
</tr>
</tbody>
</table>

**State**
The current status of the alert. Alerts are either considered open or closed. *Indicates default

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>New or unworked issues.</td>
<td>Open</td>
</tr>
<tr>
<td>Pending</td>
<td>Already known issue, but resolution hasn't started.</td>
<td>Open</td>
</tr>
<tr>
<td>Assigned*</td>
<td>Assigned to a specific user.</td>
<td>Open</td>
</tr>
<tr>
<td>In Progress</td>
<td>A resolution has been started.</td>
<td>Open</td>
</tr>
<tr>
<td>Resolved</td>
<td>The issue has been resolved.</td>
<td>Closed</td>
</tr>
<tr>
<td>Closed</td>
<td>The issue has been closed. This can be used whether or not the issue has been resolved.</td>
<td>Closed</td>
</tr>
</tbody>
</table>

**Owner**
The administrator currently logged in is set as the default owner. You may assign it to a different owner as long as the person has previously been added as a user. See "Add Local Users" on page 357.

Alerts created by the system will show as **not assigned** in the **Owner** sorting column.

**Category**
The element affected by the alert. *Indicates default
### Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Option</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy specific.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Scripts, Shared Objects, Tenants, and Files.</td>
</tr>
<tr>
<td>Operational</td>
<td>Alerts related to the operation of a device or Management Center.</td>
</tr>
<tr>
<td>System</td>
<td>Networks linked to Management Center, including files, software, hardware, and firmware.</td>
</tr>
<tr>
<td>Security</td>
<td>Security related alerts.</td>
</tr>
<tr>
<td>Other*</td>
<td>For an issue not listed in any other category.</td>
</tr>
</tbody>
</table>

**Description**

(Optional) Enter a more detailed description of the alert and/or the reasons for it.

*If you forget any information for the detailed description, you can always Edit it or add note to the Journal tab at a later time.*

**Save/Cancel**

Save or Cancel the new alert.

**Editing Alerts**

You can edit the alerts using one of two methods:

- To edit all the information for an alert, select a message and then click Edit. Alternately, right-click a message to get the Edit option.

  **Only one message can be selected for editing at a time.**

**Edit Details Tab**

The basic information, normally set in Raise Alert, can be edited in the Details tab. A summary of the current saved status of the alert shows in a box below the editable details. The action buttons include:

- **Save Alert** for any changes you make.
- **Acknowledge** or **Unacknowledge** the receipt of the message.
- **Discard** any changes.
- **Take Ownership** to instantly assign it to yourself.
Journal Tab
A history of the changes made to the alert are logged in the **Journal** tab beneath the **Notes** field. Actions you can take include:

- Add more information in the **Notes** field.
- **Add Note** to the alert.
- **Clear** any information typed.

---

**Back**

Return to the list of alerts. Alternately, you can click on the **Alerts** link above the **Back** button to return to the list.

- Select message(s) to access the available quick **Operations**. These allow you to edit information on an alert without having to open the **Edit** screen.

---

**Assign Users**

Select a user to have ownership. You may assign it to a different owner as long as the person has previously been added as a user. See "Add Local Users" on page 357.

---

**Take Ownership**

Instantly assigns the alert to yourself.

---

**Change State**

The current status. Alerts are either considered open or closed.

*Indicates default*
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
<th><strong>Status</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>New or unworked issues.</td>
<td>Open</td>
</tr>
<tr>
<td>Pending</td>
<td>Already known issue, but resolution hasn't started.</td>
<td>Open</td>
</tr>
<tr>
<td>Assigned*</td>
<td>Assigned to a specific user.</td>
<td>Open</td>
</tr>
<tr>
<td>In Progress</td>
<td>A resolution has been started.</td>
<td>Open</td>
</tr>
<tr>
<td>Resolved</td>
<td>The issue has been resolved.</td>
<td>Closed</td>
</tr>
<tr>
<td>Closed</td>
<td>The issue has been closed. This can be used whether or not the issue has been resolved.</td>
<td>Closed</td>
</tr>
</tbody>
</table>

**Change Priority**

The importance level of resolution. *Indicates default*

<table>
<thead>
<tr>
<th><strong>Priority Level</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Low*</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Urgent</td>
</tr>
</tbody>
</table>

**Other Alert Management Options**

- Select message(s) to **Delete** them. Alternately, right-click the message(s) to get the **Delete** option.
- Messages are automatically removed by the system after a set time. The default is 120 days. See "Configure Housekeeping Settings" on page 564 for more information.

To change the amount of days alerts are retained:

1. Select **Administration > Settings > Housekeeping**.
2. Change the value in **Number of days of closed alert records to keep**.
3. Click **Save**.
4. (Optional) Click **Activate** to push your changes to the server immediately.

- Select message(s) to **Acknowledge** or **Unacknowledge** the receipt of them. Alternately, right-click the message(s) to get the acknowledgment options.

Only messages of the same receipt status can be selected at the same time for the button to work.

Example: Under the **Acknowledged** column, all messages marked **not yet**.

- **Refresh** the list of available alerts.
Back Up Device Configurations

Management Center allows you to initiate and automate the configuration backup of supported devices. You can select one or more devices or device groups to back up immediately or schedule a job for the backup.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. From the Network tab, select the supported devices or device groups to back up.
2. From the Operations drop-down list, select Backup Devices. The devices that you selected appear in the Selected list.
3. Click Next. The system displays the Backup Devices: Image Settings screen.
4. Enter the Backup Name and Backup Description. Optionally, you can use variables, as shown in the following graphic. (See “Use Device Information for Backup Job Image Metadata” on page 93.)
5. To include private key data in the backup, select **Include Private Data**.
   
   Currently, only the ProxySG and SSL Visibility appliances support this feature; the option is ignored for other device backups. For the ProxySG appliance, key rings can only be backed up if they were configured to show (Show key pair option) when created. Keys that were not configured to show are not included in backups, even if **Include Private Data** is selected.

   **Note:** Completed backups that include private key data include **pki** in the content details. ProxySG example:
   
   ```
   full-pki
   full
   ```

6. To secure the backup with the data protection key, select **Encrypt Backup**. Encrypted backups are only decrypted when the information is sent to the device. When you view the encrypted backup using the preview tab, only the encrypted data shows.

   **Caution:** Changing the Encryption Key may make any backups unrecoverable. See **Encrypt Sensitive System Data** for more information.

7. Do one of the following:
   
   - To immediately begin the backup of the selected devices, select **Run Now**.
To execute the backup of the selected devices at a later time, select Create Job...

a. In the New Job: Basic Info dialog, enter a unique name and click Next.

b. Use the default name or enter a new one. Click Next.

c. Verify that the private key options are correct. Click Next.

d. Verify that the devices you selected appear in the Devices tab. Click Next.

e. Define when you want to schedule the device backup to occur. See "Job Scheduling Options" on page 436 for descriptions of each option.

f. Click Finish.

Next Steps

<table>
<thead>
<tr>
<th>Task</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the configuration backups for a device and view the content of a backup file</td>
<td>&quot;View Device Backups&quot; on page 95</td>
</tr>
<tr>
<td>Restore a device configuration</td>
<td>&quot;Restore Device Backups&quot; on page 100</td>
</tr>
<tr>
<td>Export a device backup</td>
<td>&quot;Export Device Backups&quot; on page 98</td>
</tr>
<tr>
<td>Import a device backup</td>
<td>Import Device Backups</td>
</tr>
</tbody>
</table>

Regularly Back Up a Group of Devices

To be able to restore or roll back a configuration in case it gets corrupted, you need to back up your configurations on a regular basis. In this example, we will back up a device group on a weekly basis, during a time when the network is less
busy (such as a weekend).

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Create a device group for the devices you want to back up on a schedule. See “Add a Device Group” on page 56.

2. Create a **Backup Devices** job. Select the device group you created in step 1, and schedule the job to run on a **Periodic** basis, every 7 days starting on a weekend day. See "Back Up Device Configurations" on page 89.

3. Verify the backups are being created for each device in the group. See "View Device Backups" on page 95.

4. Restore a backup when necessary. See "Restore Device Backups" on page 100.
Use Device Information for Backup Job Image Metadata

Administrators can control the name and description of the backup created by a job (based on the specific device that is backed up). To use the device information in a backup job, administrators need to start a backup job from the **Network** tab rather than the **Jobs** tab.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Select a device from the **Network** tab.
2. From the **Operations** drop-down list, select **Backup Devices**. Select the device(s) to back up. An asterisk denotes fields that are mandatory.
3. Click **Next**. The web console displays Backup Devices: Image Settings dialog 'Manual Backup (04/04/15)' in the Backup Name field.

4. Click **Run Now**. The Job Progress dialog displays the backup while it runs. You can select **Continue in Background** or click **Close** when the backup **Status** is Complete. View all backups performed from the **Backup**
Management Center Configuration & Management tab of the device.
View Device Backups

For any device whose configuration you have backed up, you can view a list of backup files as well as view the content of the backup files. Once the list is displayed, you can delete or restore the backups.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Click the Network tab.
2. Select a device group in the left pane, and then select the device name in the right pane.

To configure the maximum number of backups stored per device, see "Set the Number of Backup Slots" on page 523.

3. Select the Backup tab displayed at the bottom of the screen. The web console displays all of the successful backups, including each backup’s name, description, date/time of the backup, device type, OS version, date/time it was last exported, and date/time it was last restored.
4. Select a backup from the list.
5. Click View. The Manual Backup Viewer displays the backup in a text editor.
6. If the backup exceeds the text editor limit, a warning displays:

Click Download. The file will download to your local Downloads folder. When the file is finished downloading, you can open it in Notepad or other text editor.

7. To pin or unpin a backup, click in the Pinned column. A checked box appears on pinned backups. A pinned backup cannot be manually deleted or automatically pruned (replaced with another backup).
8. To delete an unpinned backup, select it and click Delete.
9. To apply a particular backup configuration to the device, select it and click Restore. See "Restore Device Backups" on page 100 for more information.
Management Center Configuration & Management

Restore Device Backups

When you restore a device backup, Management Center replaces the device's current configuration with the backed up configuration. You can restore a configuration immediately, or schedule the restore for a late date.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Select the **Network** tab.
2. Select a device group in the left pane, and then select the device in the right pane.
3. Select the **Backup** tab at the bottom of your screen.
4. In the list of backups, choose the backup version you want to restore.

   If the backup you want to restore isn't listed, it's possible that it was exported and pruned from the appliance. In this case, you would need to import the backup before you can restore. See Import Device Backups.

5. Click **Restore** The web console displays the Restore Configuration dialog that displays the following information:
   - **Device** - The device name
   - **Backup Image** - The name of the backup
   - **Description** - The description given at the time that the backup was made
   - **Created** - The date and time of the backup
   - **Last Restored** - The date and time that the backup was last restored

6. (Optional) To view the contents of the backup (configuration), click **View Contents**.

7. To restore the backup later, go to **Step 9**.

   To restore the configuration immediately, click **Restore**. The web console displays the Job Progress dialog. The **Status** column displays the running/completed job and more details about the job.
8. (Optional) To view the device output from the restored backup:
   a. Select **more details**. The Device Output dialog displays the number and type of warnings.
   b. You can navigate in between the errors and warnings.
   c. Select **Download as Text** or **Close**.
9. To restore the backup later, click **Create Job** and follow the steps to configure the job. See “Add a Job” on page 430 for job options.
**Export Device Backups**

The Export Backup operation allows you to copy or move configuration backups to an external server. Copying backups to another server provides extra insurance by essentially creating a backup of a backup. Or, if you move the backups off Management Center and put them on an external server, you can make room for more backups on the Management Center appliance.

---

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

---

1. From the **Network** tab, select a device or a device group whose configuration backup you want to export.
2. From the **Operations** drop-down list, click **Export backups**. If you have configured a location for the backup already, Management Center immediately exports the backup to the configured location. However, if you have not configured a location for the backup, the New Job wizard begins, displaying the New Job: Basic Info dialog.
3. Enter a unique name and a description for the Export. Click **Next**.
4. The New Job wizard displays the **New Job: Operation** dialog. The **Operation** is already displayed as **Export Backups**.

   - **Operation**(*) - Export Backups
   - **Export to Server**(*) - Enter the server location using FTP, HTTP, HTTPS, or SCP
   - **Username** - Enter the server username.
   - **Password** - Enter the password for this user.
   - **Prune Backups** - Select this option to remove the backups from the backup slots after exporting the backups. You are essentially *moving* the backups if you select this option. If you leave this option cleared, you are *copying* the backups to an external server.
   - **Retention Count**(*) - Enter the number of backups to keep for each device. This overrides the default number of backup slots configured per device. (See "Set the Number of Backup Slots" on page 523.)


- **Prune Pinned** - Select this option to remove backups, even if they have been pinned (locked). Click **Next**.

5. In the **New Job: Targets** dialog, select additional devices or groups whose configurations you want to export. Selected devices and groups display in **Selected** pane. Click **Next**.

6. Define when you want to schedule the export to occur or select **Run Now** to export the configurations immediately. See “Job Scheduling Options” on page 436.

7. Click **Finish**.
Restore Device Backups

When you restore a device backup, Management Center replaces the device's current configuration with the backed up configuration. You can restore a configuration immediately, or schedule the restore for a late date.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Select the **Network** tab.
2. Select a device group in the left pane, and then select the device in the right pane.
3. Select the **Backup** tab at the bottom of your screen.
4. In the list of backups, choose the backup version you want to restore.

If the backup you want to restore isn't listed, it's possible that it was exported and pruned from the appliance. In this case, you would need to import the backup before you can restore. See Import Device Backups.

5. Click **Restore** The web console displays the Restore Configuration dialog that displays the following information:
   - **Device** - The device name
   - **Backup Image** - The name of the backup
   - **Description** - The description given at the time that the backup was made
   - **Created** - The date and time of the backup
   - **Last Restored** - The date and time that the backup was last restored
6. (Optional) To view the contents of the backup (configuration), click **View Contents**.
7. To restore the backup later, go to **Step 9**.

To restore the configuration immediately, click **Restore**. The web console displays the Job Progress dialog. The **Status** column displays the running/completed job and more details about the job.
8. (Optional) To view the device output from the restored backup:
   a. Select more details. The Device Output dialog displays the number and type of warnings.
   b. You can navigate in between the errors and warnings.
   c. Select Download as Text or Close.
9. To restore the backup later, click Create Job and follow the steps to configure the job. See “Add a Job” on page 430 for job options.

Set the Number of Backup Slots

By default, Management Center stores up to five backups per device, with each backup placed in a slot. After five backups, Management Center prunes (deletes) an unpinned backup to make room for the new backup. (Backups that are pinned are preserved and cannot be manually deleted or automatically pruned.) If you want Management Center to store more or fewer backups per device, you can adjust the number of backup slots.

1. Click the Administration tab and select Settings.
2. Select General on the left.
3. In the Number of backup slots enter a new value.
4. Click Save.

You can override the default number of backups that are retained for a device by entering a Retention Count when exporting backups. See “Export Device Backups” on page 98.

SSL Visibility Appliance - What is Backed up and Synchronized?

This page describes the SSL Visibility appliance configuration items that are backed up or synchronized.
Policy

- FIPS configuration and version
- Policy versions
- System options
- Rulesets
- Lists (IP address, cipher suites, certificates, etc.)

PKI

- FIPS configuration and version
- RSA and ECDH data
- Certificate authority data
- Trusted and known certificate data
- HSM data

Users

- Usernames
- Passwords
- Roles
- User IDs
- FIPS configuration and version

Platform

- Version information
- FIPS configuration and version
- Network settings
- NTP settings
- Remote logging settings
- SNMP settings
- Login banner settings

Alerts

- Mail configuration and roles
- FIPS configuration and version

Remote authentication

- TACACS settings
Monitor Device Health and Statistics

Devices can be activated or deactivated. Management Center actively monitors the health status of activated devices. Deactivated devices are not monitored. Whether you choose to activate or deactivate a device depends on your business requirements. For example, you might have already set up a pre-deployed device that is now ready to be activated, or want to deactivate a device that must be taken offline for maintenance.

Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. See Statistics Monitoring Over HTTPS for more information.

Any of the Change Monitoring Status actions can be saved to a job and scheduled. See "Add a Job" on page 430 for more information.

Change Health Monitoring Status

Deactivating a device is NOT the same as deleting a device. See "Stop Managing a Device" on page 108.

1. Select the Network tab.
2. Locate the device you want to activate or deactivate. See "Filter Devices or Device Groups in a Permission" on page 393.
3. Select the device or group, and click the Operations drop-down list.
4. Select Change Monitoring Status...
5. Select one or more devices and click Next.
6. Verify that **Change Health Monitoring state** is selected and do one of the following:
   a. To activate a deactivated device, select **Activate Device**.

   b. To deactivate an activated device, select **Deactivate Device**.

   **Deactivating a device disables all statistics monitoring.**

   If you try to activate the device when the connection parameters are not specified, you receive an error. To specify connections parameters, see "Edit a Device" on page 66.

7. Click **Run Now**. The system displays the Activate Devices - Job Results window.
Enable or Disable Statistics Monitoring

Use these options to enable or disable statistics monitoring. You can disable statistics monitoring without deactivating the device. However, Management Center can only collect statistics from activated devices.

1. Select the **Network** tab.
2. Locate the device you want to activate or deactivate. See "Filter Devices or Device Groups in a Permission" on page 393.
3. Select the device, and click the **Operations** drop-down list.
4. Select **Change Monitoring Status...**
5. Select one or more devices and click **Next**.

   The system displays the Change Monitoring Status: Operation States dialog.

6. Verify that **Change Statistics Monitoring state** is selected and do one of the following:
   a. To enable statistics monitoring, select **Enable Statistics Monitoring collections**.
      
      You can only enable statistics monitoring for activated devices.
   b. To disable statistics monitoring, select **Disable Statistics Monitoring collections**.

7. Click **Run Now**. The system displays the Activate Devices - Job Results window.
The device status can take up to 30 seconds to change.

<table>
<thead>
<tr>
<th>Target</th>
<th>Duration</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP-V50</td>
<td>0.2 seconds</td>
<td>Complete</td>
<td></td>
</tr>
</tbody>
</table>

Activate Devices - Job Results 100%
Filter by: Complete: 1, Error: 0, Running: 0

Close
Stop Managing a Device

To stop managing a device in Management Center, you delete it. You should only delete a device from your network if you are certain that you will not need to manage and it in the future.

When you delete a device, you remove it permanently from Management Center, and the only way to restore it is to add it again. If you want to stop monitoring a device temporarily, deactivate it instead of deleting it.

1. Click the **Network** tab.
2. Locate the device you want to delete. See “Search for Managed Devices” on page 116.
3. (Recommended) Verify that the device is the one you want to delete. See "Verify Device Details" on page 119.
4. Select the device, and then click **Delete**. The device and all related information, including reports is permanently removed from the system.

**Deletion cannot be undone. Once removed from the network, the device needs to be registered again.**

5. Confirm that the device was deleted. Deleting a device configuration can take up to 60 seconds to complete.
About Pre-Deployed and Deactivated Devices

You can manage devices in Management Center even if you do not have the ability to monitor their activity and statistics. These devices have an Inactive status in the system; when you select them, the System Metrics and Health Checks tabs at the bottom of the screen display no data.

To look for inactive devices in the system, click the Network tab and clear all the statuses beside Filter by except Inactive:

![Filter by: Error, Warning, OK, Inactive]

The Network tab displays only the Inactive devices.

Inactive devices consist of two types: pre-deployed devices and deactivated devices. The following are examples of why you might need to manage inactive devices:

- You add a device that has not arrived in your organization yet or is not set up. In this scenario, in the Add Device wizard, you select Unavailable (pre-deployment) for the deployment status. Connection parameters are not required when you select the pre-deployment status, so you must specify them before you activate the device later.

- To allow for scheduled maintenance or other scenarios where devices must be powered off. In this scenario, to prevent error alert messages, you could deactivate the affected devices by selecting them and clicking Deactivate. Then, reactivate the devices when maintenance is complete.

For more information about device status and the use of color in the web console, see "About Color-Coded Status Indicators" on page 34.

Restart a Device

If you need to reboot a managed device, you can restart it from Management Center’s web console.

1. Select the Network tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. From the Operations drop-down list, click Restart.
4. Click OK to confirm the reboot.
Synchronize Devices

Management Center supports synchronization of the following device types: SSL Visibility, Content Analysis, and Malware Analysis.

When devices have similar or exact configurations, you can copy the configuration of one device (the source) to one or more similar devices running the same or later OS versions. As an example, you can’t synch from a non-FIPS image to a FIPS image.

Prerequisites

- Determine which device has the configuration settings you want to synchronize to other devices. This device will be your source device.
- Under **Devices** on the **Network** tab, identify the target devices and verify that their OS version is the same or later than the source device. The OS version is displayed in the device’s Overview tab. See “View System Metrics” on page 121.

Device Sync Details

Different settings may be synched for each device.

Support for SSL Visibility Appliance

Important Notes

- Management Center does not allow synchronization from a newer version of an operating system to an older version. For example, you cannot synchronize a 3.8.3 operating system version to a 3.8.2 operating system.
- SSL Visibility 4.x (and later) appliances synchronize Policy and PKI only.
- SSL Visibility appliances do not report platform information in the device overview. Platform is displayed as N/A as shown in the example.

What to Synchronize

You can synchronize the following:

- **Alerts** - alerting and notifications used on the device
- **Users** - names and passwords on the device
- **PKI** - certificate (or the database store)
- **Policy** - rules for decrypting traffic
- **Remote authentication** - controls the way the device authenticates, as for TACACS

Advanced Synchronization Options

SSLV 3.x now supports the following synchronization options for certificate resigning. These options are not supported in SSL Visibility 4.x:
- **Retain default resigning keys**
  When you enable this option, the resigning certificate (EC or RSA) identified as default on a ruleset option for EC or RSA will not be changed on the target device. Selecting this option allows you to use different default resigning certificates on different target devices. When using this option, Symantec recommends that you set individual rules to use “default” such that the certificate used by the rule will be the same as that specified in the ruleset options.

- **Retain rule resigning keys**
  When you enable this option, the resigning certificate (EC or RSA) specified on a rule will not be changed on the target device. Selecting this option allows you to use different resigning certificates on different target devices.

- **Retain segment definitions**
  When you enable this option, the segment definitions of the target device will not be changed. This option should only be used in rare circumstances when you want to synchronize policy but want different segment definitions. This option is only supported in SSLV 3.12.3.1 and later.

**Support for Content Analysis**

Management Center does not allow synchronization from a newer version of an operating system to an older version.

What to Synchronize:

- Select **Configuration**. Not all elements of your Content Analysis appliance configuration can be saved/restored. Administration details and network information defined in the initial deployment of your appliance must be manually assigned. The following components are included:
  - Global Anti-Virus Policy
  - Kaspersky Policy
  - Sophos Policy
  - Alert Settings
  - Alert Templates
  - SMTP Settings
  - Consent Banner
  - Custom Logo
  - NTP Settings
  - Timezone Configuration
  - HTTP Settings
  - SNMP Settings
  - Sandboxing Settings
  - Static Analysis Settings

**Support for Malware Analysis Appliance (MA)**

Management Center does not allow synchronization from a newer version of an operating system to an older version.

What to Synchronize:
Settings - All settings within these groups are synced:

- File reputation (enabled/disabled)
- Cleanup daemon
- Proxy Server
- YARA state (enabled/disabled)
- Virus Total key
- Task Defaults
- Updates (enabled/disabled)
- WebPulse

Pattern groups created by users.

Note: Patterns and pattern groups are only synchronized when they are not marked in the Malware Analysis configuration as Global. See the topic, “Identify Malware Patterns” in your Malware Analysis or Content Analysis 2.x configuration guide for more details.

Perform Device Synchronization

Follow this basic procedure.

1. Click the Jobs tab.
2. Select New Job. The web console runs the New Job wizard. An asterisk denotes fields that are mandatory.
3. Enter a Name(*) and Description.
4. Click Next.
5. From the Operation(*) drop-down list, select Synchronize Devices.
6. Select a Source Device(*) from the list of available devices. After selecting a source device, click OK.
7. Select the check boxes to define What to synchronize(*). Available choices are specific to the device and are not platform specific.
8. Click Next. Select target devices or device groups that you want to keep in sync with the source device. If you select a device group that includes devices that are not supported, the synchronization job automatically filters out any devices that are not the correct device type.
9. Click Next. Define a schedule to run the Synchronize Devices job. See "Job Scheduling Options" on page 436.
Configure Hierarchy for Devices and Device Groups

The Hierarchy is the highest level in the device structure in Management Center. Any hierarchies that you create are at the same level as the predefined Location and Organization hierarchies. Because you can manage 500 devices, creating hierarchies is critical in managing device health, status, deploying policy and handling large jobs.

The Hierarchical structure of Management Center enables users to manage policy across a large number of data centers in a way that users can segregate the administration of policy.

Hierarchical Configurations

Management Center organizes its many managed devices into hierarchies with parent and child configurations. The key to understanding Management Center hierarchical configurations is to remember the basic rules of managing device groups, devices, and managing policies that can be deployed to all the devices in your organization.

Using the hierarchical structure, multiple devices can merge their policy attributes, devices can inherit policy attributes from a parent device group, or child devices can be directly assigned policy.

Device Groups can belong to other Device Groups, but cannot belong to multiple Hierarchies (for example, you cannot have the same Device Group in both Location and Organization).

Create hierarchies to represent geographical regions, organizational or departmental structure, deployment type, or anything else appropriate for your network. You can then add device groups to as many hierarchies as needed.

1. Click the Network tab. In the left pane, to the right of the Group By drop-down list box, click the Manage Hierarchies icon 🌟.
2. Click **Add Hierarchy**. In the **Hierarchy Name** field, enter a unique name.
3. In the **Comments** field, enter useful comments to differentiate this hierarchy from others. Fields marked with a red asterisk (*) are required settings.
4. The name you entered in step 2 automatically populates the **Root Folder Name** field. Accept the name if you do not want to create a root folder within the hierarchy.
5. To create a new root folder, enter a name for it in the **Root Folder Name** field. Click **Save**.

The root folder is the parent folder for all subfolders. For example, in the Beach Names hierarchy, Beach Names is the parent folder for the subfolders (West Coast Beaches, East Coast Beaches and Gulf Coast Beaches).
Edit a Hierarchy

1. To edit a hierarchy, from Groups select a device group name, click Edit. The Edit Hierarchy dialog displays.

![Edit Hierarchy dialog]

2. Edit the name, comments, and root folder name as needed. Fields marked with a red asterisk (*) are required settings.
3. Click Save to save your hierarchy changes or click Cancel to return to the Manage Hierarchies dialog.

⚠️ You can delete any hierarchy except for the Location hierarchy.

Delete a Hierarchy

1. To delete a hierarchy, from Groups select a hierarchy, click Delete. A Delete Confirmation displays.
2. Confirm the deletion; click Delete.

⚠️ If you delete a hierarchy that contains devices, the devices are still members of any other hierarchies to which they belong. If you delete the last hierarchy to which a device belongs, you can click Unassigned Devices to see the device.

To add a device group to the Hierarchy, see "Add a Device Group" on page 56.
Management Center Configuration & Management

Search for Managed Devices

You can search for devices in your network using several methods.

Search by Name or IP Address

In most cases, searching by the name or IP address is the most efficient way to locate a device.

1. Click the **Network** tab.
2. In the search field at the top of the tab, enter one of the following:
   - Device name
   - String in the device name
   - IP address of the device
   - Octet or part of an octet in the device IP address
3. Press Enter or click the search icon (magnifying glass).

The system returns a list of all devices that match the search criteria in a **Search** window. Select a device to view it, or click the X in the top right corner of the window to close it.

Browse the Hierarchy

Select the **Network** tab and browse the hierarchy and folders for the device. This method is convenient if you know where the device is located in the folder structure, or if the folder structure is not too deep or complex.
Perform an Operation on a Managed Device

The status of a managed device can control which operations are allowed on a device. See "Monitor Device Health " on page 58.

Operations that are not available for the selected device or device group are grayed out in the Operations drop-down list.

1. Select the Network tab.
2. Select the device group in the left pane, and the device in the right pane.
3. Click Operations to display the drop-down list of options.
4. Select the desired option:
   - View Licenses
   - Launch Console
   - Restart
   - Delete
   - Change Monitoring Status
   - Backup Devices
   - Export Backups
   - Import Backups
   - Import from File (Add Multiple Devices)
   - RMA Device
   - Purge Stats Monitoring
   - Remove Unused Tenant Policy
Ensure Devices Belong to Device Groups

Symantec recommends that you periodically verify that all devices are assigned to groups. A device might become unassigned if no groups were selected when the device was added to Management Center, or if the groups to which the device was assigned were deleted. See "Edit a Device Group" on page 68.

Because unassigned devices do not display in any groups, users might not manage them or even be aware of them if they work only in device groups or only have access to specific device groups in their role filters.

A device group can be inside another device group, but a device group cannot be in multiple hierarchies.

1. Click the **Network** tab. From the left pane, click **Unassigned Devices**. Unassigned devices display in the right pane.

2. Select a device you want to assign to groups and click **Edit**. The web console displays a wizard with the following tabs:
   - Basic Info
   - Connection Parameters
   - Membership
   - Attributes
   - Policies

   An error message displays at the bottom, citing the reason why the device is not assigned to a device group.

3. Click **Membership**. Enter a location for the device.

4. Click **Save**. A message stating: [device name] was saved successfully.

5. (Optional) To assign by dragging and dropping the device to a device group, select the device and drag it into the device group into the tree on the left. Drop the device. Confirm the move. Click **OK**.
Verify Device Details

To verify a device’s information after you have added it, or to help identify a device, do the following:

1. Click the **Network** tab and select a device to view. Select the device whose details that you want to view.
2. At the bottom of the screen, click the up arrow 🔽. The monitor window expands from the bottom of the screen.
3. **Overview, System Metrics,** and **Health Checks** and **Backup** tabs display at the bottom of the expanded window.
4. Click Overview. The web console displays information about the system resources.
5. Inside the **Overview** tab, click **Launch Console** to launch the console of the device, or click **Refresh** to query the device for the latest values to display within these device tabs.

   After you upgrade or downgrade the device, use the **Refresh** button to display the latest values correctly. See "Upgrade/Downgrade System Images" on page 544.

6. To close the device monitor window, click the down arrow 🔽.

### Device Overview Tab

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Icon</td>
<td>The icon used to depict a certain device type, for example a ProxySG appliance is depicted by the <img src="proxysg.png" alt="icon" /> icon.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
</tbody>
</table>
| Last update    | The date and time of the last update starting with how long ago the last update began (in seconds).                                                                                                                                                                     
<p>| Example:       | &lt; 20 s ago                                                                                                                                                                                                                                                                  |
| 6/1/15 6:02 PM GMT-05:00 | The example shown is when &lt;6/1/15&gt; equals the date in short format, &lt;6:02 PM&gt; equals the time on a 12-hour clock and <a href="">GMT-05:00</a> equals the time zone &lt;Greenwich Mean Time minus 5 hours&gt; which at the time of this documentation equals Central Daylight Time. |
| System started | The date and time that the system started.                                                                                                                                                                                                                                         |
| Example:       | 5/26/15 11:42 AM GMT-05:00                                                                                                                                                                                                                                               |
|                | The example shown is when &lt;5/26/15&gt; equals the date in short format, &lt;11:42 AM&gt; equals the time on a 12-hour clock and <a href="">GMT-05:00</a> equals the time zone &lt;Greenwich Mean Time minus 5 hours&gt; which at the time of this documentation equals Central Daylight Time. |</p>
<table>
<thead>
<tr>
<th><strong>Value</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>The appliance model of the appliance.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>VA</td>
</tr>
<tr>
<td></td>
<td>The example shown is where &lt;VA&gt; equals a virtual appliance.</td>
</tr>
<tr>
<td>Platform</td>
<td>The Symantec platform information that the software is running on.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Symantec SGVA Series</td>
</tr>
<tr>
<td></td>
<td>The example shown is when Symantec &lt;SGVA&gt; Series equals ProxySG Virtual Appliance Series.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number assigned to the selected device.ian</td>
</tr>
<tr>
<td>Host</td>
<td>The host IP address of the selected device.ian</td>
</tr>
<tr>
<td>OS version</td>
<td>The version of the operating system, including the version number and edition.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>SGOS 6.5.5.410 SWG Edition</td>
</tr>
<tr>
<td></td>
<td>The example shown is when &lt;SGOS&gt; equals the ProxySG Operating System, &lt;6.5.5.410&gt; equals the version number and &lt;SWG&gt; equals Secure Web Gateway Edition.</td>
</tr>
<tr>
<td>Build</td>
<td>The build number of the software running on the selected device.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>150788 64-bit, gbd, optimized</td>
</tr>
<tr>
<td></td>
<td>The example shown is when &lt;150788&gt; equals the build number, &lt;64-bit&gt; equals the capacity at which bits can be processed and stored and &lt;optimized&gt; equals clock optimization for this particular build number.</td>
</tr>
</tbody>
</table>
View System Metrics

In Management Center, device metrics refer to key hardware components such as CPU usage, disk status, fan status, and motherboard temperature. Refer to these metrics to verify availability and performance of system resources.

1. Select the Network tab. Select a device to view metrics.
2. At the bottom of the screen, click the up arrow . The monitor window expands from the bottom of the screen.
3. The web console displays the Overview, System Metrics, and Device Health and Backup tabs.
4. (Optional) If the device is always in an error state (yellow or red) and you are unable to update the license or restore a good configuration, you may need to perform an RMA for the device. See "RMA a Device" on page 123.
5. Click System Metrics. The web console displays information about the system resources. If available, scroll down to see all of the metrics available for the selected device. To see device details in the overview tab, see Verify Device Details.

Management Center can collect metrics only from activated devices. If you select a deactivated or pre-deployment device, the Overview, System Metrics, Health Checks and Backup tabs display no information.

The System Metrics Tab

The Systems Metrics tab provides a snapshot glance of the disk status as well as the percentage that both the CPU and Memory are currently being used, and the threshold settings for both Warning and Critical. To configure warning and critical thresholds displayed in the System Metrics tab, see "Configure Hardware Monitor Settings" on page 532. An example of a ProxySG appliance is displayed in the table shown below.

<table>
<thead>
<tr>
<th>Metric Description</th>
<th>Status</th>
<th>Current Value</th>
<th>Warning Threshold</th>
<th>Critical Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Utilization</td>
<td>OK</td>
<td>3%</td>
<td>80%</td>
<td>95%</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>OK</td>
<td>25%</td>
<td>90%</td>
<td>95%</td>
</tr>
<tr>
<td>Disk 1 Status</td>
<td>OK</td>
<td>present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk 2 Status</td>
<td>OK</td>
<td>present</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Health Checks Tab

The Health Checks tab displays information based on the type of device that you have selected. An example of an SSL Visibility appliance is displayed in the table shown below. The top row displays General with the number of health checks that are routinely performed on the device. To see other places within the web console to view device health, see "Monitor Device Health" on page 58.

<table>
<thead>
<tr>
<th>Name</th>
<th>Info</th>
<th>State</th>
<th>UP/DOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>- General (4)</td>
<td></td>
<td>OK</td>
<td>Up</td>
</tr>
<tr>
<td>License</td>
<td></td>
<td>OK</td>
<td>Up</td>
</tr>
<tr>
<td>Load</td>
<td></td>
<td>OK</td>
<td>Up</td>
</tr>
</tbody>
</table>
The Backup Tab

The Backup tab displays all of the device backups for the selected device. The Backup tab also displays whether a device backup has been exported to an external server, and whether it has been restored. Perhaps most importantly, you can pin a backup to ensure that it doesn't get deleted when Management Center deletes old backups when performing routine disk maintenance. When importing a backup, Management Center will not replace pinned backups unless specified when you "Restore Device Backups" on page 100. You must select a backup from the list to View, Restore, or Delete a backup. See "Monitor Device Health " on page 58. An example of a ProxySG appliance backup information is displayed in the table shown below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Date/Time</th>
<th>Device Type</th>
<th>OS Version</th>
<th>Exported Date</th>
<th>Restored Date</th>
<th>Pinned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>SG in Dallas</td>
<td>7/3/15 8:05 PM GMT</td>
<td>ProxySG</td>
<td>SGOS 6.5.5.410</td>
<td>7/11/15 1:58 AM GMT</td>
<td>7/12/15 3:30 PM GMT</td>
<td>✗</td>
</tr>
<tr>
<td>Device Name</td>
<td>Joe's SG</td>
<td>5/3/15 8:01 PM GMT</td>
<td>ProxySG</td>
<td>SGOS 6.5.5.410</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Matt's SG</td>
<td>5/3/15 8:03 PM GMT</td>
<td>ProxySG</td>
<td>SGOS 6.5.5.410</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export device backups to an external server.</td>
<td>&quot;Export Device Backups&quot; on page 98</td>
</tr>
<tr>
<td>Verify device details in the Overview tab.</td>
<td>Verify Device Details</td>
</tr>
<tr>
<td>View device backup in a text editor.</td>
<td>&quot;Monitor Device Health &quot; on page 58</td>
</tr>
</tbody>
</table>
RMA a Device

If you need to return a device to Symantec using Return Merchandise Authorization (RMA), follow the procedure below to replace the defective device with the replacement device in Management Center. This procedure assumes you have initiated the RMA process with Symantec.

1. Record the serial number of the defective device. You will need this number when performing the RMA Device operation below.

2. (Optional) Deactivate the defective device. See "Monitor Device Health and Statistics" on page 103.

   Deactivated devices show on the Network tab with a gray status. If you don't deactivate the device, it will show on the Network tab with a red status.

3. Return the defective device to Symantec.
4. Install the replacement device in the network. If you assign it the same IP address and credentials, you do not need to add the device into Management Center; otherwise, you will need to "Add a Device" on page 447.
5. Go to the Network tab and select the replacement device.
6. From the Operations drop-down list, select RMA Device. An asterisk denotes fields that are mandatory.

   Management Center will attempt to connect to the device and retrieve its serial number. If it succeeds, it will display it next to Serial Number detected on device.

7. In the Provide previous Serial Number field, enter the serial number of the defective device.
8. (ProxySGs only) Decide whether you want to apply existing Statistics Monitoring data from the defective device and migrate it to the replacement device. Select the desired option:

- migrate Statistics Monitoring data
- ignore Statistics Monitoring data

9. Click Update Device.
10. From the Operations drop-down list, click Restart.
Put Device in Read-Only Mode

You might want to monitor some devices while also preventing configuration changes on them. Management Center displays a lock next to devices in read-only mode, as shown below.

All Devices

Read-only devices can be selected as targets for jobs, scripts, etc., but that job step will fail.

Allowed Operations for Read-Only Mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Allowed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Metadata</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit Attributes</td>
<td>Yes</td>
</tr>
<tr>
<td>RMA</td>
<td>Yes</td>
</tr>
<tr>
<td>Purge Stats Monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td>Import from file</td>
<td>Yes</td>
</tr>
<tr>
<td>Assign Group Membership</td>
<td>Yes</td>
</tr>
<tr>
<td>Use as a policy target</td>
<td>Yes</td>
</tr>
<tr>
<td>Install Policy</td>
<td>No</td>
</tr>
<tr>
<td>Remove unused policy</td>
<td>No</td>
</tr>
<tr>
<td>Execute script</td>
<td>No</td>
</tr>
<tr>
<td>Backup Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Export Backup</td>
<td>Yes</td>
</tr>
<tr>
<td>Restore Backup</td>
<td>No</td>
</tr>
<tr>
<td>Launch Console</td>
<td>Yes</td>
</tr>
<tr>
<td>Activate Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Deactivate Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Restart Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Device sync as a source</td>
<td>Yes</td>
</tr>
<tr>
<td>Device sync as a Target</td>
<td>No</td>
</tr>
</tbody>
</table>
Add a Device in Read-Only Mode

The Management Center system only allows existing devices to be set in read-only mode.

1. Select the **Network** tab.
2. Select **Add Device**.
3. Select the type of device.
4. Select the Existing device from the **Deployment status** menu.

![Device Management Modes](image)

**Devices added with the Deployment Status set to Unavailable (pre-deployment) cannot be set to Read Only.**

5. Set the **Edit mode** as **Read Only**.
6. Enter the connection details and follow the rest of the **Add a Device** process.
Put an Existing Device in Monitor-Only Mode

1. Select the **Network** tab.
2. Locate the device, select it, and click **Edit**.
3. In the **Edit mode** field, select **Read Only**.
4. Click **Save**.
Use WAF Policy To Protect Servers From Attacks

As more and more organizations move to web applications, they are exposed to new and sophisticated threats. While traditional firewalls and IPS systems are effective for detecting threats in layers 3 and 4, they cannot interpret the logic inside the application layer, making them ineffective against web application threats. Web Application Firewalls (WAF) were designed for just this purpose. WAF devices protect web applications by inspecting traffic and controlling access to applications.

As the following diagram shows, the ProxySG WAF appliance is typically deployed behind the firewall and in front of the back-end content servers. It is typically paired with the Malware Analysis and Content Analysis appliances, while Reporter and Management Center provide reporting and remote management services.

In Management Center 1.5.x and later, you can use Management Center to construct Web Application Firewall (WAF) policies for your ProxySG appliances. These WAF policies are designed to protect back-end web applications and servers in a reverse proxy deployment from external security threats. The ProxySG WAF solution provides the following:

- OWASP top 10 threats protection
- Content Nature Detection
- Virtual Patching
- Cookie signing
- Denial of Service (DoS) protection
- Whitelisting and blacklisting
- Advanced policies (CSP, HSTS, HPKP, etc.)
- Analytics filter (heuristics anomaly detection)
- GEO location intelligence
- Normalization
- Signature versions per application
- JSON / XML security

Requirements

To use the WAF features, you must purchase the following:
- Web Application Protection (WAP) Subscription (included with Management Center but must be purchased for your ProxySG appliances).

If you have purchased a subscription, it is automatically downloaded to Management Center. To manage your subscription, see #subscriptions in the Management Center Configuration WebGuide.

In Management Center 1.6.1.1, the subscriptions command controls only the Web Application Protection (WAP) subscription. To use Web Application Firewall (WAF) features, you must ensure that Management Center can connect to https://subscription.es.bluecoat.com to download the WAP subscription bundle. If the WAP subscription cannot be downloaded, the Blacklist and Analytics Filter rules table in the Security Profile will not be available. However, all other WAF features should still be available and functioning. The WAP subscription cannot currently be loaded when Management Center is in offline mode.

- Multi-Tenant Policy License.

These licenses are purchased on a per ProxySG appliance basis.

Software Version Requirements

- ProxySG appliance: Must run SGOS 6.6.3 or later.
- Reporter: Must run 10.1.3 or later, which provides the new WAF database.
- Management Center: Must run 1.5 or later, which provides the new WAF interface.

Recommended Reading

Before using these WAF features, Symantec strongly recommends reading and familiarizing yourself with the following ProxySG appliance documents:

- Web Application Firewall Solutions Guide
- Multi-Tenant Policy Deployment Guide

Solution Steps

1. Learn about WAF policy.
2. Select a tenant.

   Tenants are administrative entities defined on ProxySG appliances. Each tenant has a unique instance of policy governing its traffic. To begin, first deploy WAF policy to the default tenant. You can add additional tenants later if you require WAF application objects with different security profiles.

3. Create a Tenant Determination File.

   This object controls how requests are routed to the tenant slots in policy. A Tenant Determination File always references the default tenant. Optional tenant references and rules controlling their selection can be added as needed when additional tenant slots are created.

4. Deploy the Tenant Determination File to the appropriate ProxySG appliances.

5. Create and configure a WAF Security Profile.
Management Center Configuration & Management

A WAF Security Profile defines the security rules for the Web Application Firewall.

6. Create and configure a WAF application object, associating a tenant and WAF Security Profile.
   A WAF application object represents a web application (or group of Web applications) and its associated WAF security settings.

7. Add targets and deploy the WAF application object to those targets.

8. Run web application traffic through the WAF and review your logs for false positives.

| The bcreporterwarp_v1 access log format is recommended for reverse proxy WAF deployments. For more information, refer to the Web Application Firewall Solutions Guide. |

9. Refine your WAF Security Policy:
   a. Add exemptions to your WAF security policy.
   b. Change WAF protections controls from Monitor-mode to Block-mode.
   c. Optional—Configure Effective Date to intelligently handle subscription updates.

About WAF Policy

As described in "Use WAF Policy To Protect Servers From Attacks" on page 130, WAF policies are designed to protect backend web applications and servers in a reverse proxy deployment from external security threats.

The Management Center WAF policy feature uses the following policy elements:

Tenants. Management Center WAF policy is centered around the concept of tenants. Tenants are administrative entities defined on the ProxySG appliance that allow policy to be applied to a request matching specific properties or conditions. Tenants represent one or more web applications. Each WAF application object (see below) is associated with a tenant.

Tenant Determination File. A Tenant Determination file includes policy conditions that control which tenant policy slot is evaluated for an HTTP request. When policy matches a request, the tenant is identified and all policy associated with the tenant ID is applied to the request. For example, a tenant's rules could indicate that all traffic to port 80 must have this tenant's policy applied to it. After setting these rules on Management Center, you deploy this file to your ProxySG appliances.

WAF Security Profile. A WAF security profile is a shared object (a policy element that can be referenced by multiple policy objects) that defines the Web Application Firewall settings for the associated WAF application object. For its rules to be enforced, a WAF security profile must be associate with a WAF application object.

WAF Application Object. WAF policy is configured through the use of a WAF application object. A WAF application represents a tenant (a web application or group of web applications) and its associated WAF security profile settings. Therefore, to create a WAF application, you must associate it with a tenant (web application) and a WAF security profile (security settings).

About the Default Tenant

For new WAF deployments, you begin by associating a WAF application with the default tenant. The default tenant contains the policy rules applied to all requests that do not match a specific tenant. This ensures that all requests have a base level of WAF protection, and simplifies the deployment process.
After deploying policy to the default tenant, create additional tenants as needed. For example, you can define a tenant for your Salesforce application and another tenant for your SharePoint application. Then, you can create and apply specific policy to protect and control each of those tenants.

**About Tenant Determination**

The criteria that determines the correct tenant policy to apply to a request are called *tenant determination rules*. As shown below, tenant determination is controlled through the use of a `<tenant>` layer in the Landlord CPL slot on the ProxySG appliance.

On Management Center, you configure the Landlord slot by creating a [Tenant Determination File](#). In other words, the Landlord slot on the ProxySG appliance is referred to as a Tenant Determination File on Management Center.

The `<tenant>` layer in the Landlord slot specifies conditions and `tenant()` properties. Within this layer, a small subset of CPL conditions are supported. These conditions are used like a switch statement (conditional logic flow) to specify which tenant slot CPL should be evaluated for a given request. When the conditions on a line evaluate to true, the `tenant()` property is set and evaluation of the current layer ends.

After tenant determination, the request is routed through a tenant, whose policy is evaluated for that transaction. When no specific tenant is determined for a request, the default tenant policy is used. Tenant determination criteria governs which tenant's policy applies to a given request.

**Reference: Conditions and Examples**

**Supported Conditions**

The following table shows the tenant conditions supported in Management Center.
<table>
<thead>
<tr>
<th>Condition</th>
<th>Available Qualifiers</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Address</td>
<td>matches</td>
<td>Client Address matches 10.167.3.25</td>
</tr>
<tr>
<td>Client Effective</td>
<td>matches</td>
<td>Client Effective Address matches 10.167.0.87</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>matches</td>
<td>Proxy Address matches 10.140.2.104</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>=</td>
<td>Proxy Port = 8080</td>
</tr>
<tr>
<td>Port</td>
<td>=</td>
<td>Port = 80</td>
</tr>
<tr>
<td>URL</td>
<td>equals contains matches regex</td>
<td>URL equals <a href="http://www.example.com/test">http://www.example.com/test</a></td>
</tr>
<tr>
<td>URL Domain</td>
<td>contains</td>
<td>URL Domain contains example.com</td>
</tr>
<tr>
<td>URL Extension</td>
<td>equals is not present</td>
<td>URL Extension equals .net</td>
</tr>
<tr>
<td>URL Host</td>
<td>equals contains matches regex</td>
<td>URL Host equals <a href="http://www.example.com">http://www.example.com</a></td>
</tr>
<tr>
<td>URL Path</td>
<td>equals contains matches regex</td>
<td>URL Path equals /example</td>
</tr>
<tr>
<td>URL Query</td>
<td>equals contains matches regex</td>
<td>URL Query contains ?name=</td>
</tr>
</tbody>
</table>

### Tenant Determination CPL Example

The following CPL rules provide an example of tenant determination in the Landlord slot.

```xml
<tenant>
  url.path.substring="/Webapp/portal" tenant(webapp_portal)
  url="http://domain.com/mail" tenant(domain_mail)
  tenant(default)
</tenant>
```

In the preceding CPL, the condition on each line is evaluated. If the condition is a match, the `tenant()` property on that line is set appropriately and the evaluation of the `<tenant>` layer exits. If no tenant is determined, the `tenant(default)` is used.

---

The `tenant(default)` property is implicit and does not actually need to be included in the CPL rules. Always deploy WAF policy to the default tenant to ensure that all requests are processed by the WAF. Specific applications (or groups of applications) that require different WAF security settings can then be split off into unique tenants as required.

### WAF Policy Evaluation Example

The example below describes WAF policy evaluation:
Management Center Configuration & Management

1. The ProxySG appliance intercepts a request.
2. The appliance examines the initial connection parameters (source, destination, port, URL).
3. The appliance applies policy to the traffic.
4. The Landlord policy (Tenant Determination File) is examined.
5. The request is set to a specific tenant slot, or to the default tenant slot.
6. The appliance re-evaluates the request using a CPL stack that contains the appropriate tenant policy.
7. If allowed by policy, the ProxySG appliance sends the traffic to the appropriate server.

Manage Tenants

Tenants are administrative entities defined on ProxySG appliances. Each request is routed through a tenant, whose policy is evaluated for that transaction. When no specific tenant is determined for a request, the default tenant policy is used. Tenant determination criteria governs which tenant’s policy applies to a given request. Add these tenants to Management Center to create and deploy tenant-specific policy.

On the ProxySG appliance, there are two options for controlling tenancy determination:

1. The `#(config general) multi-tenant criterion` command specifies a substitution expression that is evaluated for tenancy determination.
2. Using the `<tenant>` layer in the Landlord CPL slot to specify conditions and tenant() properties.

The Management Center WAF interface leverages option #2 to control tenancy determination via the Tenant Determination object. See "About WAF Policy" on page 132 for more information.

When evaluating an HTTP request, if the tenant determination rules produce a match against an installed tenant, then that tenant’s policy will be evaluated. If that fails to set the tenant() property, or the tenant() property setting does not correspond to an installed tenant policy, then the default tenant policy is applied to this traffic. Default tenant policy applies to all requests where tenancy couldn’t be determined during the initial connection.

Obtain the tenant identifiers before you write multi-tenant policy in Management Center. For more information on multi-tenant policy, refer to the Multi-Tenant Policy Deployment Guide.

WAF Policy Use

Selecting a tenant is step 2 in "Use WAF Policy To Protect Servers From Attacks" on page 130. A base-level of WAF policy should be installed to the default tenant before any additional tenants are created. This ensures that all requests are processed by the WAF.

Add a Tenant

An asterisk denotes fields that are mandatory.
1. Select **Configuration > Tenants**.

2. Click **Add Tenant**.

The web console displays the **Add Tenant** dialog.
3. Enter a **Display Name**.
4. Enter the **Tenant ID**. This controls the name of the tenant slot where policy will be installed. This ID is also used in the tenant determination CPL using the **tenant()** property.
5. (Optional) Enter a **Description** (up to 1024 characters).
6. Click **Save**.

By default, the **Tenants** list is sorted in alphabetical order by Display Name. You can also sort by **Tenant ID** or **Description** by clicking the column headings. If the list is long, use the Keyword Search field to search for any string in the name, ID, or description. The search is case-sensitive.

**Modify a Tenant**

1. Select **Configuration > Tenants**.
2. From the Tenants list, select the tenant to modify and click **Edit**. The web console displays the **Edit Tenant** dialog.

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Tenant ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>default</td>
</tr>
<tr>
<td>Outlook_Lab3</td>
<td>OutLa3</td>
</tr>
<tr>
<td>Sharepoint</td>
<td>Sharepoint</td>
</tr>
<tr>
<td>WAF App</td>
<td>WAFApp</td>
</tr>
</tbody>
</table>

3. Edit the **Display Name** or **Description**. An asterisk denotes fields that are mandatory.
4. Click **Save**.

**Delete One or More Tenants**

1. Select **Configuration > Tenants**.
2. From the Tenants list, select one or more tenants to remove.
3. Click **Delete**.

4. Select **Yes** to delete the selected tenants.
You cannot delete the default tenant or any tenant that is currently referenced in Management Center policy. Attempting to delete the default or a referenced tenant results in a "Delete failed" error message.

Specify Tenant Determination Rules

A Tenant Determination file includes policy conditions that control which tenant policy slot is evaluated for an HTTP request. When policy matches a request, the tenant is identified and all policy associated with the tenant ID is applied to the request. On the ProxySG appliance, this file is called the "Landlord Policy." See "About WAF Policy" on page 132 for more information about the Landlord policy.

WAF Policy Use

Specifying Tenant Determination rules is step 3 in "Use WAF Policy To Protect Servers From Attacks" on page 130.

Step 1 – Create a Tenant Determination File

1. Select Configuration > Policy and click Add Policy.

The web console displays the Create New Policy: Basic Information wizard. An asterisk denotes fields that are mandatory.

2. Enter a name for the policy object.
3. Select Tenant Determination File for the Policy Type.
4. (Optional) In the **Reference Id** field, enter a Reference ID that you can filter on when building policy.

   - The Reference ID must begin with a letter, and must contain only letters, numbers and "_."

5. (Optional) Enter a description in the **Description** field. Although entering a description is optional, entering a description can help you understand the purpose of the policy when you later refer to it.
6. Click **Next**.
7. Enter or select values for the defined attributes.
8. Click **Finish**.

   The new tenant determination policy object appears in the Policy Objects editor. When installed on a ProxySG appliance, this tenant determination file configures the policy in the ProxySG Landlord slot. Because no other tenants have yet been defined, this policy object directs requests to the default tenant. (The default tenant contains the policy rules applied to all requests that do not match a specific tenant.) For initial setups, WAF policy should be installed to the default tenant. To proceed, deploy the tenant determination file to your ProxySG appliances and continue to "Configure WAF Security Rules " on page 141 to create a Security Profile.

9. (Optional) **Add Target Devices**.
10. (Optional) **Install Policy**.

**Step 2 — Optional: Add Tenant Determination Rules for Other Tenants**

Use this optional procedure to add additional tenants after deploying WAF policy to the default tenant. Only complete these steps if you require WAF application objects with different security profiles.

Tenant determination rules specify the properties used to identify a tenant. You specify these properties using a simple, natural language interface that generates equivalent CPL rules.

1. Select **Configuration > Policy**.
2. Click the policy name hyperlink or highlight the row and click **Edit**.

   **Policy Objects**

   ![Policy Objects](image)

   - Name: abc
   - Acceptable Use: A Landlord Policy

   The selected file displays in the **Editor** tab.

3. Click **Add Rule**.
The system displays the Add Rule dialog.

4. Click the **Tenant** field and select a tenant from the Select Tenant dialog.

The Select Tenants dialog displays existing tenants in Management Center. For more information, see "Manage Tenants" on page 282.

5. Click **OK** to exit the Select Tenant dialog.

6. In the **Determination Rules** field, use the natural language fields to create the tenant’s determination rules:
   
a. Select **All** or **Any** of the following rules.

   b. Select a rule condition, for example, **URL Extension**.

      The following conditions are available: **Client Address**, **Client Effective Address**, **Port**, **Proxy Address**, **Proxy Port**, **URL**, **URL Domain**, **URL Extension**, **URL Host**, **URL Path**, **URL Query**.

      Starting with ProxySG 6.7, the tenant rule conditions include redirect-based authentication controls within a tenant slot, `tenant.connection()`). This gives an early trigger for client gestures, such as **URL Port** and **Proxy Port**. The CPL generated includes conditional text to prevent ProxySG 6.6 or earlier from running the trigger. Also, the connection does not apply to the default tenant.

   c. Select an operator, for example, **equals**.

      The available operators may change based on the specified rule condition.

   d. Enter a value, for example, **.pdf**.

Address fields support IPv4 and IPv6 single and subnet addresses. For example:
7. Use the ‾ ‾ ‾ icons to add more rules.

   - To add another rule, click ‾‾.
   - To delete a rule, click ‾‾.
   - To add a nested set of rules, click ‾‾.

8. When you are finished making changes, click Save.

9. (Optional) Add Target Devices.

10. (Optional) Install Policy.

Tenant determination rules are enabled by default. To disable a rule, highlight the rule and click Disable.

Tenant Determination Rule Example

Configure WAF Security Rules

A WAF security profile is a shared object (a policy element that can be referenced by multiple policy objects) that defines the Web Application Firewall settings for the associated WAF application object. You associate the WAF security profile with a WAF application object to define the security rules for that object. You can create as many WAF security profiles as
you need but a WAF application object can be associated with only one security profile.

**WAF Policy Use**

Configuring a WAF security profile is step 5 in "Use WAF Policy To Protect Servers From Attacks" on page 130.

### Step 1 – Create a WAF Security Profile

1. Select **Configuration > Shared Objects > Add Object.**

   ![Image of Symantec Management Center interface](image)

   The web console displays the Create New Shared Object: Basic Information wizard. An asterisk denotes fields that are mandatory.

2. Enter a name for the policy object.
3. Select **WAF Security Profile** for the **Object Type**.
4. (Optional) In the **Reference ID** field, enter a Reference ID that you can filter on when building policy.
   
   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".
5. Enter a description in the **Description** field. Although entering a description is optional, entering a description can help you understand the purpose of the policy when you later refer to it.
6. Click **Next**.
7. Enter or select values for the defined attributes.
8. Click **Finish**.
   The new WAF security profile object appears in the Policy Objects editor.

**Step 2 – Configure WAF Security Rules**

1. Select **Configuration > Shared Objects**.
2. Click the WAF security profile hyperlink or highlight the row and click **Edit**.

   **Shared Policy Objects**

   ![Shared Policy Objects Table]

   The selected file displays in the **Editor** tab.
3. Review the following settings and adjust to create the desired security settings:

Refer to the Web Application Firewall Solutions Guide for information about these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Validation</td>
<td>Controls general HTTP request properties such as size restrictions, WAF validation properties, allowed methods, and allowed file types.</td>
</tr>
<tr>
<td>Request Normalization</td>
<td>Enables the recommended normalization settings for each request part, and what action to take when normalization issues are encountered. For advanced normalization control, refer to the Content Policy Language Reference.</td>
</tr>
<tr>
<td><strong>Blacklist</strong></td>
<td>Enables/disables the blacklist engine and sets block/monitor behavior when a request triggers one of the blacklist rules. The signature-based blacklist discovers well-known attack patterns quickly and efficiently.</td>
</tr>
<tr>
<td><strong>Analytics Filter</strong></td>
<td>Enables/disables the Analytics Filter engine and sets Analytics Filter block/monitor behavior. Analytics Filter is a scoring engine that detects attack characteristics and triggers intelligently based on the sum of the anomalies.</td>
</tr>
<tr>
<td><strong>Security Engines</strong></td>
<td>Specifies security engine settings (these are known as WAF engines in the ProxySG documentation). The content nature detection engines include HTML Injection, Command Injection, Code Injection, SQL Injection, XSS, and Directory Traversal.</td>
</tr>
<tr>
<td><strong>XML Validation</strong></td>
<td>These options ensure the XML is valid and check for potentially malicious constructs.</td>
</tr>
<tr>
<td><strong>Request Security</strong></td>
<td>These options ensure that requests are safe by checking for common attacks like HTML tag injection, buffer overflow, header injection, and request smuggling.</td>
</tr>
<tr>
<td><strong>Response Security</strong></td>
<td>These options make server responses more secure by obfuscating the back-end technology and directing browsers to implement additional client-side security.</td>
</tr>
<tr>
<td><strong>Optimizations</strong></td>
<td>Disable WAF controls for POST requests consisting of binary data; bypass WAF scanning for cache hits.</td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td>These options control the behavior that determines how the header and body of HTTP requests are logged to the x-bluecoat-request-details-header and x-bluecoat-request-details-body access log fields.</td>
</tr>
<tr>
<td><strong>Cross-Site Request Forgery</strong></td>
<td>Detects Cross-Site Request Forgery (CSRF) attacks. Once enabled, select the WAF event (block, monitor, or ignore), the expiry of the token, and the authentication link for User IDs and the Client IP.</td>
</tr>
<tr>
<td><strong>Exemptions</strong></td>
<td>Define exemptions to your WAF policy to handle false positives.</td>
</tr>
</tbody>
</table>

Many of the options include a Block/Monitor/Ignore setting. This setting indicates the action taken when suspicious content is identified. For new WAF deployments, Symantec recommends setting the action to Monitor.

4. *(Optional)* After making one or more changes, click **Compare** to review a side-by-side comparison of the changes.
5. Click **Save**.

To create exemptions to your WAF policy, set a security control to “Ignore,” or create an appropriate exemption definition, see “Manage WAF Security Policy” on page 152.

### Configure WAF Application Objects

A WAF application object represents a web application (or group of applications) and its associated WAF security settings. The WAF application object is associated with a specific tenant and WAF Security Policy. You install this policy on ProxySG appliances to configure WAF settings.

**WAF Policy Use**

Configuring a WAF application object is step 6 in “Use WAF Policy To Protect Servers From Attacks” on page 130.

**Create a WAF Application Object**
1. Select Configuration > Policy and click Add Policy.

The web console displays the Create New Policy: Basic Information wizard. An asterisk denotes fields that are mandatory.

2. Enter a name for the policy object.
3. Select WAF Application Object for the Policy Type.
4. (Optional) In the Reference Id field, enter a Reference ID that you can filter on when building policy.

   The Reference ID must begin with a letter, and must contain only letters, numbers and ".".

5. Click the Tenant field, select a tenant from the Select Tenant dialog or click Add to create a new one, and click OK. If this is a new WAF deployment, select the default tenant.

   A WAF application should first be deployed to the default tenant slot to ensure that all requests are processed by the WAF. Additional WAF applications, security profiles, and tenants can then be created to handle specific web application requirements.
6. Enter a description in the **Description** field. Although entering a description is optional, the description helps differentiate versions of the same policy.
7. Click **Next**.
8. Enter or select values for the defined attributes.
9. Click **Finish**.

The new WAF application object appears in the Policy Objects editor.

**Configure the WAF Application Object**

If you are not already editing the WAF application object, select **Configuration > Policy** and click the policy name hyperlink or highlight the row and click **Edit**. The selected file displays in the **Editor** tab.

**Step 1 - Confirm Tenant Selection**

Confirm your tenant selection. To select a different tenant, select the pencil icon. Show screen.

**Step 2 - Specify WAF Application Settings**

The WAF Application Settings panel enables you to set policy generation controls.
1. Select a WAF Security Profile:
   a. Click the **WAF Security Profile** text field or pencil icon.
   b. In the Select Policy dialog, select the desired WAF Security Profile or click **Add** to create a new one.
   c. Click **OK** to close the Select Policy dialog.
   d. Specify the WAF Security Profile version to use. Select **Always Use the Latest Version** or specify a specific version in the **Use Specific Version**: field.

2. (Optional) To override all WAF Security Profile settings, select **Disable entire Security Profile**.

3. (Optional) To globally change all Block/Monitor verdicts, select **Change all WAF controls to**: **Monitor** or **Block**.
   
   To set the behavior to **Ignore**, disable the entire WAF Security Profile.

4. Specify the user notification (exception) page to use for blocked requests.

**Step 3 - Set Compression**
Select Enable compression level (Low, Medium, High) to allow WAF to compress data in transit.

Step 4 - Specify Allow Rules

Set the criteria for allowing traffic through the ProxySG appliance. Specify these rules using rules associated with a tenant, a CPL fragment, or by manually entering them using the Custom Rules option. If you do not want allow rules or want to add your own in CPL, select No Allow Rules.

Because reverse proxy deployments have a global Deny policy, you must specify rules to allow traffic. If this WAF application is associated with the default tenant, you will receive an error (because the default tenant has no allow rules) and must specify the allow rules using one of the other methods.

Step 5 - Add CPL Fragments

Adding a CPL fragment is optional. Add valid CPL layers only. Do not add individual CPL rules. Adding individual rules can lead to errors and unpredictable results.
1. Click **Add CPL Fragment**. The web console displays the Add CPL Fragment dialog.

![Add CPL Fragment dialog](image)

- **CPL Fragment Name:**
- **Always use the latest version**
- **Use specific version:**

a. Click the CPL Fragment text field or pencil icon. The web console displays the Select Policy dialog.

![Select Policy dialog](image)

b. Select the CPL Fragment. See "Create a CPL Policy Fragment" on page 223 for information about creating CPL fragments.

c. Click **OK**.

d. Select **Always Use the Latest Version** or specify a specific version in the **Use Specific Version:** field.

If **Always use the latest version** is selected, Management Center will always include the latest available version of the Security Profile when installing the WAF application to a ProxySG appliance. If you are concerned about deploying untested changes, select **Use Specific Version**.

### Save Changes and Next Steps

To finalize your settings, you must review your policy and save your changes.

1. *(Optional)* After making one or more changes, click **Compare** to review a side-by-side comparison of the changes.
2. When you are finished making changes, click **Save**.
3. *(Optional)* **Add Target Devices**.
4. *(Optional)* **Install Policy**.

### Analyze and Refine WAF Policy (Mitigate False Positives)

After installing an initial version of WAF policy on one or more target devices, you can analyze the results of the traffic to determine what attacks have been detected. There is a chance that the detection engines have flagged a legitimate request as an attack. For example, if a blog post includes an example of a cross-site scripting (XSS) attack, the appliance interprets the example as an actual attack and blocks the post. This might be undesirable behavior and considered a false positive.
Address this and other kinds of false positives with the following workflow. Refer to the [Web Application Firewall Solutions Guide](#) for more information.

**WAF Policy Use**

Analyze and Refine WAF Policy describes steps 8 and 9 in "Use WAF Policy To Protect Servers From Attacks" on page 130.

### Analyze and Refine WAF Policy Workflow

<table>
<thead>
<tr>
<th>Step</th>
<th>Overview</th>
<th>References</th>
</tr>
</thead>
</table>
| 1    | Check access logs to determine which rules or engines you must update to address false positives, false negatives, and other wanted behavior. A useful search criteria is the transaction ID. For example, when a user tries to visit a page and receives an exception page, you can use the associated transaction ID to run a forensics report. The Full Log Detail report then displays the log line matching that transaction ID. | "View a Reporter Report" on page 453  
"Reference: Report Descriptions" on page 465  
"Search for Specific Report Data (Search and Forensic Report)" on page 485 |
| 2    | Optional-Perform a policy trace.                                           | "Launch a Device Console" on page 69  
To enable policy tracing on the ProxySG appliance, select **Configuration > Policy > Policy Options**. Under **Default Policy Tracing**, select **Trace all policy execution** and click **Apply**. |
| 3    | Based on your analysis of the access logs, create policy exemptions to eliminate false positives and other unwanted behavior. | "Manage WAF Security Policy" on the next page |
| 4    | Run traffic through the appliance and confirm through access logs (and optionally, other troubleshooting tasks) that requests match both general rules and exceptions appropriately. | Repeat steps 1 through 3 in this table as often as required. |

After confirming that false positives no longer occur, consider your next step. You can do any of the following according to your needs:

- Update policy actions from monitor to block. Then, move to a production environment when your WAF policy is stable and you observe no other issues with how the appliance handles traffic.
- Continue to test and refine policy, move to production, and then update policy actions to block.
- Continue to test and refine policy, move to production, and gradually update each engine or policy’s actions to block.

Repeat the previous steps as needed. Configure Monitor/Block actions: "Manage WAF Security Policy" on the next page.
Manage WAF Security Policy

As described in "Analyze and Refine WAF Policy (Mitigate False Positives)" on page 150, you will need to refine your WAF security policy to ensure it is working properly.

WAF Policy Use

Refining your WAF Security Policy is step 9 in "Use WAF Policy To Protect Servers From Attacks" on page 130.

Add Exemptions

After installing the WAF protection policy and reviewing the access logs, you will likely find several sites that were incorrectly characterized as threats. To troubleshoot this, add exemptions to your WAF security policy. You can add exemptions using the available security options or define your own in CPL.

1. Select Configuration > Shared Objects.
2. Click the hyperlink associated with the WAF security profile or highlight the row and click Edit.

3. Click Exemptions> Add Exemption.
The system displays the Add Exemption dialog.

4. Provide a name for the exemption in the Description field.

5. Add a URL Exemption from the available security options or a custom CPL exemption:
   - Standard exemption:
     a. In the Build exemption from:, click Security Profile Sections.
     b. Enter the URL for this exemption.
     c. Select the desired Validation, Normalization, Security Engines, Blacklist, and Analytics Filter options.

     You can exempt the URL from all Blacklist or Analytics Filter processing or per rule (by specifying a CSV list of rule IDs).

     d. Click Save to close the Add Exemption dialog.
   - Custom CPL exemption:
     a. in the Build exemption from:, click Custom CPL.
     b. Add the CPL and click Save to close the Add Exemption dialog.

   The system adds the exemption for the URL or CPL. If the exemption list is long, filter for specific exemptions using the search box above the table. To clear the filter, delete the text and press Enter (or click the magnifying glass).

6. In the policy editor, click Save.

Set Block/Monitor/Ignore Actions

When first implementing a WAF protection policy, it is important to observe the effects of rules before inadvertently
Management Center Configuration & Management

blocking traffic. To begin, ensure that new rule actions are set to Monitor. Then review access logs to identify false positives, create policy exemptions (as described above) to address those issues, and repeat until false positives no longer occur. Then, update policy actions from Monitor to Block.

Options that support the Block/Monitor/ Ignore action include an action drop-down menu. To set, select the appropriate action and click Save.

For example, to set the Blacklist action to Block:

1. Select Configuration > Shared Objects.
2. Select the WAF Security Policy and click Edit.
3. Click Blacklist.
4. Verify that Enable Blacklist is selected.
5. Select Block and click Save.

Some options allow you to be even more granular, allowing you to modify individual rules, as shown below.

Use Effective Date to Manage New Rule Updates

When Application Protection Subscription (APS) updates are published, the updated Blacklist and Analytics engine content is immediately available. Because the updated engine rules can potentially change the behavior of the existing WAF security policy, Management Center enables you to use this activation date as a decision point. The Effective Date option is that decision point, enabling you to control rule selection based on the date the rules were added.
For example, rules qualified in a pre-production environment can be set to block-mode, and new rules can be set to monitor mode. This functionality enables an organization to take advantage of new rules immediately, but in a manner that will not introduce new false positives that cause requests to be blocked. After the new rules are sufficiently qualified, the effective date can be migrated forward, thereby setting the new rules into block mode.

Additionally, by using multi-tenancy this can be controlled on a per-tenant basis. This facilitates different update strategies and a tenant-configurable update cadence. For example, some tenants may choose to always use the latest rules, whereas some risk-adverse tenants may employ a very deliberate APS update qualification process. Multi-tenancy provides flexibility for diverse infrastructures where a one-size-fits-all approach may not be ideal.

Only Blacklist and Analytics Filter use the Effective Date option.
Distribute Configurations to Devices

The Symantec Management Center enables you to distribute common configurations and policies that you created and want enacted across other managed ProxySG appliances. Your enterprise might have dispersed data centers that contain hundreds of hierarchies, device groups and devices. Groups of devices might have different functions, thus requiring different sets of configurations or policies.

Two methods provide this ability.

- **Script Method**—Create scripts that contain common device configurations for specific managed devices. Give various users (with the correct permissions) the ability to create and modify script objects.

  Execute a ProxySG Configuration Script on Multiple Devices

- **Policy Method**—Use Symantec Content Policy Language (CPL) or the Visual Policy Manager (VPM) to define policy and validate it before distributing to other managed devices.

  Distribute ProxySG Policy to Multiple Devices
Create and Distribute Configurations Using Scripts

One method for distributing configurations is creating and modifying existing scripts to execute on command across dispersed data centers that contain hundreds of hierarchies (managed device groups and devices).

Create a Script.

1. Select Configuration > Scripts.
2. From the Script Objects page, click Add Script. The web console displays the Add Script dialog.

   Enter the following information (a red asterisk (*) denotes a field that is mandatory).
   a. **Name** the script.
   b. Select a device **Type** from the drop-down list
   c. (Optional) A **Description** helps to differentiate between similarly named scripts.
   d. (Optional) Select **Substitution Variables**. The Management Center attempts to replace variables with the values associated with the device where the policy is installed or the script is executed. For more information, see "Use Substitution Variables in Policies and Scripts" on page 202.
3. Click **Save**. The new script displays in the Script Objects list.
4. Select the script and click **Edit**. The Management Center displays the script Editor.
5. Create the script.
6. Click **Save**.

Execute a Script on a Device.

The Management Center provides two places where you can run a script on a device now.

1. Select Configuration > Scripts.
2. Select a script from the **Script Object** list. If needed, search for the object; see "Filter by Attributes and Keyword Search" on page 167.
3. Click **Execute on Device**. Select the device **Target** and click **Execute**.

OR

4. Select Edit and click the Editor tab. At times, administrators with the correct privileges want to execute a script immediately after updating a script. While in the rich text editor ensures that all edits have been saved and click **Execute on Device**. Select the device **Target** and click **Execute**.

   Each time you start a job manually, the Management Center displays a Job Progress dialog. To run the script in the background (no window) while you perform other tasks, click **Continue in Background**.

Preview a Script With Variables Replaced

Management Center enables you to check the validity of a script before you execute the script to a device. Symantec recommends that you preview scripts before executing a script. Devices that are in your network deployment should not be used to test configurations. Previewing a script avoids inadvertently changing a device configuration.
Management Center Configuration & Management

For scripts that use commands not in configure mode, you must exit configure mode before executing the script. Most commands are executed in configure mode. Licensing commands are the exception, and cannot execute in configure mode.

1. Select Configuration > Scripts.
2. Open a script object.

3. From the Editor tab, click Preview.
4. Select a device to preview the script and click OK.

5. The Preview Script window displays the entire script.
6. Click Close.

(Optional) Create a Job to Execute a Script on a Schedule.

Management Center makes it easy to create a job to Execute a script without the hassle of going through the entire job wizard.

1. Select Configuration > Scripts.
2. Select a script from the Script Object list. If needed, search for the object; see "Filter by Attributes and Keyword Search" on page 167.
3. Click Execute on Device. Select the device Target and click Create Job. The web console displays the New Job dialog.
   a. Name the job; click Next.
   b. Select an Operation; for this example: Execute Script; click Next
   c. Select the Devices to receive this configuration; click Next
   e. Click Finish.

Manage Scripts

Navigate to the following sections for more information.

- "Customize Object Filters" on page 161—Limit view of script objects.
- "View Script Information" on page 173—View versions and attributes.
- "Manage Attributes" on page 400—View current and add new attributes.
- "Filter by Attributes and Keyword Search" on page 167—Find a script by the attributes assigned to the script.
- "Import Script from a Device" on page 169—Import a configuration from a selected device.
- "Restore a Version of Script " on page 172—Roll back to a previous configuration while you perform modifications to the current version.
- "Compare Versions of the Script" on the next page—Useful for troubleshooting.
Compare Versions of the Script

As a troubleshooting step or as part of performance evaluation, you might want to identify the changes between an earlier version and a later version of a script. Management Center shows the changes made.

1. Select **Configuration > Scripts**. From the **Script Objects** list, select the script name. If needed, search for the object; see "Filter by Attributes and Keyword Search" on page 167.
2. After you select the script, click **Edit**. Click the **Versions** tab.
3. Select an earlier version of the script to compare with the current version.
4. Press and hold the CTRL key while selecting the later version of the script to compare.
5. Click **Compare**. The web console displays the Compare Scripts dialog.

The two scripts are displayed side-by-side; the web console displays the version you selected first (earlier version) on the left and your second selection (later version) on the right.

- A script highlighted in red exists in the former version and was removed in the later version.
- A script highlighted in yellow indicates that a line exists in both versions of script, but there are differences in the line.
- A script marked in green does not exist in the former version and was added in the later version.

See "Restore a Version of Script " on page 172.
Customize Object Filters

Filters control the specific objects that are searchable.

1. Select **Configuration > Policy** or **Scripts**.
2. The **Filter** panel contains the following fields.
   - **Name**—Filters by the Object Name.
   - **Reference Id**—Filters by the Operation type.
   - **Type**—Filters by the Object Type.
   - **Description**—Filters by the Object Description.
   - **Author**—Filters by the user who last changed the Object.

   To substitute variables in policies, policy fragments or scripts, see "Use Substitution Variables in Policies and Scripts" on page 202.

3. The **Filter** panel also includes mandatory attributes. See "Manage Attributes" on page 400.
4. To customize filters, click **Customize**.

   a. Select the filters to be visible on the **Filter** panel.
   b. Click **Save**.
Execute Scripts

You can execute any script that is saved in Management Center in the Script Object list. Before executing a script, you can "Preview a Script With Variables Replaced" on page 157. This shows the script variables without committing them to a device and inadvertently causing a device configuration to change.

Scripts are automatically assumed to execute in configure mode on the ProxySG appliance. For scripts that use commands not in configure mode, exit configure mode before executing the script. Licensing commands are the exception, and cannot execute in configure mode. Example:

```plaintext
;;exit configure mode
exit
user-license queue
;;re-enter configure mode
configure terminal
```

Execute a Single Script

Direct from a Script

1. Select Configuration > Scripts.
2. Select a script object and then click Edit.
3. To execute the script, click Execute on Device.
4. Select a target device or device group. Click Execute. (Optional) You can execute the script at a later time (on a schedule) by clicking Create Job...See New Job (under Execute Multiple Scripts), starting with step 3, for details.

From a Job Operation

See New Job (under Execute Multiple Scripts) for details on executing a single script from a job.

Execute Multiple Scripts

New Job

1. Select Jobs > Scheduled Jobs.
2. Click Add New Job.
3. Enter a name (required) and a description. Click Next.
4. Select Execute Script from the Operation menu.
5. Select the Device Type from that menu.
Because a script is specific to a device, variable substitution requires that you select the appropriate device.

6. Click **Add Script**.
7. Select the desired script(s) and then click OK.

- You can also set a job to run a single script.

8. (Optional) Use Delete, Move Up, and Move Down to edit the available scripts and their order.

- Scripts run, one right after another, based on the order shown on the list. If one script fails, the next script continues to execute. Be sure the scripts are ordered how you want them to run.

9. Click Next.

10. (Optional) Select a target device or device group.

11. Click Next.

12. Select a schedule to run the script(s). See Job Scheduling Options for more information. Click Finish.

Edit an Existing Job

1. Select Jobs > Scheduled Jobs.

2. Select a job and then click Edit.

3. Click the Operation tab.
4. Click **Add Script**.
5. Select the desired script(s) and then click **OK**.
6. (Optional) Use **Delete**, **Move Up**, and **Move Down** to edit the available scripts and their execution order.
7. Click **Save**.

(Optional for all script executions) While the Job Progress dialog displays the script executing, click **more details** to view the **Output**, **Download as Text**, or **Close** the dialog.
Filter by Attributes and Keyword Search

You can search for existing objects by filtering on attributes and then using the keyword search. When you are managing hundreds or policies and scripts across multiple devices, it is important to be able to find a particular object quickly.

You are not limited to the displayed Filter fields. See "Customize Object Filters" on page 161.

1. Click the Configuration tab and select Policy or Scripts. From the Filters list on the right pane, the following fields are available by default.
   - Name—Filters by the Object Name
   - Reference Id—Filters by the Object Reference Id
   - Type—Filters by the Object Type
   - Description—Filters by the Object Description
   - Author—Filters by who user who last changed the Object

   Additional fields are created when you create a new attribute. See "Manage Attributes" on page 400.
   - Tenant—Filters by tenant ID.

2. To filter by a particular type of policy, click the Type drop-down list and select a policy type.

3. Two options:
   - Click Apply Filters. The Policy Objects and Script Objects lists only those objects you defined by Type.
   - Filter by particular device type for which you created a script; select the device type from the Type drop-down list.

5. Click Apply Filters. The Script Objects list displays only those scripts you defined by type.

Search by Keyword

When searching, Management Center breaks text into keywords and then searches for keywords entered. Management Center’s index system has a special case for dot. Although Management Center sees dots as separating letters within a word (for example, Management Center considers dots as a part of a word).

The wildcard symbol is *. Management Center automatically appends an * at the end of your search term but if you want to start with a wildcard search, you have to enter it yourself.

Colons are treated like other non-letters by splitting keywords apart. IPv4 and IPv6 addresses work differently because of colons.

You cannot search on special characters, such as ^% | ~.
Management Center Configuration & Management

Procedure

1. From the **Keyword Search** field, enter your search term.
2. Press Enter or click the magnifying glass icon.

**Can quotes be used in a search?**

Use quotes when non-letters are part of the search term. For example, your search term includes a colon.

---

The exception to this search rule is the use of a dot because a dot that is *not* followed by whitespace is considered part of the keyword.

---

**How do you search for whole words?**

Enter the whole word. If there is more than one word, separate each word with a space. If using special characters, enclose each word in double quotes.

**How do you search for partial words?**

Enter the partial term, and Management Center attempts to complete the search. For example, enter **hi** and Management Center matches that to both **highlight** and **high**.

---

**Example Searches**

**IPv4 127.0.0.1**

- **127.0.0.0**—Matches any IPv4 starting with **127.0.0**.
- ***0.0.1**—Matches any IPv4 ending in **0.0.1**.

**IPv6 "0:0:0:0:1"**

Use quotes for IPv6 addresses because IPv6 uses colons instead of dots as the separator.

- **"0:0:0"**—Matches any IPv6 start with **0:0:0**.
- **"*0:0:1"**—Matches any IPv6 ending with **0:0:1**.

**Hostnames**

- **abc.com**—Matches a host named **abc.com**.
- ***.com**—Matches a hostname ending in **.com**.
- **"*:8080"**—Matches a hostname with **:8080** as the port.

**What if the search finds no match?**

If the search finds no match, the right pane displays a message indicating that no objects match the keyword filter. You can search again using a different keyword.

**What if the search succeeds in finding matches?**

If the search finds matches, the results display in alphabetical order in the **Objects** list.

**How do you clear the search results?**

To clear search results and display all objects in the system, click the **X** in the search field.
Import Script from a Device

Scripts are sequentially-running CLI commands for a device configuration. It makes sense to import device configurations that are currently on a device because you know that the configuration is correct. Importing an entire device configuration is essentially backing up a device into Management Center and may not exist as a whole such as in the following situations:

- You want to restore a previous version of script that exists only on a device. For example, you started editing script in Management Center, but realize that the script on the device is correct and complete.

- A device has a full configuration that you want to use as a script (template) to execute on another like device. An asterisk denotes fields that are mandatory.

1. Select **Configuration > Scripts**.
2. Scripts can only be imported into an existing script object. Select a script name. Click **Edit**.
3. Click **Import**.
4. Select a device to import the script. Click **OK**. The web console displays the Import Script dialog.
5. From What to Import, select **Entire Configuration** or **Only selected sub-sections**.

![Import Script from Device dialog]

1. Select Configuration > Scripts.
2. Scripts can only be imported into an existing script object. Select a script name. Click **Edit**.
3. Click **Import**.
4. Select a device to import the script. Click **OK**. The web console displays the Import Script dialog.
5. From What to Import, select **Entire Configuration** or **Only selected sub-sections**.

![Import Script from Device dialog]
6. Click **Import**.
   The comment you enter is saved as script metadata.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>View existing script information.</td>
<td>&quot;View Script Information&quot; on page 173</td>
</tr>
<tr>
<td>Restore a version of the script.</td>
<td>&quot;Restore a Version of Script &quot; on page 172</td>
</tr>
<tr>
<td>Execute the script, as is, to devices.</td>
<td>&quot;Execute Scripts&quot; on page 162</td>
</tr>
</tbody>
</table>
Manage Attributes

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Because you have different devices and appliances to manage, those devices require and are often restricted to certain attributes. Attributes are custom metadata used to refine and edit devices, device groups policy, and scripts. Attributes can be used to filter on specific devices, device groups or objects.

1. Select Administration > Attributes.
2. From the Manage Attributes list, select one the following:
   - Device
   - Device Group
   - Policy
   - Device Script
3. To add an attribute, click Add Attribute. See "Add Attributes" on page 401.
4. To edit an attribute, select the attribute name and click Edit. See "Edit Attributes" on page 404.
5. To enable group inheritance, see Enable Attribute Group Inheritance.

View and Sort the Following Attributes Lists

- **Name**—The attribute name (with no spaces).
- **Display Name**—The format that users must enter or select values.
- **Type**—The format that users must enter or select values.
- **Default Value**—Select the default value that displays in the Attributes list. Default values can be substituted by other variables. See "Use Substitution Variables in Policies and Scripts" on page 202.
- **Mandatory**—The value of attributes that are marked as mandatory is required when you create a new or add a device, device group, create a policy, and create a script.
- **Inheritable**—Applies specifically to devices and device groups. When this is selected, the device or device group inherits attributes from its parent device group.
- **Description**—Describes the attribute and must be specific to the device, device group, policy, or script to which you are applying the attribute.

You are able to search for specific objects based on the attributes you define. See "Filter by Attributes and Keyword Search" on page 167.
Management Center Configuration & Management

**Restore a Version of Script**

After time, you might find that the script executed on devices needs improvement or must change because of changes in business requirements or practices. In such situations, you can modify scripts as needed, or revert to an earlier version of a script that is appropriate. When you have determined which version of script to restore, you can restore it using the version history.

1. Click the **Configuration** tab and select **Scripts**. From the **Script Objects** list, select the script name. If required, search for the object; see "Filter by Attributes and Keyword Search" on page 167.
2. Click **Edit**. Click the **Versions** tab. Versions of the script are listed in descending numerical order.
3. From the **Version Control** page, verify that the version you want to restore is the correct one. Perform one or both of the following as required.
   - Check the version metadata. See "View Script Information" on the facing page.
   - Preview a script with the variables replaced.
4. After you have identify the version to restore, select it and click **Restore**. The web console displays the Restore dialog.
5. In the **Comment** field, specify the reason for the restore.
6. Click **Restore**.
   The restored version of the script is incremented to the latest version in the **Script Objects** list, and the comment you entered in step 6 is displayed in the **Comments** column.
View Script Information

Whenever you create a script, Management Center automatically saves information about it. This information is called metadata.

1. Select Configuration > Scripts.
2. From the Script Objects list, select a script and click Edit. An asterisk denotes fields that are mandatory.

View Script Object Information

1. Click the Info tab.
2. Under General Information, the Overview displays the information you entered when creating the script object:
   - Name(*)—The name of the script that you gave it when you created it
   - Type(*)—The device type that the script applies to
   - Description—This describes the script, but is not a required field
   - Replace substitution variables

3. Metadata displays under Latest Revision. Click Save.

   If you edited any of the fields in Overview, fields marked with a red asterisk (*) are required and cannot be left blank.

View Script Versions

1. Click the Versions tab. The Version Control page lists all versions of the selected script. When a script object is created it is assigned the version number 1.0. Every time that the script attributes change or the script is edited, the version increases by increments of 0.1.
2. Select an early version of script to compare.
3. Press and hold the Ctrl key while selecting the newer version of the script.

   - Version Number—When a script object is first created, its version is 1.0. Each subsequent time the object is modified—for example, if the object properties are edited the version number increments by 0.1. For example, when you add script text to the object and save it, the version becomes 1.1.
   - Date—The time and date stamp indicates when the script was last updated.
   - Author—The author is the user who saved the current version of the script displayed.

   - Comments—If the author entered comments or a description about the script, they are displayed here. Metadata displays automatically-generated comments as follows:
     - "Script Object created"—When the script container is initially created and script has not been added yet.
     - "Name changed"—When the script name is edited.
     - "Description changed - former script has been overridden"—When the script description is edited.
     - "Name and description changed - former script has been overridden"—When both the name and description are edited.

   Of these metadata, the comments are usually the most important in helping you and other users understand the purpose and intent of creating the specific script version. Symantec recommends that you always enter clear, helpful comments when creating scripts.
View Script Attributes

Click the Attributes tab. The Attributes page displays all attributes currently assigned to selected script. The attributes are custom attributes that you created. See "Manage Attributes" on page 400.

View Device Script Output

When you execute a script on a device, the Job Progress dialog displays the status of the executing script. You can view the device output of currently executing scripts and scripts that have already executed on a device by clicking More Details. Any output line that starts with "%" is considered a warning (and is standard for ProxySG appliances). Navigation buttons enable you to jump between warnings and are useful when viewing the device output for long scripts. You can view the raw output in a text editor by selecting Download as Text.

Set the Maximum Number of Script Revisions to Store in Management Center

After you create or import a script, you can edit the script to execute on devices of the same type. You can specify the number of revisions of scripts to store before Management Center begins to prune. You can specify up to 999 script revisions.

1. Select the Administration > Settings. Click General. General fields display on the right. An asterisk denotes fields that are mandatory.
2. Select Maximum number of script revisions to store.
3. Enter a number (limit) from 0 to 999.
4. Do one of the following:
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server.
   - Click Activate to cause the server to load and apply the currently saved configuration.

Apply Logical Expressions to Scripts and Policy

Logical expressions allow you to build intelligence into scripts and policy, so they to make decisions when executing. As the system processes a script or pushes policy to devices, it can process ${if ...} and ${else} expressions to determine whether to apply elements of the configuration to all, or only some, of the selected devices or policies.

For example, logical expressions could be applied to a configuration change where some members of a group of ProxySG appliances have a user group called "clerks" while another group of appliances does not. If the "clerks" policy is found in appliances in locations where those users exist, update policy. If it does not, skip that update.

When used in conjunction with the ${if ...} and ${else expressions, ${foreach ...} can be used to iterate over a set of values, in order to to apply unique ${if ...} and ${else logic to loop script processing to test for a specific value.

Supported Expressions

${if variable}

Test for the existence of a variable. If the variable has a value, the scripted condition evaluates as true.

💡 You can use two hyphens to comment out an if condition. When ${--if ...} is encountered, the script will skip the associated action.
${if variable=value}
Test for the value of a variable. If the variable has a matching value, the scripted condition evaluates as true. If the value entry includes spaces, enclose in quotation marks.

⚠️ You cannot have spaces around the =.

${else ..}
Used in conjunction with an ${if ..} expression. During script processing, when an ${if ..} expression is not matched, an ${else} expression determines an alternate course of action.

${foreach ..}
Used in configuration scripts and policy to iterate over the values in a collection of attributes. Though not required in scripts where ${if ..} and ${else} are used, ${foreach ..} triggers a loop of processing, while testing each target device to match trigger attributes.

Examples
The examples below use custom variables. For more information on defining variables and using them in scripts, see "Use Substitution Variables in Policies and Scripts" on page 202.

Define simple if else logic flow
This example defines one DNS server address on ProxySG devices running in a network named "Guest Wireless", and set another DNS address on appliances in other, unspecified networks.

${if device.attributes.Network="Guest_Wireless"}
  dns-forwarding
  edit primary
  add server 8.8.8.8
${else}
  dns-forwarding
  edit primary
  add server 203.0.113.5
${end}

Define advanced if else logic flow with foreach
In this example, the script uses foreach to identify only the specific device members Management Center will apply configuration changes to. Unlike the previous example, defining the script in this manner takes action only on those devices that are explicitly identified in the script.

${foreach device.memberOf group}
  ${if group='Data Center 2'}
    dns-forwarding
    edit primary
  ${end}
Use Substitution Variables in Policies and Scripts

Substitution variables are generic terms (like attributes or shared objects) that you can include in policies and scripts. These terms are attributes you might have setup on your devices, groups, etc. When Management Center installs policy or executes a script that includes substitution variables, it attempts to replace them with values specific to the current transaction—that is, the current device, policy, or script. For example, if you install policy that includes the substitution variable `${device.name}`, the variable is replaced with the device name set in Management Center.

Use in Shared Policy

When you include shared policy objects in your policy, you must enable variable substitution or the shared object’s CPL will not be substituted for the `include` variable. For example, if you create a URL list called `whitelist` and include it in a policy object, the system creates the CPL entry `${include:whitelist}`. The `whitelist` URL list will only be included if `Replace substitution variables` is selected when the policy is installed.

While you may use substitution variables in CPL layers, Management Center performs the substitution when installing the CPL to the device. The UI markup (XML) remains unchanged. Therefore, if you open the installed VPM policy locally from the ProxySG appliance and try to install it, the substitution variables will not be replaced in the resulting CPL (because this workflow bypasses Management Center). This could result in malformed or unexpected policy, depending on how the variables are being used.

To include and process substitution variables:

1. Verify that `Replace substitution variables` is enabled in the policy object (see [Create a CPL Policy Object](#)) or script (see [Create and Distribute Configurations Using Scripts](#)).
2. Include substitution variables in the CPL or script. See "Supported Variables" on the facing page below.
3. Install the policy or execute the script. As the target device processes the policy or script, it attempts to replace the variables with the appropriate values.

   If the policy or script is associated with a device group, Management Center inspects every device in the group structure for the variable and attempts to replace all instances with specific values.

**Syntax**

Substitutions have the following form:

`${name}`

where `name` is an expression that expands to a string or block of text at runtime.
For example, the substitution `${device.description}` expands to the description entered in the current device’s properties in Management Center.

If the device does not have a description (because Description is an optional field), the substitution expands to an empty string unless you also specify a default value. See “Specify a Default Substitution Value” on page 179 below for details.

**Examples**

Substitute the device's serial number.

`${device.serialNumber}`

Substitute the value of the device's Rack attribute.

`${device.attributes.Rack}`

Substitution variables are case-sensitive. To ensure that you have entered them with correct spelling and case, use the Preview option before installing policies or executing scripts. The preview warns you if a substitution variable is invalid.

**Supported Variables**

**Device - `${device.field}`**

The following variables are available for policies and scripts.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${device.memberOf}</code></td>
<td>List of the groups to which a device is assigned</td>
</tr>
<tr>
<td><code>${device.uuid}</code></td>
<td>Internal ID of device</td>
</tr>
<tr>
<td><code>${device.modelNumber}</code></td>
<td>Device model number</td>
</tr>
<tr>
<td><code>${device.description}</code></td>
<td>Text in the Description field in device properties in Management Center</td>
</tr>
<tr>
<td><code>${device.name}</code></td>
<td>Text in the Device Name field in device properties in Management Center</td>
</tr>
<tr>
<td><code>${device.serialNumber}</code></td>
<td>Device's serial number</td>
</tr>
<tr>
<td><code>${device.osVersion}</code></td>
<td>Operating system version running on the device</td>
</tr>
<tr>
<td><code>${device.type}</code></td>
<td>The device type, for example, ProxySG.</td>
</tr>
<tr>
<td><code>${device.attributes.name}</code></td>
<td>System or user-defined device attribute value, including any values inherited from the device group</td>
</tr>
</tbody>
</table>

**Device Connection - `${device.connection.field}`**

The following variables are available for policies and scripts. A variable might not be applicable to every device.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${device.connection.host}</code></td>
<td>Host IP address</td>
</tr>
<tr>
<td><code>${device.connection.port}</code></td>
<td>Port number</td>
</tr>
</tbody>
</table>
Designates the way the connection is established and optionally how authentication is performed. For example, **SSH_PUBLIC_KEY**

**PRODUCTION** or **PREPRODUCTION**

User name for authentication. Only relevant for ProxySG/ASG when credentials are used.

---

**Policy - ${policy.field}**

The following variables are available for policies only (not scripts).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${policy.author}</td>
<td>Last user who edited and saved the policy</td>
</tr>
<tr>
<td>${policy.description}</td>
<td>Text in the Description field in policy properties</td>
</tr>
<tr>
<td>${policy.name}</td>
<td>Text in the Name field in policy properties</td>
</tr>
<tr>
<td>${policy.referenceId}</td>
<td>Text in the Reference Id field in policy properties</td>
</tr>
<tr>
<td>${policy.revision}</td>
<td>Policy's current Version number</td>
</tr>
<tr>
<td>${policy.revisionDescription}</td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td>${policy.attributes.name}</td>
<td>User-defined policy attribute value</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>where name is the attribute name</td>
<td></td>
</tr>
</tbody>
</table>

**Policy Fragment- ${fragment.field}**

The following variables are available for policy fragments.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${fragment.author}</td>
<td>Last user who edited and saved the policy fragment</td>
</tr>
<tr>
<td>${fragment.description}</td>
<td>Text in the Description field in policy fragment properties</td>
</tr>
<tr>
<td>${fragment.name}</td>
<td>Text in the Name field in policy fragment properties</td>
</tr>
<tr>
<td>${fragment.referenceId}</td>
<td>Text in the Reference Id field in policy fragment properties</td>
</tr>
<tr>
<td>${fragment.revision}</td>
<td>Policy fragment's current Version number</td>
</tr>
<tr>
<td>${fragment.revisionDescription}</td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td>${fragment.attributes.name}</td>
<td>User-defined policy fragment attribute value</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>where name is the attribute name</td>
<td></td>
</tr>
</tbody>
</table>

**Script - ${script.field}**

The following variables are available for scripts only (not policies).
Variable | Description
--- | ---
${script.author}$ | Last user who edited and saved the script
${script.description}$ | Text in the Description field in script properties
${script.versionDate}$ | Date of last update
${script.name}$ | Text in the Name field in script properties
${script.type}$ | Selected Type in script properties
${script.revision}$ | Script’s current Version number
${script.revisionDescription}$ | Comments entered for the last revision
${script.attributes.name}$ | User-defined script attribute value
where *name* is the attribute name

**Specify a Default Substitution Value**

Unless you specify a default value, some transactions can produce unsubstituted variables, resulting in empty strings. The following are examples of such transactions:

- An optional field such as Description is empty
- An attribute that is not marked as mandatory has no value
- A field is not applicable, such as when a script or policy has not been revised

**Syntax**

A default substitution has the following form:

${name(default_name)}$

where:

- *name* is an expression that expands to a string or block of text at runtime
- *default_name* is the value that will be used instead of an unsubstituted variable

**Example**

If a policy fragment was edited, use the comments entered for the last revision. If the fragment was never edited, use the specified text "No revision".

${fragment.revisionDescription(No revision)}$

**Use Regular Expressions**

Policy and script processing can make use of Regular Expressions (RegEx).

**Syntax**

regex

**Example**

RegEx can be used in variables to produce generic results as follows:

${device.osVersion;regex(SGOS (.*))}$ will return just the number portion of SGOS version for SG devices
And RegEx can be used as part of a condition with specific strings:
\$\{device.osVersion;regex(SGOS (.*) )="6.7.3.100\}" will test for the specific version of SGOS.

Organize Scripts by Attribute

This use case describes how to use attributes to logically organize your scripts. This technique can be useful when you have a large number of scripts and want to better organize them. Think of the attributes as folders for your scripts. By adding different attributes, you can organize your scripts in different ways.

In this example, we want to organize scripts by their purpose, but you can organize them in other ways as well.

1. Select Administration > Attributes > Device Scripts.
2. Click Add Attribute to create a new attribute definition.

The new attribute's name is **Purpose** because we want to logically arrange the scripts by their purpose.
3. Click **Save**.

4. Select **Configuration > Scripts**. You will see the **Purpose** header on the grid.

![Image of script list grid with Purpose header highlighted]

If you want to move the **Purpose** column, you can drag it to a different position.

5. Hover the mouse cursor over the **Purpose** header to display the down arrow and click it.

![Image of dropdown menu for Purpose header]

6. Select **Group by this field**.

7. Select a script and click **Edit**.

8. Select the **Attributes** tab and enter a value in the **Purpose** field.
9. In this example, we have used **Test, Iteration 1**, and **Iteration 2**. You can see how the grid now organizes the scripts around their attribute values.

<table>
<thead>
<tr>
<th>Purpose: Iteration 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local_DB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose: Iteration 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>scriptjob</td>
</tr>
</tbody>
</table>

You can also setup the attribute to be a picklist if you want to have predefined values.


Create and Distribute Policy

When you first configure Management Center, you can create new policies or import existing policies from managed devices. When you have been managing devices from Management Center for a longer period of time, you might also want to edit policies to change current device configurations. One of Management Center’s most powerful features is the ability to create and modify policy objects before deploying multiple policies across data centers containing hundreds of hierarchies, device groups, and devices.

Policy Editing Conflict Management (Policy File Locking)

Starting with Management Center 1.6, a policy file is automatically "locked" as soon as a user starts editing policy. If another user tries to edit the same policy, that user will receive the following message.

The policy lock is released after the user saves or cancels the changes. When a policy lock is active, another user may force that policy to unlock by clicking Unlock on the policy grid.

Policy locking affects the content of policy only. Other attributes (Targets, Info, etc.) can be changed even while the policy is being edited by another user.

Create and Edit CPL Policies

Content Policy Language is a language for specifying the policy rules for the ProxySG appliance.

For complete information about the Content Policy Language, refer to the Content Policy Language Reference. Another way to create CPL policy is to create CPL fragments (or building blocks). See "Create a CPL Policy Fragment" on page 223.

Management Center gives you great flexibility for creating and modifying CPL policies, as well as the power to deploy multiple policies to a range of devices or device groups. Use CPL to accomplish the following:

- Create and modify the CPL directly from the policy editor (Configuration > Policy > PolicyName > Edit). See "Use Content Policy Language (CPL) to Create Policy" on page 187.
- Create policy without assigning it to devices immediately. See "Create a CPL Policy Object" on page 189
Create VPM Policies

The Visual Policy Manager enables you to specify the policy rules using a GUI editor for the ProxySG appliance and install the policy to the VPM slot. For complete information about the Visual Policy Manager, refer to the Visual Policy Manager Reference and Advanced Policy Tasks.

You can:

- Create and modify policy in the VPM. See "Launch Visual Policy Manager" on page 210 and Add a VPM Policy Object.
- Select a reference device to edit VPM policy. See "Select Reference Device for VPM Policy" on page 212.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy" on page 335.
- View the CPL or XML source.
- View or compare policy versions.
- Create or "Edit Attributes" on page 404 and apply them to policy objects.
- Add target devices and install policy to them.
- Deploy multiple policies to a group of devices by using Management Center's job feature. See "Install Multiple Policies" on page 307.
- Import existing policy from a managed device. See "Import Policy or Shared Objects" on page 308.
- Check the consistency of installed policy.
- View the deployed policy on a device.
- View existing policy information. See "View Existing Policy Information" on page 319.
- Clone to universal VPM policy.

Create Universal VPM Policies

Universal policy is a set of global rules created on Management Center that can be applied to users in any location. The policy can contain global rules that apply to both on-premises and Web Security Service (WSS) users, as well as individual rules that apply to only one or the other. It can also contain location-specific policy when necessary. In essence, universal policy comprises the various rules that reflect your organization's acceptable use policy. Using Management Center to create and distribute the policy to on-premises devices and the WSS makes it easy to apply the relevant policy to all users.
in your organization.

- **Deploy** universal policy.
- **Create** a universal policy object.
- Import existing policy from a managed device. See "Import Policy or Shared Objects" on page 308.
- **Transform** existing VPM policy into universal policy.
- Use the Visual Policy Manager to apply policy to on-premises and remote users.
- Select a reference device to edit VPM policy. See "Select Reference Device for VPM Policy" on page 212.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy " on page 335.
- **View** the CPL or XML source.
- **View or compare** policy versions.
- Create or "Edit Attributes" on page 404 and apply them to policy objects.
- Add target devices and install policy to them.
- Deploy multiple policies to a group of devices by using Management Center's job feature. See "Install Multiple Policies" on page 307.
- Check the consistency of installed policy.
- View the deployed policy on a device.
- View existing policy information. See "View Existing Policy Information" on page 319.

Create Tenant Determination Policies

A Tenant Determination File contains rules for routing request traffic to the proper tenant. This determination criteria controls which set of tenant policy will be evaluated for a given request. If a tenant determination cannot be made, the "default" tenant policy is used. You can:

- Create and edit tenant determination policies directly from the policy editor (Configuration > Policy > PolicyName > Edit) (without assigning the policy to devices immediately).
- Use tenant determination rules to properly route traffic to the correct web application (or group of web applications). See "Specify Tenant Determination Rules " on page 138 and "Use WAF Policy To Protect Servers From Attacks" on page 130.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy " on page 335.
- Create policy attributes and apply them to policy objects. See "Add Attributes" on page 401
- Add target devices and install policy to them.
- Deploy multiple policies to a group of devices by using Management Center's job feature. See "Install Multiple Policies" on page 307.
- Check the consistency of installed policy.
- View the deployed policy on a device.
- View existing policy information. See "View Existing Policy Information" on page 319.

Create WAF Application Policies

A WAF Application Object represents a web application (or group of applications) and the associated WAF security settings. The WAF application object is associated with a specific tenant and WAF Security Profile. You can:

- Use WAF Application policies to associate a Security Profile to a tenant, manage optional CPL fragments, and control WAF Application settings. See "Configure WAF Security Rules " on page 141 and "Use WAF Policy To Protect Servers From Attacks" on page 130.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy " on page 335.
Management Center Configuration & Management

- Create policy attributes and apply them to policy objects. See "Add Attributes" on page 401.
- Deploy multiple policies to a group of devices by using Management Center's job feature. See "Install Multiple Policies" on page 307.
- View existing policy information. See "View Existing Policy Information" on page 319.

Create SSL Visibility URL List Policies

You can create policy in Management Center that manages URL lists for SSL Visibility appliances, and then deploy the policy to a group of SSL Visibility appliances. See "Create SSL Visibility URL List Policy" on page 269.

Create SSL Visibility IP Address List Policies

You can create policy in Management Center that manages IP address lists for SSL Visibility appliances, and then deploy the policy to a group of SSL Visibility appliances. See "Create SSL Visibility IP Address List" on page 277.

Create Local Content Filter Databases

You can create a local content filter database in Management Center that all of your ProxySG or Advanced Secure Gateway appliances can use in policy. This database is hosted on Management Center. See "Create a Local Content Filter Database" on page 255 for details.
Use Content Policy Language (CPL) to Create Policy

Before writing policies in CPL, Symantec strongly recommends that you understand the fundamental concepts underlying policy enforcement in ProxySG appliances, as well as how to write correct CPL. For comprehensive information on CPL, refer to the Content Policy Language Reference.

You can compose CPL directly in the web console editor.

1. Select Configuration > Policy. From the Policy Objects list, select the policy object to edit. Ensure that the policy’s object type is CPL. Select the policy. If you have a lot of policies narrow your search using “Filter and Keyword Search” on page 407.
2. Select Edit and the Editor tab. The other tabs available for viewing and editing purposes are the following:
   - Targets
   - Versions
   - Attributes
   - Info
3. The middle pane displays the sections in the policy, and the Quick Navigation pane on the right displays a summary of the sections in the object.
4. In either the middle pane or in Quick Navigation, select the section you want to edit. If needed, expand the sub-section (default, override, or mandatory) to edit.

A policy object is organized into sections. Each section has a name and a purpose, and can contain up to three sub-sections of CPL that you can use to organize policy: Default, Override, and Mandatory. See "Edit a Policy Section" on page 192.

If the modular sections perform slowly, you can select the Single Pane Layout icon. This is useful if the CPL is particularly long or if you prefer working with a single pane of code. Note that switching to a single pane and saving the policy erases all metadata about your sections. You cannot recover the sections by switching back. However, you can either discard the changes without a save, or you can restore a previous version.

5. Enter the CPL in the appropriate sub-section(s).
6. Repeat steps 3 and 4 as needed. An asterisk denotes fields that are mandatory.
7. Click Save. Management Center prompts you to enter a comment for the save operation.

8. (Optional) Click Compare to see the differences between the previous version and the version you are about to commit. For information on comparing versions, see "Compare Different Versions of the Same Policy" on page 331 and "Compare the Device Policy Version with Current Policy Version" on page 332.
9. Enter a description of your changes and click Save.
   The comment you enter is saved as policy metadata. For information on metadata, see "View Existing Policy Information" on page 319.
Working with CPL Policy Fragments

A fragment is a piece of CPL that you can include in a CPL policy. Fragments are meant to be reusable. For example, you can create a library of policy fragments, and then include them in larger CPL policies later. For instance, you can define a host black list using just a fragment, and then include that host black list fragment into a larger policy file later. See "Create a CPL Policy Fragment" on page 223 and "Include a Shared Policy Object in CPL or VPM Policy" on page 232.

If you do NOT enable variable substitution in the CPL, variable substitution is not enabled for CPL Fragments as well.

Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable variable substitution for CPL Policy and CPL Policy Fragments.</td>
<td>&quot;Use Substitution Variables in Policies and Scripts&quot; on page 202</td>
</tr>
<tr>
<td>Add new attributes that can be made available to the CPL Policy.</td>
<td>&quot;Add Attributes&quot; on page 401</td>
</tr>
<tr>
<td>Add or edit sections of a CPL Policy.</td>
<td>&quot;Add or Edit CPL Policy Sections&quot; on page 191</td>
</tr>
<tr>
<td>Import a policy from a device to Management Center.</td>
<td>&quot;Import Policy or Shared Objects&quot; on page 308</td>
</tr>
<tr>
<td>Modify/test policy and group related rules together.</td>
<td>&quot;Refine Existing CPL Policy&quot; on page 193</td>
</tr>
</tbody>
</table>
Create a CPL Policy Object

You can create policy in CPL to specify the behaviors that you want for devices. The first step to create policy in Management Center is to create the container for the CPL, or the policy object.

Before writing policies in CPL, Symantec strongly recommends that you understand the fundamental concepts underlying policy enforcement in ProxySG appliances, as well as how to write correct CPL. For comprehensive information on CPL, refer to the Content Policy Language Reference.

1. Select Configuration > Policy.
2. Click Add Policy. From the Create New Policy: Basic Information dialog, fill in the following fields: An asterisk denotes fields that are mandatory.
3. Enter the Policy name(*) - The name that displays in the Policy Object list.
4. Select CPL from the drop-down list.
5. Enter the Reference Id - Enter a Reference Id that you can filter on when building policy.

The Reference Id must begin with a letter, and must contain only letters, numbers and ".".

6. Select the Tenant to which this policy object will be applied.
7. Enter a Description. Although entering a description is optional, the description helps differentiate versions of the same policy. For more information, see "View Existing Policy Information" on page 319.
8. To enable variable substitution, select the check box Replace substitution variables. See "Use Substitution Variables in Policies and Scripts" on page 202 Click Next.

If you do NOT enable variable substitution in the CPL, variable substitution is not enabled for CPL Fragments as well. See "Create a CPL Policy Fragment" on page 223.

9. From the Attributes page, select the attributes to apply to the CPL Policy. All attributes that are marked as mandatory with a red asterisk are required. You can change the value of the required attribute before continuing. Click Next.
10. Select the devices to install the CPL. You can associate devices with the policy at any time. See "Add or Remove Devices Associated with Policy" on page 326
11. Choose the slot where your Policy will be installed. With CPL as the Policy type, the following slots are available:
   - Local - Use this file to store policy specific to your organization, such as departmental policies and company-wide policies. This option is selected by default.
   - Forward - This file contains forwarding rules.
   - Central - This slot contains policy common to your entire organization.
12. Click Finish. The newly created policy object displays in the Policy Objects list.

Determine Your Next Step

After you create a policy object, you can refine it or leave it as an empty object while you perform other tasks (for example, associate devices with it or edit policy details). Refer to the following table to determine the next step to take.
<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine an existing CPL policy.</td>
<td>“Refine Existing CPL Policy” on page 193</td>
</tr>
<tr>
<td>Enable variable substitution for CPL Policy and CPL Policy Fragments.</td>
<td>”Use Substitution Variables in Policies and Scripts” on page 202</td>
</tr>
<tr>
<td>Validate existing policy.</td>
<td>Preview Policy Before Installing It</td>
</tr>
<tr>
<td>Import an external CPL policy.</td>
<td>&quot;Import External Policy &quot; on page 315</td>
</tr>
<tr>
<td>Create a new CPL policy section.</td>
<td>&quot;Add or Edit CPL Policy Sections&quot; on the facing page</td>
</tr>
<tr>
<td>Manage your CPL policies.</td>
<td>”Manage CPL Policies” on page 195</td>
</tr>
</tbody>
</table>
Add or Edit CPL Policy Sections

You can add a policy section using one of two methods: you can use part of existing policy to create the section, or add a new section and then add policy to it.

These features are only available if the Modular Layout is selected.

Add a Section Based on an Existing Policy Section

While composing the CPL or after importing policy from a device, you might find some policy rules that should be extracted from their respective sections and put into a new section. You can select some or all of the text in a section and convert the selection to a new section. When you convert a selection, the Policy Editor preserves the order of the CPL already written.

1. Select Configuration > Policy.
2. In the Policy Objects list, select the CPL policy to which you want to add a section. Click Edit.
3. From the Editor tab, locate the policy section that contains the text you want to convert to a new section.
4. Select the text and click Operations > Convert Selection to New Section. The Policy Editor displays the new section.
5. Enter or modify the CPL as needed. Click OK.
6. Click Save.

Add a New Section

You can add more sections to a new or existing policy object. A new policy object has an empty section by default.

1. Select Configuration > Policy.
2. In the Policy Objects list, select the CPL policy that you want to add a section. Select the policy name. Click Edit.
3. Click the Editor tab. Locate the area that you want to add a new policy section. Click the Operations > New Section.
4. In the Section name field, enter a name for the section.
Management Center Configuration & Management

5. From the Purpose drop-down list, select from the list of defined policy purposes or you can create your own Custom Solution.

6. Click OK. The new section is added at the top of the Editor. Continue to edit the CPL as needed.

   If you do not name the section, and only give it a purpose, the section appears as Untitled.

7. To commit your changes, click Save.

Edit a Policy Section

While creating a CPL policy or after importing a policy from a device, you might it useful to edit the policy rules within a section. Because policy is applied to devices and can contain many types of rules, you can edit those rules within a section making policy easier to navigate, organize and deploy.

1. Select Configuration > Policy.
2. In the Policy Objects list, select the CPL policy that you want to edit and click Edit.
3. Click the Editor tab. Locate the policy section that you want to edit. You can search for a section in the Quick Navigation pane. Click Edit. The Policy Editor displays the Edit Section dialog. Although you can name the section what best suits your needs, from the Purpose drop-down list, select from a defined list of rules that can be applied to your policy section:
   - Connection - Access Control
   - Connection - Termination
   - Authorization
   - Threat protection - Outbound Policy - Forward Proxy
   - Threat protection - Outbound Policy - Reverse Proxy
   - Threat protection - Inbound Policy
   - DLP Policy
   - Privacy
   - Content Filtering
   - Quality of Service
   - Caching
   - Bandwidth Management
   - Custom Solution
4. Click OK. The edited section is added at the top of the Editor.

   If you do not name the section, and only give it a purpose, the section appears as Untitled.

5. To commit your changes, enter a comment for the commit operation and click Save. The comment you enter is saved as policy metadata.
6. (Optional) To exit without saving your edits, click Cancel.
7. (Optional) Click Compare to see the differences between the existing policy version and the version you are about to commit.
Refine Existing CPL Policy

The policy that you write is deployed to devices as it displays in the Policy Editor; Management Center does not attempt to compile or otherwise validate the CPL. If the policy does not compile, the Policy Editor displays a "Policy Install Failed" error message after you attempt to install it.

Much of the flexibility of managing policy in Management Center derives from the ability to organize policy rules in one or more policy sections, which you can use to group similar or related rules together.

CPL Policy objects and sections

Policy in Management Center is structured thus:

- **Policy object**—The container for all policy that can be installed to a specific slot on a device. It has metadata and can be versioned. Device association is done at this level.
  - **Policy section**—A container for a high-level category of policy.
  - **Sub-section**—A container for the CPL; it specifies the default, override, and mandatory behavior affected by the policy.

If the modular sections perform slowly, you can select the Single Pane Layout icon. This is useful if the CPL is particularly long or if you prefer working with a single pane of code.

Switching to a single pane and saving the policy erases all metadata about your sections. You cannot recover the sections by switching back. However, you can either discard the changes without a save, or you can restore a previous version.

See "Work with CPL Policy Sections" on page 196 for more information.

After you have written CPL directly in the Policy Editor or imported policy from a device, you should attempt to refine it as much as possible using these sections. Writing policy in sections, or breaking down an imported policy into sections, makes policy easier to read and edit.

Configuring policy for specific devices or multiple devices at once involves several methods of creating, testing, and updating policy.

1. Search for policy objects that contain the CPL you want to edit; see "Filter by Attributes and Keyword Search" on page 167.
   Once you have found the policy object, you can determine the policy section to edit; see "Find a Policy Section" on page 199.
2. (Optional) Make sure that the policy you are editing is the one you want. See "View Existing Policy Information" on page 319.
3. (If applicable) Edit the CPL directly in the Policy Editor. See "Use Content Policy Language (CPL) to Create Policy" on page 187.
   Refer to the Content Policy Language Reference for information on CPL syntax.
4. (If applicable) If policy does not behave as intended or must be improved, modify it by moving sections within policy. See "Change the Order in which Policy Rules are Evaluated" on page 201.
5. If the policy isn't working properly, you may want to compare the OS version on the associated device with the policy version. See "Check Consistency between Policy and Devices" on page 329.
6. (If applicable) Add sections to contain policy for other purposes. See “Add or Edit CPL Policy Sections” on page 191.
7. (If applicable) Edit a section’s name or purpose. See "Edit a Policy Section" on page 192.
8. Click Delete Policy, if you want to Delete a selected policy. A message displays “Are you sure you want to delete the policy?” Click Yes or No.
Manage CPL Policies

When you are first setting up Management Center, you can create new policies or import existing policies from managed devices; however, when you have been managing devices from Management Center for a longer period of time, you might also want to edit policies to change current device configurations.

Management Center gives you great flexibility in both creating and modifying your policies. You can:

- Create and modify the CPL directly in the Policy Editor
- Correct and modify the behavior of existing policy by re-ordering policy sections
- Create versions of policy, and restore previous versions when needed
- Create policy without deploying it to devices immediately

Ensuring that devices are configured and behave as required could involve creating, modifying, and testing policy. For example, you might create policy in your evaluation environment, install it to a small group of devices, observe the devices in a test phase, and then edit the policy as needed based on your observations.

Learn about creating and maintaining policy in Management Center:

1. **Create policy** and deploy it to devices. You could do some or all of the following:
   - "Use Content Policy Language (CPL) to Create Policy" on page 187 in the Policy Editor.
   - "Import Policy or Shared Objects" on page 308.
   - "Add Attributes" on page 401
   - "Install Policy" on page 302 to devices or device groups.
   - "Install Multiple Policies" on page 307 to devices or device groups.

2. To add custom metadata to policies, see "Add Attributes" on page 401.

3. "View Existing Policy Information" on page 319 to see the revisions and policy information.

4. "Compare Different Versions of the Same Policy" on page 331 to find the edited version of a policy that you want to use.
Work with CPL Policy Sections

Layout Modes

Single Pane Layout

If the modular sections perform slowly, you can select the Single Pane Layout icon. This is useful if the CPL is particularly long or if you prefer working with a single pane of code.

Switching to a single pane and saving the policy erases all metadata about your sections. You cannot recover the sections by switching back. However, you can either discard the changes without a save, or you can restore a previous version.

Modular Layout

When you open a policy for editing, it defaults to the Modular Layout. If your policy contains numerous sections or sub-sections, you can use features here to make writing and reviewing policy more manageable.
Navigate sections

These sections only appear in the Modular Layout.

The **Quick Navigation** pane displays an overview of all the sections in the policy object you are viewing. Each section is represented thus:

*Name* *(Purpose)*

- default
- override
- mandatory

where *Name* is the section name and *Purpose* is the purpose you selected when you created or edited the section.

When you change the order of policy sections or change a section name or purpose, the Quick Navigation pane displays the update immediately.

### Collapse a section

Policy sections are expanded by default.

- To collapse a policy section, click the up arrow in the section title bar.
- To expand a collapsed section, click the down arrow in the title bar.
Management Center Configuration & Management

**Collapse all sections**

- To collapse all policy sections, click the **Collapse all sections** icon.
- To expand all sections, click the **Expand all sections** icon.

**Move sections**

You can move policy sections:

- Click the order up icon in a section title bar to move the section up.
- Click the order down icon in a section title bar to move the section down.
- Hover over the title bar of the section you want to move until the pointer changes to a . Drag the section to its new location.

Moving policy sections affects how policy is evaluated. See "Change the Order in which Policy Rules are Evaluated" on page 201 for information.
Find a Policy Section

You can search for an existing policy section using keywords. When you perform the keyword search, the system searches policy sections and matches partial and full strings. The search does not include previous versions of policy.

1. Select Configuration > Policy. From Policy Objects, find the CPL Policy you want under Type. Or from the Filters dialog on the right, go to the Type drop-down list and select CPL. Click Apply Filters. From the displayed CPL policies, select the policy you want. Click Edit.
2. Click the Editor tab. Above the Quick Navigation pane, in the search field, enter your search term. You can perform this search with all sections collapsed; any matches will cause sections to expand.
3. Press Enter or click the magnifying glass icon.

If the search finds no match

If the search does not find a match, the display does not change. You can search again using a different keyword.

If the search finds matches

If the search finds matches:

- To the right of the search field, the navigation arrows and the number of results display, as in the following example:

  ![Navigation Arrows]

  1 of 13

- In the main Policy Editor pane, the first match is highlighted.
- In the Quick Navigation pane, the section that contains the first match is highlighted.

To go to the next search result, click the right navigation arrow. The result number shows the next match (for example, "2 of 13") and the selections in the main pane and Quick Navigation update to reflect the match.

Clear the search results

To clear search results, click the X in the search field.
Manage Attributes

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Because you have different devices and appliances to manage, those devices require and are often restricted to certain attributes. Attributes are custom metadata used to refine and edit devices, device groups policy, and scripts. Attributes can be used to filter on specific devices, device groups or objects.

1. Select Administration > Attributes.
2. From the Manage Attributes list, select one the following:
   - Device
   - Device Group
   - Policy
   - Device Script
3. To add an attribute, click Add Attribute. See "Add Attributes" on page 401.
4. To edit an attribute, select the attribute name and click Edit. See "Edit Attributes" on page 404.
5. To enable group inheritance, see Enable Attribute Group Inheritance.

View and Sort the Following Attributes Lists

- **Name**
- **Display Name**—The attribute name (with no spaces).
- **Type**—The format that users must enter or select values.
- **Default Value**—Select the default value that displays in the Attributes list. Default values can be substituted by other variables. See "Use Substitution Variables in Policies and Scripts" on page 202.
- **Mandatory**—The value of attributes that are marked as mandatory is required when you create a new or add a device, device group, create a policy, and create a script.
- **Inheritable**—Applies specifically to devices and device groups. When this is selected, the device or device group inherits attributes from its parent device group.
- **Description**—Describes the attribute and must be specific to the device, device group, policy, or script to which you are applying the attribute.

You are able to search for specific objects based on the attributes you define. See "Filter by Attributes and Keyword Search" on page 167.
Change the Order in which Policy Rules are Evaluated

You can change the order of the sections in policy, which in turn changes policy behavior. The CPL is evaluated from top to bottom—lower layers override higher layers; thus, the order of sections affects the order in which policy rules in each section are evaluated. Changing the order of policy sections can alter the effectiveness of policy, result in a rule overriding other rules, or cause unintended behaviors. See the following examples.

1. Select **Configuration > Policy**.
2. In the **Policy Objects** list, select the policy. If needed, search for the object; see "Filter by Attributes and Keyword Search" on page 167.
3. (Recommended) To collapse a section, click the  at the left of the title bar. You can click the  on the title bar of a collapsed section to expand it.
4. Hover over the title bar of the section you want to move. The pointer changes to a . Drag the section to its new location.

   Alternatively, you can use the selection arrows  and  in the title bar to move the section up or down, respectively.

5. Move sections around in the policy object until you are satisfied that the policy will evaluate as you intend. If the policy has many sections, you can use the **Quick Navigation** pane on the right to quickly go to the section you want. See "Work with CPL Policy Sections" on page 196 for instructions.

   A red asterisk (*) beside the policy object name denotes pending changes.

6. Click **Save**.

Example

The following is a basic example of how changing the order of sections can change the behavior of policy.

Consider a policy section with the purpose **Threat protection - Inbound Policy**. It contains the following CPL:

```xml
; Deny EXE downloads
url.extension=.exe DENY
```

Another policy section has the purpose **Access Control**. It contains the following CPL:

```xml
; Users in specified subnet are allowed transactions
client.address=192.0.2.0/24 ALLOW
```

Refer to the following table to see how the order of policy sections can affect the behavior of policy.
### Order of policy sections

<table>
<thead>
<tr>
<th>Order of policy sections</th>
<th>How policy is evaluated</th>
<th>Resulting behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Threat protection - Inbound Policy</td>
<td>The Access Control section overrides the Threat protection section.</td>
<td>Everyone in the network is denied EXE downloads except for users in the specified subnet.</td>
</tr>
<tr>
<td>2. Access Control</td>
<td>The Threat protection section overrides the Access Control section.</td>
<td>Users in the specified subnet are allowed transactions with the exception of EXE downloads; everyone in the network is also denied EXE downloads.</td>
</tr>
</tbody>
</table>

### Use Substitution Variables in Policies and Scripts

Substitution variables are generic terms (like attributes or shared objects) that you can include in policies and scripts. These terms are attributes you might have setup on your devices, groups, etc. When Management Center installs policy or executes a script that includes substitution variables, it attempts to replace them with values specific to the current transaction—that is, the current device, policy, or script. For example, if you install policy that includes the substitution variable `${device.name}`, the variable is replaced with the device name set in Management Center.

### Use in Shared Policy

When you include shared policy objects in your policy, you must enable variable substitution or the shared object’s CPL will not be substituted for the `include` variable. For example, if you create a URL list called `whitelist` and include it in a policy object, the system creates the CPL entry `@(include:whitelist)`. The `whitelist` URL list will only be included if `Replace substitution variables` is selected when the policy is installed.

While you may use substitution variables in CPL layers, Management Center performs the substitution when installing the CPL to the device. The UI markup (XML) remains unchanged. Therefore, if you open the installed VPM policy locally from the ProxySG appliance and try to install it, the substitution variables will not be replaced in the resulting CPL (because this workflow bypasses Management Center). This could result in malformed or unexpected policy, depending on how the variables are being used.

### To include and process substitution variables:

1. Verify that `Replace substitution variables` is enabled in the policy object (see [Create a CPL Policy Object](#)) or script (see [Create and Distribute Configurations Using Scripts](#)).

2. Include substitution variables in the CPL or script. See "Supported Variables" on the facing page below.

3. Install the policy or execute the script. As the target device processes the policy or script, it attempts to replace the variables with the appropriate values.

If the policy or script is associated with a device group, Management Center inspects every device in the group structure for the variable and attempts to replace all instances with specific values.
### Syntax

Substitutions have the following form:

\[ \${name} \]

where \( name \) is an expression that expands to a string or block of text at runtime.

For example, the substitution \( \${device.description} \) expands to the description entered in the current device's properties in Management Center.

If the device does not have a description (because Description is an optional field), the substitution expands to an empty string unless you also specify a default value. See "Specify a Default Substitution Value" on page 205 below for details.

### Examples

Substitute the device's serial number.

\( \${device.serialNumber} \)

Substitute the value of the device's Rack attribute.

\( \${device.attributes.Rack} \)

Substitution variables are case-sensitive. To ensure that you have entered them with correct spelling and case, use the Preview option before installing policies or executing scripts. The preview warns you if a substitution variable is invalid.

### Supported Variables

#### Device - \( \${device.field} \)

The following variables are available for policies and scripts.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${device.memberOf}</td>
<td>List of the groups to which a device is assigned</td>
</tr>
<tr>
<td>${device.uuid}</td>
<td>Internal ID of device</td>
</tr>
<tr>
<td>${device.modelNumber}</td>
<td>Device model number</td>
</tr>
<tr>
<td>${device.description}</td>
<td>Text in the Description field in device properties in Management Center</td>
</tr>
<tr>
<td>${device.name}</td>
<td>Text in the Device Name field in device properties in Management Center</td>
</tr>
<tr>
<td>${device.serialNumber}</td>
<td>Device's serial number</td>
</tr>
<tr>
<td>${device.osVersion}</td>
<td>Operating system version running on the device</td>
</tr>
<tr>
<td>${device.type}</td>
<td>The device type, for example, ProxySG.</td>
</tr>
<tr>
<td>${device.attributes.name}</td>
<td>System or user-defined device attribute value, including any values inherited from the device group</td>
</tr>
</tbody>
</table>

where \( name \) is the attribute name

#### Device Connection - \( \${device.connection.field} \)

The following variables are available for policies and scripts. A variable might not be applicable to every device.
### Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${device.connection.host}</code></td>
<td>Host IP address</td>
</tr>
<tr>
<td><code>${device.connection.port}</code></td>
<td>Port number</td>
</tr>
<tr>
<td><code>${device.connection.connectionType}</code></td>
<td>Designates the way the connection is established and optionally how authentication is performed. For example, <strong>SSH_PUBLIC_KEY</strong> <strong>PRODUCTION</strong> or <strong>PREPRODUCTION</strong></td>
</tr>
<tr>
<td><code>${device.connection.network}</code></td>
<td></td>
</tr>
<tr>
<td><code>${device.connection.username}</code></td>
<td>User name for authentication. Only relevant for ProxySG/ASG when credentials are used.</td>
</tr>
</tbody>
</table>

### Policy - `${policy.field}`

The following variables are available for policies only (not scripts).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${policy.author}</code></td>
<td>Last user who edited and saved the policy</td>
</tr>
<tr>
<td><code>${policy.description}</code></td>
<td>Text in the Description field in policy properties</td>
</tr>
<tr>
<td><code>${policy.name}</code></td>
<td>Text in the Name field in policy properties</td>
</tr>
<tr>
<td><code>${policy.referenceId}</code></td>
<td>Text in the Reference Id field in policy properties</td>
</tr>
<tr>
<td><code>${policy.revision}</code></td>
<td>Policy’s current Version number</td>
</tr>
<tr>
<td><code>${policy.revisionDescription}</code></td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td><code>${policy.attributes.name}</code></td>
<td>User-defined policy attribute value</td>
</tr>
</tbody>
</table>

### Policy Fragment- `${fragment.field}`

The following variables are available for policy fragments.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${fragment.author}</code></td>
<td>Last user who edited and saved the policy</td>
</tr>
<tr>
<td><code>${fragment.description}</code></td>
<td>Text in the Description field in policy fragment properties</td>
</tr>
<tr>
<td><code>${fragment.name}</code></td>
<td>Text in the Name field in policy fragment properties</td>
</tr>
<tr>
<td><code>${fragment.referenceId}</code></td>
<td>Text in the Reference Id field in policy fragment properties</td>
</tr>
<tr>
<td><code>${fragment.revision}</code></td>
<td>Policy fragment’s current Version number</td>
</tr>
<tr>
<td><code>${fragment.revisionDescription}</code></td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td><code>${fragment.attributes.name}</code></td>
<td>User-defined policy fragment attribute value</td>
</tr>
</tbody>
</table>

### Script - `${script.field}`
The following variables are available for scripts only (not policies).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${script.author}</code></td>
<td>Last user who edited and saved the script</td>
</tr>
<tr>
<td><code>${script.description}</code></td>
<td>Text in the Description field in script properties</td>
</tr>
<tr>
<td><code>${script.versionDate}</code></td>
<td>Date of last update</td>
</tr>
<tr>
<td><code>${script.name}</code></td>
<td>Text in the Name field in script properties</td>
</tr>
<tr>
<td><code>${script.type}</code></td>
<td>Selected Type in script properties</td>
</tr>
<tr>
<td><code>${script.revision}</code></td>
<td>Script's current Version number</td>
</tr>
<tr>
<td><code>${script.revisionDescription}</code></td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td><code>${script.attributes.name}</code></td>
<td>User-defined script attribute value</td>
</tr>
<tr>
<td>where name is the attribute name</td>
<td></td>
</tr>
</tbody>
</table>

Specify a Default Substitution Value

Unless you specify a default value, some transactions can produce unsubstituted variables, resulting in empty strings. The following are examples of such transactions:

- An optional field such as Description is empty
- An attribute that is not marked as mandatory has no value
- A field is not applicable, such as when a script or policy has not been revised

Syntax

A default substitution has the following form:

$\{name(default_name)\}$

where:

- name is an expression that expands to a string or block of text at runtime
- default_name is the value that will be used instead of an unsubstituted variable

Example

If a policy fragment was edited, use the comments entered for the last revision. If the fragment was never edited, use the specified text "No revision".

$\{fragment.revisionDescription(No revision)\}$

Use Regular Expressions

Policy and script processing can make use of Regular Expressions (RegEx).

Syntax

regex

Example
RegEx can be used in variables to produce generic results as follows:

```
${device.osVersion;regex(SGOS (.*))} will return just the number portion of SGOS version for SG devices
```

And RegEx can be used as part of a condition with specific strings:

```
${device.osVersion;regex(SGOS (.*))="6.7.3.100"} will test for the specific version of SGOS.
```
Launch Visual Policy Manager

This topic describes the requirements for running the Visual Policy Manager (VPM). Refer to the ProxySG appliance Visual Policy Manager Reference for information on constructing policy using the VPM. This topic assumes that you are familiar with those steps.

VPM Requirements

- When using the VPM editor, Symantec recommends that you use the recommended Java version listed [here](https://support.symantec.com/content/dam/bluecoat/download/modules/security/SGv6/policyclassifier.xml).

  Releases prior to Java 1.8 use a vulnerable cryptographic hash (SHA1) function that Management Center no longer supports. If you are using Java 1.8.131 or later, you will need to upgrade the ProxySG to SGOS version 6.6.4 (or later) or 6.7.2 (or later) to launch the VPM editor. Versions prior to these SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.

- If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command. See "# security" on page 617 for more information.

- Before using the VPM editor in Management Center, Symantec strongly recommends that you understand how the VPM Editor works and underlying policy enforcement in ProxySG appliances. For comprehensive information on creating policy policy, as well as assigning and changing enforcement domains for policy rules in the VPM, refer to the ProxySG Appliance Visual Policy Manager Reference and Advanced Policy Tasks.

- Ensure that you have the latest VPM resource XML file installed on your ProxySG. You can download the XML file from the Symantec Support site: https://support.symantec.com/content/dam/bluecoat/download/modules/security/SGv6/policyclassifier.xml

Launch the VPM

1. Select **Configuration > Policy**. From the Policy Objects list, locate the VPM policy object you want to edit. To narrow your search, you can do a "Filter by Attributes and Keyword Search" on page 167.

   To add a new VPM policy object, refer to Add a VPM Policy Object.

2. Click the policy name hyperlink or highlight the row and click **Edit**. Verify that you are in the **Editor** tab.
3. If necessary, import policy from the reference device. Click **Import**. See "Select Reference Device for VPM Policy" on page 212.
4. Click **Launch VPM Editor**. When the system displays the following message, click **Run**.
5. If you see a Security Warning, check the IP address and click **Continue**.

6. The web console displays the Visual Policy Manager.

7. Add layers and rules, as required by your policy.

8. Click **Save policy** when finished. The edited policy displays in the Policy Objects list with an updated revision number.

---

If Java is not enabled on your browser, the VPM Editor cannot launch. See “Set Up and Enable Java in Your Browser” on the facing page.
Set Up and Enable Java in Your Browser

When using the VPM editor, Symantec recommends that you use the recommended Java version listed [here](#).

Releases prior to Java 1.8 use a vulnerable cryptographic hash (SHA1) function that Management Center no longer supports. If you are using Java 1.8.131 or later, you will need to upgrade the ProxySG to SGOS version 6.6.4 (or later) or 6.7.2 (or later) to launch the VPM editor. Versions prior to these SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.

If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command. See "# security" on page 617 for more information.

1. From your browser, install the recommended Java version. Enable Java in your browser. Because every browser behaves differently, confirm that the correct Java version is installed and enabled by using your browser to go to: [https://www.java.com/verify](https://www.java.com/verify)

   You may need to restart your browser after updating Java.

   Note: Some browsers no longer support Java.

2. After you have verified that your Java version is correct and a reference device is available, the Launch VPM Editor button is enabled.

3. Click Launch VPM Editor to open the Visual Policy Manager Editor. However, the following error can occur:

   ![Error Message]

   If you see this error after relaunching the VPM Editor it means that you need to allow java to run in your browser and accept the certificates that Java requires.
Launch Visual Policy Manager

This topic describes the requirements for running the Visual Policy Manager (VPM). Refer to the ProxySG appliance Visual Policy Manager Reference for information on constructing policy using the VPM. This topic assumes that you are familiar with those steps.

VPM Requirements

- When using the VPM editor, Symantec recommends that you use the recommended Java version listed here.

  Releases prior to Java 1.8 use a vulnerable cryptographic hash (SHA1) function that Management Center no longer supports. If you are using Java 1.8.131 or later, you will need to upgrade the ProxySG to SGOS version 6.6.4 (or later) or 6.7.2 (or later) to launch the VPM editor. Versions prior to these SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.

- If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command. See "# security" on page 617 for more information.

- Before using the VPM editor in Management Center, Symantec strongly recommends that you understand how the VPM Editor works and underlying policy enforcement in ProxySG appliances. For comprehensive information on creating policy policy, as well as assigning and changing enforcement domains for policy rules in the VPM, refer to the ProxySG Appliance Visual Policy Manager Reference and Advanced Policy Tasks.

- Ensure that you have the latest VPM resource XML file installed on your ProxySG. You can download the XML file from the Symantec Support site: 
  https://support.symantec.com/content/dam/bluecoat/download/modules/security/SGv6/policyclassifier.xml

Launch the VPM

1. Select Configuration > Policy. From the Policy Objects list, locate the VPM policy object you want to edit. To narrow your search, you can do a "Filter by Attributes and Keyword Search" on page 167.

   To add a new VPM policy object, refer to Add a VPM Policy Object.

2. Click the policy name hyperlink or highlight the row and click Edit. Verify that you are in the Editor tab.

3. If necessary, import policy from the reference device. Click Import. See "Select Reference Device for VPM Policy" on page 212.

4. Click Launch VPM Editor. When the system displays the following message, click Run.
5. If you see a Security Warning, check the IP address and click Continue.

6. The web console displays the Visual Policy Manager.

7. Add layers and rules, as required by your policy.

8. Click Save policy when finished. The edited policy displays in the Policy Objects list with an updated revision number.

If Java is not enabled on your browser, the VPM Editor cannot launch. See "Set Up and Enable Java in Your Browser" on page 209.
Select Reference Device for VPM Policy

The reference device is the device you designate as the source device for VPM policy configurations. You must select a reference device to launch the VPM editor.

1. Select **Configuration > Policy**. From the Policy Objects list, select a VPM policy. Click **Edit**.

   A default reference device is not automatically populated. Associate a least one deployed device with the policy or manually configure a reference device to enable editing.

2. While the **Editor** tab is selected, select a Reference Device, using the object selector 🖋. Resolve displayed warnings before launching the VPM editor. The Launch VPM Editor button is grayed out if warnings ⚠️ are present.

3. To associate a reference device, from the Select Device dialog, select the check box by the device that you want to use as a reference. The selected device automatically displays in the Selected view. Click **OK**.
4. (Optional) You can create and edit a VPM policy as soon as you have selected a reference device and no warnings are displayed. Click **Launch VPM Editor**.

### Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove devices associated with the policy.</td>
<td>&quot;Add or Remove Devices Associated with Policy&quot; on page 326</td>
</tr>
<tr>
<td>Restore a version of the policy.</td>
<td>&quot;Restore a Version of Policy&quot; on page 335</td>
</tr>
<tr>
<td>Create and edit a VPM policy using the VPM Editor.</td>
<td>&quot;Launch Visual Policy Manager&quot; on page 210</td>
</tr>
<tr>
<td>Import a policy configuration from a device.</td>
<td>&quot;Import Policy or Shared Objects&quot; on page 308</td>
</tr>
</tbody>
</table>

### View VPM Policy Source

Management Center enables you to view the CPL or XML policy source of a VPM policy.

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the VPM policy name.
   
   If needed, search for the policy object; see "Filter by Attributes and Keyword Search" on page 167.
3. With the policy selected, click **Editor**. The system displays the editor.
4. View the policy:
5. (Optional) **Edit** the policy.

### Restrict Access Only to a Specific Object Included in a VPM Layer

This topic describes how to restrict user access to an object included in the VPM Web Access Layer. The intention of the policy is to allow users to edit the whitelist, but preclude them from altering other policy in the VPM.

Although this can be accomplished with CPL, it is easier to create a shared object, restrict access to that object, and then include the object in the VPM policy.

**Step 1—Create the URL List Object**

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose **URL List**.
c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.

   - The Reference ID must begin with a letter and must contain only letters, numbers, and "_".

d. **Description** - Enter a meaningful description to help you when reusing this fragment.

4. Click **Next**. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See "Add Attributes" on page 401.

5. Click **Finish**. The URL list displays in the editor.

**Step 2—Add URLs**

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired URL list. The system displays the URL list editor.
3. Enter the URL in the **URL** field and click **Add**.
The system displays the text entered into the Description field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:
   a. Create a URL list and copy the URLs.
   b. Click Paste URLs. The system opens the Paste URLs: Enter URLs dialog.
      c. Copy the URLs into the Paste URLs: Enter URLs dialog. Press CTRL+V or right-click and click Paste. The URLs are added to the list.
      d. Click Next. The system opens the Paste URLs: Validate dialog.
      e. Click Finish.

5. Click Save.

Step 3—Add a Whitelist Editing Role

1. Select Administration > Roles and click Add Role.

2. In the Add Role: Basic Info dialog, enter a name for the role. In this example, you might use "Whitelist Editor."
   If you authenticate users against LDAP, Active Directory or RADIUS, create a role in sync with the directory service.

3. (Optional) Enter a description.

4. Click Next.

5. In the Add Role: Permissions dialog, click Add Permission.

6. From the Object drop-down list, select Policy.

7. From the Action drop-down list, delete All Operations and select Edit Contents.

8. In the Filter drop-down list, select the URL whitelist you created in steps 1 and 2.
9. Click **Finish**.

**Step 4—Assign Users to the Whitelist Editing Role**

1. Select **Administration > Users**.
2. In the **Users** left pane, select the user whose roles you want to change. The user's details display.
3. Click **Edit**. The web console displays the Edit User dialog.
4. Click **Assign Roles**. The dialog displays a list of all the roles in the system. Roles to which the user is not assigned are listed under **Available Roles**. Roles to which the user is currently assigned are listed under **Assigned Roles**.
5. Select the **Whitelist Editor** role from **Available Roles** and, using the arrow, add it to the **Assigned Roles** list.
Management Center Configuration & Management

6. Click **Save**. The web console banner displays an alert indicating that the user was saved.

Roles are linked to user sessions. If you edit users’ roles while they are logged in to the web console, instruct them to log out and log in again to see the effects of the change.

---

**Step 5—Create the VPM Policy Object**

Skip to step 6 if you are going to add your URL list to an existing policy object.

To add a VPM policy object, complete the following steps.

1. Select **Configuration > Policy**.
2. Click **Add Policy**. The system displays the Create New Policy: Basic Information dialog. An asterisk denotes fields that are mandatory.
3. Enter a name for the policy object.
4. Select **VPM** for the **Policy Type**.
5. Enter a **Reference ID**. Although entering a reference ID is not required, it is useful for filtering objects when building policy. If you do not enter a reference ID, the system assigns a default ID based on the policy name you enter. Imported policy objects are assigned a default ID.
   
   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".

6. Enter a description in the **Description** field. Although entering a description is not required, the description helps differentiate versions of the same policy.
7. If you are to include shared objects, verify that **Replace Substitution Variables** is enabled. See "Use Substitution Variables in Policies and Scripts" on page 202 for more information.
8. Click **Next**.
9. Enter or select values for the defined attributes.
10. Click **Finish**.

---

**Step 6—Add the URL List to the VPM Policy**

On the desired line number, right click the field under **Destination** and select **Set** from the menu.

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Click the **Included Objects** tab.
4. Any lists already included in the policy show on the **Included Objects** list. You may only reference shared objects if they are associated with the policy. To add available lists:
   
   a. Click **Add Object**.
   b. Select the additional lists to add to the policy, then click **OK**.

   You can search for lists using the **Keyword Search**.

5. Make note of the reference ID for the object(s) you want to set.
6. (Optional) If you want to limit the lists to specific revisions in order to avoid unintentional changes, you can lock the revision version.
a. Select an object.
b. Click **Select Version**.
c. Select **Use specific version**.
d. Select the version number from the menu.
e. Click **Save**.

7. (Optional) Select any lists to remove and click **Delete**.

---

If any of the lists are in use, you need to launch the VPM Editor to remove or change the rules that reference them in the policy.

---

8. Once finished editing the available shared objects for the policy, click **Save**.
9. Click **Launch VPM Editor**.
10. Select or create the desired policy layer.
11. On the desired line number, right click the field under **Destination** and select **Set** from the menu.

---

12. Select the desired list:
By the reference ID from the objects list.

For a category, select any VPM object that lists categories. In this example, a new Request URL Category object is selected.
Shared objects are read-only. You cannot use the **Edit** option when setting the destination object. If you do try to edit it, it gets overwritten it the next time you open the VPM editor.

13. (Optional) Set the desired action condition by right-clicking under the **Action** field.
14. When finished setting the destination and conditions, click **Save policy**. (Optional) To exit the VPM Editor without saving changes, close the VPM Editor and then click **Do not Save Policy**.
15. Enter a brief description of the policy changes in the **Save Changes** field, click **OK**, then click **Close**.
16. Close the VPM Editor.
17. Back in Management Center, on the VPM policy, click the **Info** tab.
18. Ensure that **Replace substitution variables** is selected, then click **Save**.

For more information about adding or editing VPM Shared Objects, see **Create Shared Objects**.

You are now ready to install the policy. From this point on, any user with the correct permissions can edit the list as needed without having to open the VPM.

**Create Shared Objects**

Shared objects are policy elements that can be referenced by multiple policy objects. A shared object cannot be deployed by itself; it must be included in another policy type, such as CPL or a WAF Application.

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit ${include} and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

Users are warned if they attempt to delete a shared object currently assigned to a policy object. The error message lists all policies to which the shared object is assigned. When presented with the message, the user must confirm the deletion by selecting **I understand that once I choose to delete the Object above, this action cannot be undone**.

**Create CPL Fragments**

CPL policy fragments are reusable building blocks of CPL policy. Because fragments are not complete CPL policy, you do not deploy them to devices but include them within policy that you deploy to devices.

"Create a CPL Policy Fragment" on page 223

"Include a Shared Policy Object in CPL or VPM Policy" on page 232

**Create a Category List**

A **category list** is a named set of URL categories that can be easily referenced in policy, allowing you to assign an allow or deny condition to all the categories in one simple rule, or reuse the list in multiple policy rules.

"Create Category Lists" on page 237

"Category List Example" on page 240

**Create a Category List Template**
A category list template provides a starting point for defining which categories to include in a category list. The template contains a subset of the complete list of WebPulse categories, typically used to restrict the categories a less-privileged user can select when creating a category list.

"Use Category List Templates" on page 247

Create a URL List

URL lists allow you to easily create URL exceptions to your policy. The URL list can be easily included in your existing policy.

"Create URL List (URL Policy Exceptions)" on page 224
"URL List Example" on page 227

Create an IP Address List

Easily create IP address lists for use on the SSL Visibility appliance.

"Create SSL Visibility IP Address List " on page 277

Manage List Triggers

When you create a URL or category list, Management Center includes subconditions and associated triggers optimized for the type of URL or category entered. These triggers are enabled by default but you have the option to disable some of them.

"Manage URL and Category List Triggers" on page 230

Create WAF Security Profile

A WAF Security Profile is a shared object that defines the Web Application Firewall settings for the associated WAF application object. The WAF Security Profile is assigned to one or more WAF applications that can be installed on ProxySG appliances to set WAF policy.

"Configure WAF Security Rules " on page 141

Creating a WAF Security Profile is step 3 in "Use WAF Policy To Protect Servers From Attacks" on page 130.
Create a CPL Policy Fragment

CPL fragments are shared objects. Like other shared objects, Policy fragments are reusable building blocks of CPL policy. Because fragments are not complete CPL policy, you do not deploy them to devices but include them within policy that you deploy to devices. Create a CPL Policy Fragment in the same way that you create CPL Policy.

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit $\{\text{include}\}$ and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard. Fill in required fields. An asterisk denotes fields that are mandatory.
   - **Object name** (*) - Required name
   - **Object type** (*) - From the drop-down list, choose CPL Fragment.
   - **Reference ID** (*) - Enter a Reference ID that you can filter on when building policy.
     - The Reference ID must begin with a letter, and must contain only letters, numbers and "_".
   - **Description** - Enter a meaningful description to help you when reusing this fragment.
   - **Replace substitution variables** - select this if you want to replace specific values within the policy fragment. See "Use Substitution Variables in Policies and Scripts" on page 202.

If Replace substitution variables is NOT selected when creating a CPL Policy, the CPL Policy
3. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See "Add Attributes" on page 401.
5. To add the fragment to policy, see Include a Policy Fragment.

**Create URL List (URL Policy Exceptions)**

URL lists allow you to easily create URL lists for use in policy. These lists can then be included in your existing policy for ProxySG or SSL Visibility appliances. An example implementation is described here.

URL lists are shared objects. Because URL lists are not complete policy, you do not deploy them to devices but include them within policy that you deploy to devices.

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit $${include}$$ and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

URL lists include policy triggers that you may want to disable to improve performance.

**Step 1 - Create the URL List Object**
1. Select **Configuration > Shared Objects**.

2. Click **Add Object**. The web console displays the Create New Shared Object wizard.

3. Fill in required fields. An asterisk denotes fields that are mandatory.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose **URL List**.

   ![Create New Shared Object: Basic Information](image)

   c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.

   The Reference ID must begin with a letter and must contain only letters, numbers, and ".".

   d. **Description** - Enter a meaningful description to help you when reusing this fragment.

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See "Add Attributes" on page 401.

5. Click **Finish**. The URL list displays in the editor.

**Step 2 - Add URLs**

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired URL list. The system displays the URL list editor.
3. Enter the URL in the **URL** field and click **Add**.
Management Center Configuration & Management

The system displays the text entered into the Description field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:
   a. Create a URL list and copy the URLs.
   b. Click Paste URLs. The system opens the Paste URLs: Enter URLs dialog.
   c. Copy the URLs into the Paste URLs: Enter URLs dialog. Press CTRL+V or right-click and click Paste. The URLs are added to the list.
   d. Click Next. The system opens the Paste URLs: Validate dialog.
   e. Click Finish.
5. Click Save.

Enabling and Disabling URLs
You can disable an individual URL by selecting it and clicking Disable.
You can enable a URL by selecting it and clicking **Enable**.

**Step 3 - Include the URL List in Policy**

When you have completed your changes, you can include the URL list in CPL, as described in "Include a Shared Policy Object in CPL or VPM Policy" on page 232. The URL list will be included in the CPL as a named condition that can then be referenced using `condition=referenceId`. See the example below for details.

You can then install your policy as described in "Install Policy" on page 302.

**Whitelist Scenario Example**

**URL List Example**

In this example, the administrator has created a simple acceptable use policy and would like to allow some URLs that would otherwise be blocked.

```plaintext
Define subnet corporate_subnet
    198.51.100.0/24
end

<proxy "Web Access">
    client.address=corporate_subnet  ALLOW
</proxy>

<proxy "Web Auth">
    authenticate(corp_realm)
</proxy>

<proxy "Web Filter">
    url.domain=playboy.com  FORCE_DENY
    category=(gambling, hacking, games, news)  exception(content_filter_denied)
</proxy>

<proxy "Restricted Access">
    group=execs, managers  url.domain=fantasyfootball.com  ALLOW
</proxy>
```

This CPL is stored in a policy object called **ASUP**. The **ASUP** policy object has **Replace substitution variables** enabled.

Though the URL filtering blocks all news sites, she would like to allow cnn.com, yahoo.com, and nytimes.com. To allow these sites, the administrator does the following.

**Step One - Create the URL List Object**

1. Selects **Configuration > Shared Objects**.
2. Clicks **Add Object**. The web console displays the Create New Shared Object wizard.
3. Enters the following data:
   a. Object name: **whitelist**
   b. Object type: **URL List**
   c. Reference ID: autofill
   d. Description: **List of allowed URLs**
4. Clicks **Next**.
5. Clicks **Finish**.
Step Two - Add Allowed URLs

1. In the whitelist policy editor, the administrator enters cnn.com in the URL field and clicks Add.
2. Adds yahoo.com and nytimes.com, as described in the preceding step.
3. Clicks Save and enters a brief description of the change. The whitelist object now looks like this.

<table>
<thead>
<tr>
<th>Enabled</th>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>cnn.com</td>
<td>Added on 1/05/2017</td>
</tr>
<tr>
<td>✓</td>
<td>yahoo.com</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>nytimes.com</td>
<td></td>
</tr>
</tbody>
</table>

Step Three - Add the URL List to the ASUP Policy

1. Selects Configuration > Policy > ASUP. The ASUP policy opens in the editor. Remember that the administrator has previously enabled Replace substitution variables.
2. Clicks Operations > Insert > Insert Include.
3. In the Insert Policy Include window, selects whitelist and clicks OK.

The ASUP CPL now looks like this:

```cpl
Define subnet corporate_subnet
198.51.100.0/24
end

${include:whitelist}

<proxy "Web Access">
    client.address=corporate_subnet  ALLOW
</proxy>

<proxy "Web Auth">
    authenticate(corp_realm)
</proxy>

<proxy "Web Filter">
    url.domain=playboy.com  FORCE_DENY
    category=(gambling, hacking, games, news)  exception(content_filter_denied)
</proxy>

<proxy "Restricted Access">
    group=execs, managers  url.domain=fantasyfootball.com  ALLOW
</proxy>
```

When the administrator previews the policy, it looks like this:
Define subnet corporate_subnet
  198.51.100.0/24
end

define url.domain condition whitelist/url_domains
cnn.com
  yahoo.com
  nytimes.com
end

define condition whitelist/certificate_hostnames
  server.certificate.hostname=cnn.com
  server.certificate.hostname=yahoo.com
  server.certificate.hostname=nytimes.com
end

define condition whitelist
  condition=whitelist/url_domains
  condition=whitelist/certificate_hostnames
end

<proxy "Web Access">
  client.address=corporate_subnet  ALLOW
</proxy>

<proxy "Web Auth">
  authenticate(corp_realm)
</proxy>

<proxy "Web Filter">
  url.domain=playboy.com  FORCE_DENY
  category=(gambling, hacking, games, news)  exception(content_filter_denied)
</proxy>

<proxy "Restricted Access">
  group=execs, managers  url.domain=fantasyfootball.com  ALLOW
</proxy>

---

The name of the condition corresponds to the shared object's reference ID, not its name. You can preview the policy by going to the Targets tab, adding a target, selecting the target, and clicking Preview.

Though the URLs have been defined, they have not been added as a rule.

4. To create the rule, the administrator adds the following rule to the CPL to implement the whitelist:

condition=whitelist ALLOW

See example below.

```
<proxy "Web Filter">
  url.domain=playboy.com  FORCE_DENY
  condition=whitelist ALLOW
  category=(gambling, hacking, games, news)  exception(content_filter_denied)
</proxy>
```

5. Clicks Save.

The ASUP CPL is now ready to be pushed to target devices.
Manage URL and Category List Triggers

The policy rules that are created when you generate CPL for a URL or category list consist of a subcondition and a trigger.

A condition (or subcondition) is a boolean combination of trigger expressions. Triggers are individual tests that can be made against components of the request. With a few notable exceptions, triggers test one aspect of request, response, or associated state against a boolean expression of values. For more information about CPL conditions and triggers, refer to the Content Policy Language Reference.

When you create a URL or category list, Management Center includes subconditions and associated triggers optimized for the type of URL or category entered. These triggers are enabled by default but you have the option to disable some of them. You might want to disable a trigger to improve performance for long lists, for example.

URL List Triggers

The included URL list subconditions and triggers are described in the following table.

<table>
<thead>
<tr>
<th>Subcondition</th>
<th>Associated Trigger</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_name/url.domains</td>
<td>url.domain</td>
<td>example.com/us example.com</td>
</tr>
<tr>
<td></td>
<td>All URLs that have been entered are included in this subcondition.</td>
<td>example.com/us</td>
</tr>
<tr>
<td></td>
<td>You cannot disable this subcondition.</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td>list_name/certificate_hostnames</td>
<td>server.certificate.hostname</td>
<td>example.com</td>
</tr>
<tr>
<td></td>
<td>URLs that do not specify a path are included in this subcondition. The associated trigger examines the SSL certificate to detect the host that is being visited.</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td></td>
<td>Server.certificate.hostname is used to match policy against HTTPS URLs, where the ProxySG can only see the SSL certificate presented by the OCS. Transparent proxy deployments that don't use SSL interception will need this to match policy against this URL list. Without it, the ProxySG will never be able to match requests against the standard url.domains subcondition, as the ProxySG only sees the OCS IP address and certificate; not the hostname in the client's request.</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td></td>
<td>You can disable this subcondition.</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td>list_name/addresses</td>
<td>url.address</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td></td>
<td>All IP addresses that have been entered are included in this subcondition.</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td></td>
<td>url.address allows the ProxySG to compare an IP-address-based URL list entry to the server's IPv4 address.</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td></td>
<td>You can disable this subcondition.</td>
<td>198.51.100.10</td>
</tr>
</tbody>
</table>

Category List Triggers

The included category list subconditions and triggers are described in the following table.
### Disable URL or Category List Triggers

1. Select **Configuration > Policy > Shared Objects** and edit the URL or category list.
2. Click the gear icon to open the Advanced Settings dialog.
3. Disable the desired triggers and click **Save**.

---

<table>
<thead>
<tr>
<th>Subcondition</th>
<th>Associated Trigger</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_name/category</td>
<td>category</td>
<td>category='Adult/Mature Content'</td>
</tr>
<tr>
<td></td>
<td>Matches the content categories using the requested URL.</td>
<td></td>
</tr>
<tr>
<td>list_name/cert_category</td>
<td>server.certificate.hostname.category</td>
<td>server.certificate.hostname.category='Adult/Mature Content'</td>
</tr>
<tr>
<td></td>
<td>Matches the category using the hostname in the server certificate. This applies only to SSL connections; the associated trigger examines the SSL certificate to detect the category associated with the hostname that is being visited.</td>
<td></td>
</tr>
</tbody>
</table>
Include a Shared Policy Object in CPL or VPM Policy

Use the CPL or VPM to reference policy fragments (such as URL lists, IP address lists, categories, category lists, and CPL fragments). CPL fragments are shared objects. Because fragments are not complete CPL policy, you do not deploy them to devices but include them within policy that you deploy to devices.

To learn about creating policy fragments, see "Create a CPL Policy Fragment" on page 223.

CPL Policy Fragments

Include a CPL fragment, URL list, or category list as a building block of CPL Policy.

1. Select Configuration > Policy.
2. In the Policy Objects list, select the CPL policy to which you want to add policy fragment. The policy is displayed in the Editor.
3. Click the Info tab.
4. Ensure Replace substitution variables is selected.

If you do NOT enable variable substitution in the CPL, the CPL Fragments will not be included.

5. Place the text cursor into the policy section where you want to include the policy fragment and select Operations> Insert > Insert Include. You can only include a fragment into an existing policy section. The web console displays the Select Policies dialog.
If you have not placed your cursor where you want to insert the policy fragment, Management Center displays the following error:

If you have not placed your cursor where you want to insert the policy fragment, Management Center displays the following error:

6. From the available policy fragments, select the shared object to include.

7. Click OK. The included policy fragment is displayed in the section where you placed your cursor. You can continue editing the CPL policy.
8. To commit your changes, click Save and enter a comment for the commit operation. The comment you enter is saved as policy metadata.

9. (Optional) To exit without saving your edits, click Cancel.

10. (Optional) Click Compare to see the differences between the existing policy version and the version you are about to commit.

For more information about adding or editing CPL Policy sections, see "Add or Edit CPL Policy Sections" on page 191.

VPM Shared Objects

Reference categories, category lists, IP address lists, and URL lists in a VPM policy. Categories added from Management Center are listed in under a custom Management Center provider. To view these click Configuration > Edit Categories... in the VPM. Management Center categories can be selected in any VPM object that lists categories, such as Request URL Category.

You cannot use this procedure to add CPL fragments. To add a CPL fragment, insert an include statement with the fragment’s reference ID into the VPM CPL layer. For example, ${include:whitelist}.

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit ${include} and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

On the desired line number, right click the field under Destination and select Set from the menu.
1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Click the **Included Objects** tab.
4. Any lists already included in the policy show on the **Included Objects** list. You may only reference shared objects if they are associated with the policy. To add available lists:
   a. Click **Add Object**.
   b. Select the additional lists to add to the policy, then click **OK**.

   ![You can search for lists using the Keyword Search.]

5. Make note of the reference ID for the object(s) you want to set.
6. (Optional) If you want to limit the lists to specific revisions in order to avoid unintentional changes, you can lock the revision version.
   a. Select an object.
   b. Click **Select Version**.
   c. Select **Use specific version**.
   d. Select the version number from the menu.
   e. Click **Save**.
7. (Optional) Select any lists to remove and click **Delete**.

   ![If any of the lists are in use, you need to launch the VPM Editor to remove or change the rules that reference them in the policy.]

8. Once finished editing the available shared objects for the policy, click **Save**.
9. Click **Launch VPM Editor**.
10. Select or create the desired policy layer.
11. On the desired line number, right click the field under **Destination** and select **Set** from the menu.

<table>
<thead>
<tr>
<th>SSL Intercept Layer (1)</th>
<th>CPL Layer (1)</th>
<th>Web Access Layer (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No.</strong></td>
<td><strong>Source</strong></td>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

12. Select the desired list:
Management Center Configuration & Management

- By the reference ID from the objects list.

![Set Destination Object](image)

- For a category, select any VPM object that lists categories. In this example, a new **Request URL Category** object is selected.

![Add Request URL Category Object](image)
Shared objects are read-only. You cannot use the Edit option when setting the destination object. If you do try to edit it, it gets overwritten the next time you open the VPM editor.

13. (Optional) Set the desired action condition by right-clicking under the Action field.
14. When finished setting the destination and conditions, click Save policy. (Optional) To exit the VPM Editor without saving changes, close the VPM Editor and then click Do not Save Policy.
15. Enter a brief description of the policy changes in the Save Changes field, click OK, then click Close.
16. Close the VPM Editor.
17. Back in Management Center, on the VPM policy, click the Info tab.
18. Ensure that Replace substitution variables is selected, then click Save.

For more information about adding or editing VPM Shared Objects, see Create Shared Objects.

"Filter by Attributes and Keyword Search" on page 167
- "Edit a Policy Section" on page 192
- "Add or Edit CPL Policy Sections" on page 191
- "View Existing Policy Information" on page 319

Work with Categories

Refer to the following topics:
- "Create Category Lists" below
- "Category List Example" on page 240
- "Use Category List Templates" on page 247
- "Create Custom Categories" on page 250
- "Custom Category Example" on page 253

Create Category Lists

A category list is a named set of URL categories that can be easily referenced in policy, allowing you to assign an allow or deny condition to all the categories in one simple rule, or reuse the list in multiple policy rules. Category lists are shared objects, and are similar to URL lists.

Go to sitereview.bluecoat.com and click Descriptions to see a list of current categories recognized by Symantec WebPulse. Note that the list of categories in Management Center may not exactly match the list on the website, but will be updated in a future Management Center release as necessary. For more information about content filtering by category, refer to the SGOS Administration Guide.

Category lists include policy triggers that you may want to disable to improve performance.

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit $include) and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

Step 1 - Create the Category List Shared Object

1. Select Configuration > Shared Objects.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.

3. Fill in required fields. An asterisk denotes fields that are mandatory.
   - **Object name** (*) - Required name
   - **Object type** (*) - From the drop-down list, choose **Category List**.

   ![Create New Shared Object: Basic Information](image)

   - **Reference ID** (*) - Enter a Reference ID (or accept the default name) will be used when building policy. The ID can be specified as the condition name in CPL.
     - The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
   - **Template** – If you (or someone else) has previously created a category list template, click and select the template. The template will restrict what categories can be defined in the list. See "Use Category List Templates" on page 247 for more information.
   - **Description** - Enter a meaningful description to help you identify this category list when including in policy.

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined any policy attributes, you can choose the attribute's value for this category list. See "Add Attributes" on page 401.

5. Click **Finish**. A tree of categories displays in the Editor tab. Note that the categories are grouped into folders (Business Related, Legal Liability, Non-Productive, and so forth) for organizational purposes—these folder names are not part of the policy.
If you selected a template, you may not see all folders and categories.

Step 2 - Select Categories

After you have created the category list object, you can select the categories associated with the list. The list should include all categories that you want to treat the same way in policy. For example, the categories in the list should all be ones that you would want to deny access to or allow access to; the actual policy action (deny/allow) will be defined in the policy.

1. The tree of category folders should be displayed in the Editor. If the list isn't currently displayed, select Configuration > Shared Objects and click the defined list name to bring it up in the Editor.
2. Select the categories you want to include in your list. Follow these general guidelines:
   - To see what categories are in a folder, click the + to expand.
   - Selecting a folder's checkbox selects all categories in that folder.
   - You can unselect any category within a selected folder by clicking its check box.
   - When a folder is expanded to display its categories, Management Center displays the category descriptions.
3. To view the category names assigned to this list, look at the Selected Categories panel at the bottom of the window.
4. Click **Save** and enter a brief description of the change.

**Step 3 - Include the Category List in Policy**

When you have defined the category list, you can include the object in CPL, as described in "Include a Shared Policy Object in CPL or VPM Policy" on page 232. In addition, you must create an allow/deny condition using `condition=referenceId`. See the "Category List Example" below for details.

You can then install your policy as described in "Install Policy" on page 302.

If you want to check into which category Symantec WebPulse categorizes a URL, go to [sitereview.bluecoat.com](http://sitereview.bluecoat.com) and enter the URL.

**Category List Example**

In this example, the administrator has created a simple acceptable use policy and would like to deny access to a list of categories that should not be allowed on the corporate network.
This CPL is stored in a policy object called ASUP. The ASUP policy object has **Replace substitution variables** enabled.

**Step One - Create the Category List Object**

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Enter the following data:
   a. Object name: **blacklisted_categories**
   b. Object type: **Category List**
   c. Reference ID: **blacklisted_categories**
   d. Template: (leave blank)
   e. Description: **a list of categories that should be denied in policy**
4. Click **Next**.
5. Click **Finish**.

**Step Two - Select Categories that Should be Denied**

The administrator would like to deny access to all legal liability categories and security threats, so she will select all the categories in the Legal Liability folder and Security Threats subfolder.

1. With a tree of available categories displayed in the Editor, click the Legal Liability check box. The Adult Related and Liability Concerns folders are also checked.
2. Click the + next to the Adult Related and Liability Concerns folders to display the category names, descriptions, and examples in these folders.
3. Expand the Security Threats folder to display the category names, descriptions, and examples in this folder.
4. Click the Security Threats check box to select all of its categories.
5. Click **Save** and enter a brief description of the change.

**Step Three - Add the Category List to the ASUP Policy**

1. Select **Configuration > Policy > ASUP**. The ASUP policy opens in the editor. Remember that the administrator has previously enabled **Replace substitution variables**.
2. Place the text cursor into the policy section where you want to include the category list and click **Operations > Insert > Insert Include**.
3. In the Insert Policy Include window, select `blacklisted_categories` and click OK.

The inserted CPL now looks like this:

```
${include:blacklisted_categories}
```

Though the category list has been defined, the condition still needs to be defined to deny access.

4. To create the condition to deny access to the category list named `blacklisted_categories`, the administrator adds the following line to the CPL:

```
condition=blacklisted_categories DENY
```
5. Click **Save**.
6. To preview the code that is generated for this policy, go to the **Targets** tab, select a device, and click **Preview**.
You can see in the preview that two conditions are created. The first condition (blacklisted_categories/url_category) just looks up the URL in WebPulse to find the category. The second condition (blacklisted_categories/cert_category)
is used for SSL connections—it can sometimes glean extra information by looking up the host name in the SSL certificate.

The ASUP CPL can be pushed to target devices at the appropriate time.

Use Category List Templates

A category list template provides a starting point for defining which categories to include in a category list. The template contains a subset of the complete list of WebPulse categories, typically used to restrict the categories a less-privileged user can select when creating a category list. For example, if you have a user with restricted permissions, you may not want him to control policy for any category—just particular ones that are appropriate for his role.

Create a Category Template

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   - **Object name** (*) - Required name
   - **Object type** (*) - From the drop-down list, choose Category List Template.
Management Center Configuration & Management

- **Reference ID** - Enter a Reference ID (or accept the default name).
  
  The Reference ID must begin with a letter and must contain only letters, numbers, and "_."

- **Description** - Enter a meaningful description to help you when applying this category list template.

4. Click **Next**. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute’s value for this category list. See “Add Attributes” on page 401.

5. Click **Finish**. A tree of categories is displayed.

6. Select the categories you want to include in the template. Follow these general guidelines:
   - To see what categories are in a folder, click the + to expand.
   - Selecting a folder’s check box selects all categories in that folder.
   - You can unselect any category within a selected folder by clicking its check box.
   - When a folder is expanded to display its categories, Management Center displays the category descriptions and examples as well.

   **Example**

```
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Liability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adult Related</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liability Concerns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Productive (32 of 32)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication (5 of 5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health Related (6 of 6)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leisure (6 of 6)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multimedia (4 of 4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Interaction (4 of 4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Society/Government (7 of 7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security (4 of 14)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Transfer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

7. To view the category names assigned to this template, look at the Selected Categories panel at the bottom of the screen.

8. Click **Save** and enter a brief description of the change.

**Use a Category List Template**

To use the category list template, select it when creating a category list. The user can only select categories from this
restricted list.

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   - **Object name** (*) - Required name
   - **Object type** (*) - From the drop-down list, choose **Category List**.

![Create New Shared Object: Basic Information](image)

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute’s value for this category list. See "Add Attributes" on page 401.
5. Click **Finish**. The Editor displays just the categories in the template, and the user can create a category list by choosing from the categories in the template.
6. Select the categories you want to include in the list.
7. To view the category names assigned to this list, look at the Selected Categories panel at the bottom of the window.
8. Click Save and enter a brief description of the change.

This category list can now be used in policy. See "Include a Shared Policy Object in CPL or VPM Policy" on page 232.

To apply a category list template to an existing category list, edit the category list, go to the Info tab, select the template, and then save the list.

When the CPL for a category list is generated and the list contains categories not present in the template (most likely because the template had been changed since last saving the list), those categories are not included in the condition definition CPL. If this occurs, a warning is included as a comment above the condition CPL, indicating which categories were removed.

Create Custom Categories

The category shared object allows you to easily create custom categories for use in policy. These categories can then be included in your existing policy for ProxySG appliances. An example implementation is described here.

Although a category object appears similar to a URL list, the category object generates a `define category` instruction in policy instead of a condition and subcondition definition. For example, if you create a category called blacklist and add example.com to it, the generated policy will look like this:

```plaintext
; Generated by Management Center from Category: Complex Category
define category blacklist
http://example.com/
end
```
As shown above, all custom categories created in Management Center are preceded by a comment noting the source of the category. On the ProxySG appliance, these categories are treated as yet another category source, like WebFilter, for example.

A category differs from a category list, which is a named set of URL categories that can be easily referenced in policy.

Step 1 - Create the Custom Category

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   a. Object name (*) - Required name
   b. Object type (*) - From the drop-down list, choose Category.
   c. Reference ID (*) - Enter a Reference ID that you can filter for when building policy.
      The Reference ID must begin with a letter and must contain only letters, numbers, and ".".
   d. Description - Enter a meaningful description to help you when reusing this object.
4. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See "Add Attributes" on page 401.
5. Click Finish. The new category displays in the editor.

Step 2 - Add URLs

1. Select Configuration > Shared Objects.
Management Center Configuration & Management

2. Select or edit the desired category. The system displays the category editor.
3. Enter the URL in the **URL** field and click **Add**.

![Category Editor](image)

The system displays the text entered into the **Description** field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:
   a. Create a category and copy the URLs.
   b. Click **Paste URLs**.

![Paste URLs: Enter URLs](image)

The system opens the Paste URLs: Enter URLs dialog.

- Paste URLs below
  
  *Each URL requires its own individual line*

![Paste URLs: Enter URLs](image)

- Copy the URLs into the Paste URLs: Enter URLs dialog. Press **CTRL+V** or right-click and click **Paste**. The URLs are added to the list.
d. Click **Next**. The system opens the Paste URLs: Validate dialog.

e. Click **Finish**.

5. Click **Save**.

**Enabling and Disabling URLs**

You can disable an individual URL by selecting it and clicking **Disable**.

![URL Table]

You can enable a URL by selecting it and clicking **Enable**.

**Step 3 - Include the Category in Policy**

When you have completed your changes, you can include the category in CPL or in the VPM, as described in "Include a Shared Policy Object in CPL or VPM Policy" on page 232. The category will be included in the CPL as a category definition that you will then reference in a proxy layer. See the example below for details.

You can then install your policy as described in "Install Policy" on page 302.

**News Whitelist Scenario Example**

**Custom Category Example**

In this example, the administrator has created a simple acceptable use policy and would like to add a new whitelist category for news.
Define subnet corporate_subnet
 198.51.100.0/24
end

<proxy "Web Access">
  client.address=corporate_subnet ALLOW
</proxy>

<proxy "Web Auth">
  authenticate(corp_realm)
</proxy>

<proxy "Web Filter">
  url domain=playboy.com FORCE_DENY
  category=(gambling, hacking, games, news) exception(content_filter_denied)
</proxy>

<proxy "Restricted Access">
  group=execs, managers url domain=fantasyfootball.com ALLOW
</proxy>

This CPL is stored in a policy object called ASUP. The ASUP policy object has Replace substitution variables enabled.

Though the URL filtering blocks all news sites, she would like to allow cnn.com, yahoo.com, and nytimes.com. To allow these sites, the administrator does the following.

**Step One - Create the Category Object**

1. Selects Configuration > Shared Objects.
2. Clicks Add Object. The web console displays the Create New Shared Object wizard.
3. Enters the following data:
   a. Object name: News Whitelist
   b. Object type: Category
   c. Reference ID: autofill
   d. Description: List of allowed URLs
4. Clicks Next.
5. Clicks Finish.

**Step Two - Add URLs**

1. In the News Whitelist policy editor, the administrator enters cnn.com in the URL field and clicks Add.
2. Adds yahoo.com and nytimes.com, as described in the preceding step.
3. Clicks Save and enters a brief description of the change. The News Whitelist object now looks like this.

<table>
<thead>
<tr>
<th>Enabled</th>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cnn.com</td>
<td>Added on 1/05/2017</td>
</tr>
<tr>
<td></td>
<td>yahoo.com</td>
<td>f</td>
</tr>
<tr>
<td></td>
<td>nytimes.com</td>
<td></td>
</tr>
</tbody>
</table>
Step Three - Add the Category to the ASUP Policy

1. Selects Configuration > Policy > ASUP. The ASUP policy opens in the editor. Remember that the administrator has previously enabled Replace substitution variables.
2. Clicks Operations > Insert > Insert Include.
3. In the Insert Policy Include window, selects News Whitelist and clicks OK.

   The ASUP CPL now looks like this:

   Define subnet corporate_subnet
   198.51.100 0/24 
   end 
   ${include:News_whitelist}
   <proxy "Web Access">
   client.address=corporate_subnet ALLOW
   </proxy "Web Auth">
   authenticate(corp_realm)
   <proxy "Web Filter">
   url.domain=playboy.com FORCE_DENY
   category=News_Whitelist ALLOW
   category=(gambling, hacking, games, news) exception(content_filter_denied)
   <proxy "Restricted Access">
   group=execs, managers url.domain=fantasyfootball.com ALLOW
   
4. To create the rule, the administrator adds the following rule to the Web Filter layer in CPL to implement the News Whitelist:

   category=News_Whitelist ALLOW

   See example below.

   <proxy "Web Filter">
   url.domain=playboy.com FORCE_DENY
   category=News_Whitelist ALLOW
   category=(gambling, hacking, games, news) exception(content_filter_denied)
   <proxy "Restricted Access">
   group=execs, managers url.domain=fantasyfootball.com ALLOW

5. Clicks Save.

   The ASUP CPL is now ready to be pushed to target devices.

Create a Local Content Filter Database

The Local Content Filter Database is a list of URL categories that each of your ProxySG, Advanced Secure Gateway, and SSL Visibility (SSLV) appliances subscribe to, for use in policy. Unlike shared lists and policy-based categories, the local database feature creates a file that is hosted on the Management Center appliance. Configured ProxySG, Advanced Secure Gateway, and SSLV appliances query Management Center for updates to the database at regular intervals.
Local database content filter configuration is supported on all SGOS devices and versions. SSL Visibility supports local category database configuration in the 3.x branch in 3.9.4.1 and later (except Virtual Appliance versions), and in the 4.x branch, version 4.2.x and later.

**Step 1 - Create a Local Database Policy Object**

1. In the Management Center web user interface, Click **Configuration > Policy**.
2. Click **Add Policy**. The web console displays the **Create New Policy** wizard.
3. Fill in required fields.
   a. **Policy name (**) - Required name**
   b. **Policy type (**) - From the drop-down list, select **Local Database**.
   c. **Reference ID (**) - Enter a Reference ID that you can filter for when building policy.**
      
      The Reference ID is auto-generated. If you choose to define it manually, the Reference ID must begin with a letter and must contain only letters, numbers, or underscores.
   d. **Description** - (Optional) a meaningful description to help you when referring to this Local Database.
4. Click **Next**. The **Create New Policy** wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute values for the local database. See "Add Attributes" on page 401 for more information on working with attributes.
5. Click **Finish**. The editor displays the new local database.

**Step 2 - Add Categories to the Local Database**
Supported Local Category Syntax

The local category editor supports the following syntax:

- **Domain**: example.com
- **Domain with path**: example.com/directory/server
- **Subdomain**: server.example.com/
- **Top Level domains**: .gov, .net, .com...
- **Single label host names**: server1
- **IPv4 address**: 203.0.113.5
- **IPv6 address**: [2001:db8:0:1:1:1:1:1]
- **IPv6 with embedded IPv4 addresses**: [0:0:0:0:FFFF:203.0.113.5]

Local Category Limitations

Local category support has the following limitations:

- Each local database can contain up to 200 categories.
- The same URL cannot be included in more than four categories in a single local database.

Define and Manage Local Categories

1. Click **Add Category**. The system displays the **Add Category** dialog.

![Add Category dialog]

2. Define URLs or IP addresses for this category.
   Note the syntax and limitations note at the beginning of this section. The text editor in this dialog validates the syntax of entries with red text.
3. Repeat steps one and two until you are satisfied with the categories and their entries, then click **Save**.
   The system displays the **Save Changes** dialog. Enter a comment to save the new local database and click **Save**.

Optional Step - Import Categories

Management Center can export category content in JSON format from the **Configuration > Policy** page. If you have previously done so, you can import that file into your new database by clicking the **Import** button. For more information on exporting policy objects, see "Export Policy or Shared Objects to Local Disk" on page 333.

---

Plain text-formatted local database files (such as those exported from SGOS devices) are not compatible with the import function.
Edit a Category

Refine the entries in your database categories.

1. Click the memo pad icon at the far right of the category name for the category you want to modify. The system displays the Add Category dialog. You can enter, modify, or delete entries, just as when you initially created the category.
2. Click Save to save your changes. The Add Category dialog closes. Management Center displays an asterisk before Local Database at the top of the page, indicating that the updated category definition must be committed.
3. Click Save.

View Database Versions

Management Center uses version control to track each change to a local database. Use the following steps to view, compare, or restore versions of a local database.

1. While viewing your local database, click the Versions tab.
2. Select an entry and click View. The system displays the Preview of Version x.x dialog.
3. Click either of the buttons at the top of this list to expand all or collapse all categories.
4. Click Close to close the preview dialog.

Compare Database Versions

1. While in the Versions tab, hold CTRL or ⌘ on your keyboard and simultaneously click to select two versions of the local database you want to compare.
2. Click Compare.
   The system displays a version of the policy editor with both versions of the local database. In this display, new content highlighted in green, modified content in yellow, and removed content in red.
Management Center hosts your new local policy file, and each of your SSL Visibility, ProxySG or Advanced Secure Gateway appliances can now be configured to request it. By default, SSLV and SGOS will query the configured remote host for a local category database once an hour.

**Record the Local Database Direct URL**

Management Center automatically generates a URL from which your devices can retrieve the local database.

1. While editing a local database, click the **Info** tab.
2. In the **Direct URL** field, click the **copy icon** to copy the URL to your system's clipboard.
3. Use the Direct URL to configure the local policy remote URL on your appliance. See the next section for Local URL configuration steps for your appliance.
4. (Optional) Click the **refresh icon** to regenerate the Direct URL. The previous URL becomes invalid when a new URL is generated.
Management Center Configuration & Management

Your SSL Visibility, ProxySG or Advanced Secure Gateway appliances must have the certificate chain for Management Center in its stores before they can establish an HTTPS connection to Management Center URLs like the one used to host the local database. See your product documentation for steps to install the Management Center console certificate to initiate this trust relationship.

If your appliance does not have the Management Center certificate installed, you may modify the provided URL to use HTTP in place of HTTPS, and port 8080 in place of 8082. In addition, Management Center must also have HTTP management enabled with the CLI command: `security http enable` before it can host HTTP content.

Modified in this way, the URL in above image is as follows: `http://<MC_IP>:8080/direct/policy/F5kdR6lt`

**Manual Deployment - SSL Visibility**

Configure SSL Visibility appliances running version 3.9.4.1 or later, or 4.2.x or later.

1. Log into the SSL Visibility web management console.
2. Click Policies > Host Categorization List.
3. Under Host Categorization Database Providers, click Local. The Host Categorization Status and Database Settings details display.
4. Click the Pencil icon next to Host Categorization Database Settings. The system displays the Edit Host Categorization Status and Database Settings dialog.

![Edit Host Categorization Database Settings](image.png)

5. Paste the URL from the Direct URL field in the Info tab in the Management Center web interface into the URL field.
6. Ensure that the Manual Download Mode check is clear if you want SSLV to query Management Center periodically for updates to the local database.
7. (Optional) If your SSLV configuration requires a proxy to reach Management Center on your network, enter the connection and authentication details as appropriate.
8. 3.9.4.1 only - (Optional) if your appliance has the HTTPS CA and server certificates for Management Center, select the External CA list containing that certificate.
Manual Deployment - ProxySG and Advanced Secure Gateway

Install the URL in each appliance you want use this local database.

1. Log in to your ProxySG or Advanced Secure Gateway management console.
2. Browse to Configuration > Content Filtering > Local Database.
3. Paste the URL from the previous step into the URL field and click Apply.
4. Click Download Now to retrieve the database for the first time.
5. Browse to Content Filtering > General and put a check in the Enable box next to Local database. Click Apply. This ensures that the appliance will retrieve database updates automatically, as they become available.

(Optional) Scripted Configuration - ProxySG and Advanced Secure Gateway

Management Center can configure each of your ProxySG and Advanced Secure Gateway appliances with the help of a script. Follow the steps below if you would prefer to have Management Center push the settings to each of your ProxySG or Advanced Secure Gateway appliances.

1. In the Management Center management console, browse to Configuration > Scripts.
2. Click Add Script.
3. Name the new script. In this example, we use LocalDBSettings.
4. Select the device type of ProxySG or Advanced Secure Gateway, as appropriate, and click Save.
5. Enter the following details for your new script, replacing the URL in the example for the unique URL generated by your Management Center:
   ```
   content-filter
   local
download url http://MC_IP:8080/direct/policy/F5kdR6lt
download auto
download get-now
exit
provider local enable
   ```
6. Click Save and enter a comment for the commit operation.
7. Click Execute on Device.
8. Select one or more target appliances and click Execute. Management Center applies the script to the selected appliances and displays the results in the Job Progress dialog.

For more information on writing configuration scripts, see Create a Script.

Create SSL Visibility List Policy

You can create policy in Management Center that manages URL or IP address lists for SSL Visibility appliances, and then deploy the policy to a group of SSL Visibility appliances. The following options are available:

- Create IP address or URL lists in Management Center and add them to an SSL Visibility list policy.
- Import URL or IP address lists from an SSL Visibility appliance into a Management Center list.
Map Management Center lists to SSL Visibility IP address or URL lists; when the SSL Visibility list policy is deployed, the lists will be synchronized (with the Management Center list being the "master").

**Step 1 - Create the List Object**

Regardless of whether you are creating the list entries directly in Management Center or importing them from SSL Visibility, you first need to create an IP address or URL list object.

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose the type of list: **URL List** or **IP Address List**.

![Create New Shared Object: Basic Information](image)

   c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.

   The Reference ID must begin with a letter and must contain only letters, numbers, and ".".

d. **Description** - Enter a meaningful description to help you when reusing this object.

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See "Add Attributes" on page 401.

5. Click **Finish**. The new list displays in the editor.

**Step 2 - Add URLs or IP addresses to the List (Optional)**

You can optionally add URLs or IP addresses to this list or if the list already exists on the SSL Visibility device, you can import the list (see Step 3).
Step 3 - Import URLs or IP addresses from an SSL Visibility Appliance

If one of your SSL Visibility appliances already has URL or IP address lists, you can save time by importing the list into a Management Center list (instead of retyping the list in Management Center).

1. Select **Configuration > Shared Objects**.
2. Select the URL or IP address list you created in Step 1.

3. Select **Import > From Device**. The Source Device dialog lists all the SSL Visibility devices that have been added to Management Center.
4. Enable the check box next to the SSL Visibility device containing the list you want to import into Management Center and click **Next**. The Select Policy dialog displays the lists on the SSL Visibility device.
5. Select the list name you want to import and click Import.

6. Click Import and overwrite. The entries contained in the list in the SSL Visibility appliance are now listed in the Management Center list.

7. Click Save.

**Step 4 - Create the SSL Visibility Policy Object**

Management Center has a policy type specific to SSL Visibility lists. You create the SSL Visibility lists policy as described in this step and then add IP address or URL lists to it as described in Step 5.

1. Select Configuration > Policy.

2. Click Add Policy. The Create New Policy wizard opens.
3. **Policy name**: Enter a descriptive name for the policy.

4. **Policy type**: Choose **SSLV Lists** from the drop-down.

5. **Reference ID**: This is supplied automatically, based on the policy name (spaces are replaced with underscores).

6. (Optional) **Description**: Enter a description up to 1024 characters.

7. Click **Next**.

8. Click **Finish**.

**Step 5 - Add Lists to the SSL Visibility List Policy**

After you have created the SSL Visibility list policy, you can add one or more IP address or URL lists to it.
1. In the SSLV Lists policy screen, click **Add List**. The system displays the URL Lists window.

2. Select the check box next to the list you want to include in the policy.

3. Click **OK**. The list(s) are shown in the policy.

4. Click **Save**.

**Step 6 - Mapping Management Center Lists to SSL Visibility Lists**

When Management Center syncs policy to the SSL Visibility device, it needs to know which Management Center lists correspond to which lists on the SSL Visibility device. This is accomplished by mapping the SSL Visibility list to the Management Center list. During the policy sync, Management Center compares the entries in the mapped lists. Any entries on the Management Center list that aren't present on the SSLV list will be added to the SSL Visibility list. Any entries on the SSL Visibility list that aren't in the Management Center list will be deleted.

1. In the SSLV policy, click **Add List**.

2. Select the list.
3. In the **Subject/List Name on SSLV** field, enter the name of the SSL Visibility list that you want to map to.

4. Click **OK**.

When the list policy is synched to SSL Visibility appliances, any lists that aren’t on the SSL Visibility appliance will be created as subject/domain name lists. However, note that Management Center will not delete a subject/domain name list on the SSL Visibility appliance if it isn’t present in the Management Center policy.

You can install the SSLV list policy directly on an SSL Visibility device or create a job to schedule the policy installation.
You can create policy in Management Center that manages URL lists for SSL Visibility appliances (SSLV), and then deploy the policy to a group of SSL Visibility appliances. The following options are available:

- Create URL lists in Management Center and add them to an SSLV list policy.
- Import URL lists from SSLV into a Management Center URL list.
- Map Management Center URL lists to SSL Visibility lists; when the SSLV list policy is deployed, the lists will be synchronized (with the MC list being the "master").

**Step 1 - Create the URL List Object**

Regardless of whether you are creating the list entries directly in MC or importing them from SSLV, you first need to create
a URL list object.

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose **URL List**.
   c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.
      
      The Reference ID must begin with a letter and must contain only letters, numbers, and ".".
   d. **Description** - Enter a meaningful description to help you when reusing this fragment.
4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See "Add Attributes" on page 401.
5. Click **Finish**. The URL list displays in the editor.

**Step 2 - Add URLs to the List (Optional)**

You can optionally add URLs to this list or if the list already exists on the SSL Visibility device, you can import the URLs from the list (see Step 3).

**Step 3 - Import URLs from an SSL Visibility Appliance**

If one of your SSL Visibility appliances already has URL lists, you can save time by importing the URLs into a Management
Center URL list (instead of retyping the URLs in MC).

1. Select **Configuration > Shared Objects**.

2. Select the URL list you created in Step 1.

3. Select **Import > From Device**. The Source Device dialog lists all the SSL Visibility devices that have been added to Management Center.
4. Enable the check box next to the SSL Visibility device containing the URL list you want to import into Management Center and click **Next**. The Select Policy dialog displays the lists on the SSL Visibility device.
5. Select the list name you want to import and click **Import**.

6. Click **Import and overwrite**. The URLs contained in the list in the SSL Visibility appliance are now listed in the URL list.

7. Click **Save**.

**Step 4 - Create the SSL Visibility Policy Object**

Management Center has a policy type specific to SSLV lists. You create the SSLV lists policy as described in this step and then add URL lists to it as described in Step 5.

1. Select **Configuration > Policy**.

2. Click **Add Policy**. The Create New Policy wizard opens.
3. **Policy name**: Enter a descriptive name for the policy.

4. **Policy type**: Choose **SSLV Lists** from the drop-down.

5. **Reference ID**: This is supplied automatically, based on the policy name (spaces are replaced with underscores).

6. (Optional) **Description**: Enter a description up to 1024 characters.

7. Click **Next**.

8. Click **Finish**.

**Step 5 - Add URL Lists to the SSLV List Policy**

After you have created the SSLV lists policy, you can add one or more URL lists to it.
1. In the SSLV Lists policy screen, click **Add List**. The URL Lists window opens.

![URL Lists](image-url)

2. Select the check box next to each URL list you want to include in the policy.

3. Click **OK**. The list(s) are shown in the policy.

---

**Step 6 - Mapping Management Center URL Lists to SSL Visibility URL Lists**

When Management Center syncs policy to the SSL Visibility device, it needs to know which MC URL lists correspond to which URL lists on the SSLV device. This is accomplished by mapping the SSL Visibility list to the MC URL list. During the policy sync, Management Center compares the entries in the mapped lists. Any entries on the MC list that aren’t present on the SSLV list will be added to the SSLV list. Any entries on the SSLV list that aren’t in the MC list will be deleted.

1. In the SSLV policy, click **Add List**.

2. Select the URL list.
3. In the **Subject/List Name on SSLV** field, enter the name of the SSLV URL list that you want to map to.

4. Click **OK**.

When SSLV list policy is synched to SSL Visibility appliances, any URL lists that aren’t on the SSLV will be created as subject/domain name lists. However, note that Management Center will not delete a subject/domain name list on the SSLV if it isn’t present in the MC policy.

You can install the SSLV list policy directly on an SSL Visibility device or create a job to schedule the policy installation.
Create SSL Visibility IP Address List

Using this feature, you can easily create IP address lists for use on the SSL Visibility appliance. IP address lists are shared objects, and are similar to URL lists.

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit ${include} and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

Step 1 - Create the IP Address List Object

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose **IP Address List**.

c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.
   
   The Reference ID must begin with a letter and must contain only letters, numbers, and "_".

d. **Description** - Enter a meaningful description to help you when reusing this object.

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See "Add Attributes" on page 401.

5. Click **Finish**. The new IP address list displays in the editor.

**Step 2 - Add IP Addresses**

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired IP address list. The system displays the IP address list editor.
3. Enter the IP address in the **IP Address** field and click **Add**.

   The system displays the text entered into the **Description** field as a comment in the generated policy.
4. Alternatively, paste in multiple IP addresses:
   a. Create an IP address list and copy it in.
   b. Click **Paste IP addresses**. The system opens the Paste IP addresses: Paste IP addresses dialog.

   ![Paste IP addresses dialog](image)

   c. Copy the URLs into the Paste IP addresses: Paste IP addresses dialog. Press **CTRL+V** or right-click and click **Paste**. The URLs are added to the list.
   d. Click **Next**. The system opens the Paste IP addresses: Validate dialog.
   e. Click **Finish**.

5. Click **Save**.

### Enabling and Disabling IP Addresses

You can disable an individual IP address by selecting it and clicking **Disable**.

![IP address list](image)

You can enable an IP address by selecting it and clicking **Enable**.

### Step 3 - Include the IP Address List in Policy

When you have completed your changes, you can include the IP address list in your SSLV policy object, as described in "Create SSL Visibility List Policy" on page 261.

You can then install your policy as described in "Install Policy" on page 302.
Deploy Tenant Policy

Tenant policy describes a framework that provides large organizations with high service availability, flexibility for multiple tiers of administration, and ensures that all appliances in the network are used efficiently.

- **Tenant Policy** - An infrastructure that segregates the policy elements that effect users of each user network defined within domains. Even though they use the same ProxySG appliance, two groups of users could have vastly different policy sets.
- **Role-Based Administration** - A set of Management Center controls that allows a tiered-based approach to managing ProxySG appliances and their associated policy. The top-tier administrators can view and manage all levels of policy, second-tier (or branch) administrators can manage only their own level of policy and those beneath them, and bottom-tier or tenant-level administrators can only view the policy for their own users.

All administrators control policy appropriate to their roles. Policy can be written specifically to route traffic from where users are to one of several ProxySG appliances in your network, depending on load and availability.

Refer to the following deployment steps:

**Step 1: Plan Network Configuration**

**Who performs this step:** ProxySG administrator

Before proceeding, it is important to plan how your organization is structured. For example, determine the following:

- How user networks are grouped or separated (for example, by geographic location)
- What interfaces receive traffic from those users
- Why types of policy can be deployed to the tenant slot

**Step 2: Configure Management Center**

**Who performs this step:** Management Center admin/Super Admin

After configuring the appliance(s), add them to Management Center and define roles and administrators. Then, configure default, group, and tenant policy to the appliances. User roles will dictate which users can see and manage policy for each appliance or group of appliances.

1. **Add a configured appliance to Management Center.**
   From the Management Center web console, access the online help and search for the topic entitled *Add a Device* for the steps to add each ProxySG appliance to Management Center. Repeat this process for each configured ProxySG in your network. To import many devices at one time, from the online help search for *Add Multiple Devices at Once*.

2. **To keep your devices organized, see the instructions for how to create hierarchies, device groups and sub-groups.**
   A device group is a folder in the device organizational structure that exists below the hierarchy level and contains devices or sub-folders. Arrange device groups and devices in a way that makes sense.
   - **Configure Hierarchy for Devices and Device Groups**
   - **Add a Device Group**
   - **Drag and Drop Device Groups**

3. **Create device attributes to help manage your organization’s network of appliances and groups of appliances.**
   Device attributes can be used to identify the location of a given appliance, the region or branch office it’s associated with or
even which tenants are associated with each appliance. For more information, see the following topics in the online help:

- Manage Attributes
- Add Device Attributes
- Add Device Group Attributes

3. Assign attributes to your configured appliances. For instructions, see "Edit a Device" on page 66.
4. Create administrator roles with different sets of permissions. After you "Define Roles " on page 386 see the types of the permissions that are most valuable per role that you have created. This guide contains a reference topic "Reference: Permissions Interdependencies" on page 339 that is invaluable when creating the roles in your organization.
   The following example shows how to create a role for managing a device group that you created ("Add a Device Group" on page 56).
5. Create administrator groups. From the Administration tab, click Groups > Add Group.
6. Add admin users. For instructions on how to create administrator accounts, see "Grant Permissions" on page 390.
7. Create policy attributes. For instructions on how policy attributes can be used to organize and refine policy, see the following online help topics:
   - Manage Attributes
   - Add Policy Attributes
   - Mandatory Attributes
8. Define tenants. See "Manage Tenants" on the next page for instructions.
9. Create tenant policy in VPM ("Create a VPM Tenant Policy Object" on page 286 or CPL (see Create the Content Policy Language).
10. Confirm that the correct policies are deployed to each device slot. See "View Deployed Policy for each Device Slot" on page 323.
Manage Tenants

Tenants are administrative entities defined on ProxySG appliances. Each request is routed through a tenant, whose policy is evaluated for that transaction. When no specific tenant is determined for a request, the default tenant policy is used. Tenant determination criteria governs which tenant’s policy applies to a given request. Add these tenants to Management Center to create and deploy tenant-specific policy.

On the ProxySG appliance, there are two options for controlling tenancy determination:

1. The `#(config general) multi-tenant criterion` command specifies a substitution expression that is evaluated for tenancy determination.

2. Using the `<tenant>` layer in the Landlord CPL slot to specify conditions and `tenant()` properties.

The Management Center WAF interface leverages option #2 to control tenancy determination via the Tenant Determination object. See "About WAF Policy" on page 132 for more information.

When evaluating an HTTP request, if the tenant determination rules produce a match against an installed tenant, then that tenant’s policy will be evaluated. If that fails to set the `tenant()` property, or the `tenant()` property setting does not correspond to an installed tenant policy, then the default tenant policy is applied to this traffic. Default tenant policy applies to all requests where tenancy couldn’t be determined during the initial connection.

Obtain the tenant identifiers before you write multi-tenant policy in Management Center. For more information on multi-tenant policy, refer to the Multi-Tenant Policy Deployment Guide.

WAF Policy Use

Selecting a tenant is step 2 in "Use WAF Policy To Protect Servers From Attacks" on page 130. A base-level of WAF policy should be installed to the default tenant before any additional tenants are created. This ensures that all requests are processed by the WAF.

Add a Tenant

An asterisk denotes fields that are mandatory.
1. Select **Configuration > Tenants**.

2. Click **Add Tenant**.

The web console displays the **Add Tenant** dialog.
3. Enter a **Display Name**.
4. Enter the **Tenant ID**. This controls the name of the tenant slot where policy will be installed. This ID is also used in the tenant determination CPL using the `tenant()` property.
5. (Optional) Enter a **Description** (up to 1024 characters).
6. Click **Save**.

By default, the **Tenants** list is sorted in alphabetical order by Display Name. You can also sort by **Tenant ID** or **Description** by clicking the column headings. If the list is long, use the Keyword Search field to search for any string in the name, ID, or description. The search is case-sensitive.

### Modify a Tenant

1. Select **Configuration > Tenants**.
2. From the Tenants list, select the tenant to modify and click **Edit**. The web console displays the **Edit Tenant** dialog.

   ![Tenants panel](image)

3. Edit the **Display Name** or **Description**. An asterisk denotes fields that are mandatory.
4. Click **Save**.

### Delete One or More Tenants

1. Select **Configuration > Tenants**.
2. From the Tenants list, select one or more tenants to remove.
3. Click **Delete**.

   ![Tenants panel](image)

4. Select **Yes** to delete the selected tenants.
You cannot delete the default tenant or any tenant that is currently referenced in Management Center policy. Attempting to delete the default or a referenced tenant results in a "Delete failed" error message.
Create a VPM Tenant Policy Object

A VPM Tenant policy object defines the policy for a VPM Tenant. When creating a VPM Tenant policy object, you select the attribute values that apply to the policy (if attributes have been defined). Then, select the devices or groups to which you deploy the policy; alternatively, you can define these device/group targets later.

To write tenant policy in CPL instead of using the VPM, see Create the Content Policy Language.

To write tenant policy in CPL instead of using the VPM, see Create the Content Policy Language.

1. Select Configuration > Policy and click Add Policy.

   The web console displays the Create New Policy: Basic Information wizard. An asterisk denotes fields that are mandatory.

2. Enter a name for the policy object.

3. Select VPM Tenant for the Policy Type.

4. (Optional) In the Reference Id field, enter a Reference ID that you can filter on when building policy.

   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".

5. Select the Tenant to which this policy object will be applied.

6. Enter a description in the Description field. Although entering a description is optional, the description helps differentiate versions of the same policy.

7. Enter a description in the Description field. Although entering a description is optional, the description helps differentiate versions of the same policy.

8. Indicate whether to Replace Substitution Variables. See "Use Substitution Variables in Policies and Scripts" on page 202 for more information.

9. Click Next.

10. Enter or select values for the defined attributes.

11. Click Finish.

   The new VPM Tenant policy object displays in the Policy Objects editor.

Determine Your Next Step

After you create a tenant policy object, you can either add policy to it immediately or leave it as an empty object while you perform other tasks (for example, associate more devices with it or edit policy details). Refer to the following table to determine the next step to take.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add policy.</td>
<td>&quot;Launch Visual Policy Manager&quot; on page 210</td>
</tr>
<tr>
<td>Import policy.</td>
<td>&quot;Launch Visual Policy Manager&quot; on page 210</td>
</tr>
</tbody>
</table>
Import VPM Tenant Policy from Source Device

A VPM Tenant policy object can be used to define the policy used in a tenant slot. After creating the VPM Tenant (as described in "Create a VPM Tenant Policy Object" on the previous page), you must add policy to it. You can add policy by launching the VPM or by importing existing VPM policy from a source device.

Certain features available in normal VPM policy are not available in VPM Tenant policy. These include the Admin Access and Admin Authentication layers. Any existing Admin Access or Authentication layers will not be present in the imported contents.

To write tenant policy in CPL, see Create the Content Policy Language.

1. Select Configuration > Policy.
2. Select the VPM Tenant object and click Edit.
3. Select Import > From Device.

The system displays the Import Policy: Source Device dialog.

4. Select the source device and click Next.
5. Click **Import**.

The dialog closes and the following message is displayed in the editor:
The CPL for this VPM policy is out of date and needs to be regenerated before it can be deployed. Please launch the VPM editor and save a new revision to update the CPL.

This is because only the VPM contents are imported, not the generated CPL.

6. To regenerate the CPL, click **Launch VPM Editor**.

7. Click **Save Policy**.
8. Enter a comment for your save and click **OK**.
9. Click **Close**.

The CPL now displays in the editor.

**Determine Your Next Step**

Refer to the following table to determine the next step to take.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about deploying multi-tenancy policy on ProxySG appliances.</td>
<td><strong>Multi-Tenant Policy Deployment Guide</strong></td>
</tr>
<tr>
<td>Create and manage tenants from Management Center.</td>
<td>&quot;Manage Tenants&quot; on page 282</td>
</tr>
<tr>
<td>View policies deployed to each slot on a device.</td>
<td>&quot;View Deployed Policy for each Device Slot&quot; on page 323</td>
</tr>
</tbody>
</table>
Deploy Tenant Policy

Tenant policy describes a framework that provides large organizations with high service availability, flexibility for multiple tiers of administration, and ensures that all appliances in the network are used efficiently.

- **Tenant Policy** - An infrastructure that segregates the policy elements that effect users of each user network defined within domains. Even though they use the same ProxySG appliance, two groups of users could have vastly different policy sets.

- **Role-Based Administration** - A set of Management Center controls that allows a tiered-based approach to managing ProxySG appliances and their associated policy. The top-tier administrators can view and manage all levels of policy, second-tier (or branch) administrators can manage only their own level of policy and those beneath them, and bottom-tier or tenant-level administrators can only view the policy for their own users.

All administrators control policy appropriate to their roles. Policy can be written specifically to route traffic from where users are to one of several ProxySG appliances in your network, depending on load and availability.

Refer to the following deployment steps:

**Step 1: Plan Network Configuration**

**Who performs this step:** ProxySG administrator

Before proceeding, it is important to plan how your organization is structured. For example, detemine the following:

- How user networks are grouped or separated (for example, by geographic location)
- What interfaces receive traffic from those users
- Why types of policy can be deployed to the tenant slot

**Step 2: Configure Management Center**

**Who performs this step:** Management Center admin/Super Admin

After configuring the appliance(s), add them to Management Center and define roles and administrators. Then, configure default, group, and tenant policy to the appliances. User roles will dictate which users can see and manage policy for each appliance or group of appliances.

1. Add a configured appliance to Management Center.
   From the Management Center web console, access the online help and search for the topic entitled **Add a Device** for the steps to add each ProxySG appliance to Management Center. Repeat this process for each configured ProxySG in your network. To import many devices at one time, from the online help search for **Add Multiple Devices at Once**.
2. To keep your devices organized, see the instructions for how to create hierarchies, device groups and sub-groups. A device group is a folder in the device organizational structure that exists below the hierarchy level and contains devices or sub-folders. Arrange device groups and devices in a way that makes sense.
   - **Configure Hierarchy for Devices and Device Groups**
   - **Add a Device Group**
   - **Drag and Drop Device Groups**
3. Create device attributes to help manage your organization's network of appliances and groups of appliances. Device attributes can be used to identify the location of a given appliance, the region or branch office it's associated with or even which tenants are associated with each appliance. For more information, see the following topics in the online...
help:
  - Manage Attributes
  - Add Device Attributes
  - Add Device Group Attributes

3. Assign attributes to your configured appliances. For instructions, see "Edit a Device" on page 66.
4. Create administrator roles with different sets of permissions. After you "Define Roles " on page 386 see the types of the permissions that are most valuable per role that you have created. This guide contains a reference topic "Reference: Permissions Interdependencies" on page 339 that is invaluable when creating the roles in your organization.
   The following example shows how to create a role for managing a device group that you created ("Add a Device Group" on page 56).
5. Create administrator groups. From the Administration tab, click Groups > Add Group.
6. Add admin users. For instructions on how to create administrator accounts, see "Grant Permissions" on page 390.
7. Create policy attributes. For instructions on how policy attributes can be used to organize and refine policy, see the following online help topics:
   - Manage Attributes
   - Add Policy Attributes
   - Mandatory Attributes

9. Create tenant policy in VPM ("Create a VPM Tenant Policy Object" on page 286 or CPL (see Create the Content Policy Language).
10. Confirm that the correct policies are deployed to each device slot. See "View Deployed Policy for each Device Slot" on page 323.

Apply a Single Policy to Both On-Premises and Cloud Users

Universal policy is a set of global rules created on Management Center that can be applied to users in any location. The policy can contain global rules that apply to both on-premises and Web Security Service (WSS) users, as well as individual rules that apply to only one or the other. It can also contain location-specific policy when necessary. In essence, universal policy comprises the various rules that reflect your organization’s acceptable use policy. Using Management Center to create and distribute the policy to on-premises devices and the WSS makes it easy to apply the relevant policy to all users in your organization.

You can create universal policy using VPM or CPL.

Prerequisites

To use the universal policy feature, you must first:

- Have a valid Web Security Services (WSS) account configured to accept policy from the Management Center via the WSS on-boarding wizard. Existing WSS cloud customers may contact Customer Support for configuration assistance.
- Configure your WSS account for on-premises policy enforcement.
- Enable enforcement domains and create policy on the reference ProxySG appliance. Although you can import universal policy from a source that does not have enforcement domains enabled, you cannot deploy the policy unless you launch the VPM Editor and save a new revision of policy. This generates the CPL with enforcement domains enabled.
SSL Requirements

Universal policy requires proper SSL certificate validation. You must:

- Ensure that Management Center is able to connect to https://sgapi.es.bluecoat.com
- Verify that no inline proxies will disrupt SSL connections to your devices.
- If Management Center uses the explicit HTTP proxy, ensure that it does not decrypt traffic

Software Version Requirements

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProxySG appliance</td>
<td>6.7.1.1 or later; 6.5.9.14 or later (6.6.x is not supported at this time)</td>
</tr>
<tr>
<td>Web Security Service</td>
<td>6.9.5.1 or later</td>
</tr>
<tr>
<td>Management Center</td>
<td>1.8.1.1 or later (1.10.1.1 or later for CPL universal policy)</td>
</tr>
</tbody>
</table>

Solution Steps

1. **Add** the WSS as a device.
2. Select the policy to be used for universal policy by doing one of the following:
   a. Create a new universal VPM or CPL policy object.
   b. **Edit** an existing CPL policy object.
   c. **Transform** an existing VPM policy object into universal policy.
3. If you created a new universal VPM or CPL policy object, **import** the policy from the reference ProxySG appliance.
4. Edit the **VPM or CPL** universal policy:
   a. Use the classifier to analyze the policy to determine if it’s valid for WSS.
   b. Using the classifier results, modify your policy. Determine if a rule should apply only to the WSS, the appliance, or both (universal).
   c. Save the policy.
   d. Repeat as necessary until you are satisfied with the classifier results.
5. Add WSS and any on-premises devices **as targets**.

   You cannot add WSS and other devices as targets in the same operation because they have different deployment types. You must add WSS devices in a separate operation.

6. **Install** the policy to the targets.

Add a Universal VPM Policy Object

To add a universal VPM policy object, complete the following steps.

1. Select **Configuration > Policy**.
2. Click **Add Policy**. The system displays the Create New Policy: Basic Information dialog. An asterisk denotes fields that are mandatory.
3. Enter a name for the policy object.
4. Select **Universal VPM Policy** for the **Policy Type**.
5. Enter a **Reference ID**. Although entering a reference ID is not required, it is useful for filtering objects when building
policy. If you do not enter a reference ID, the system assigns a default ID based on the policy name you enter. Imported policy objects are assigned a default ID.

6. Enter a description in the Description field. Although entering a description is not required, the description helps differentiate versions of the same policy.
8. Click Next.
9. Enter or select values for the defined attributes.
10. Click Finish.

Transform Existing VPM Policy into Universal VPM Policy

To transform an existing VPM policy object into a universal policy object, you clone it as described below.

1. Select Configuration > Policy.
2. From the Policy Objects list, select the policy name or highlight the policy and click Edit.
3. Click Clone to Universal.
4. In the Clone and convert to Universal dialog, review the name and modify it if necessary. Then click **Clone**.

The system displays the new universal VPM policy. By default, the policy is titled with the original policy name with **Universal** appended. For example, if the original policy name is **VPM Sunnyvale**, the new universal policy name is **VPM Sunnyvale - Universal**. You can now open the VPM and edit the universal policy.

**Refine and Validate Universal VPM Policy**

After creating universal VPM policy, you must refine your universal policy rules. Each policy rule can apply only to on-premises users, only to remote users (Web Security Service - WSS), or to both (universal policy). These categories are called **enforcement domains**. Before uploading the rules to the WSS, you must analyze the policy to ensure it will run as expected.

**VPM Requirements**

- When using the VPM editor, Symantec recommends that you use the recommended Java version listed [here](#).

Releases prior to Java 1.8 use a vulnerable cryptographic hash (SHA1) function that Management Center no longer supports. If you are using Java 1.8.131 or later, you will need to upgrade the ProxySG to SGOS version 6.6.4 (or later) or 6.7.2 (or later) to launch the VPM editor. Versions prior to these SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.
If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command. See “# security” on page 617 for more information.

- Before using the VPM editor in Management Center, Symantec strongly recommends that you understand how the VPM Editor works and underlying policy enforcement in ProxySG appliances. For comprehensive information on creating policy policy, as well as assigning and changing enforcement domains for policy rules in the VPM, refer to the ProxySG Appliance Visual Policy Manager Reference and Advanced Policy Tasks.
- Ensure that you have the latest VPM resource XML file installed on your ProxySG. You can download the XML file from the Symantec Support site: https://support.symantec.com/content/dam/bluecoat/download/modules/security/SGv6/policyclassifier.xml

**Procedure**

1. Select **Configuration > Policy**. From the **Policy Objects** list, locate the universal VPM policy object you want to edit. To narrow your search, you can do a “Filter by Attributes and Keyword Search” on page 167.

2. Click the policy name hyperlink or highlight the row and click **Edit**. Verify that you are in the **Editor** tab.

3. If necessary, import policy from the reference device. Click **Import**. See “Select Reference Device for VPM Policy” on page 212.

4. Click **Analyze Policy > Analyze in Production** to open the policy classifier.

![Policy Classifier](image)

- If you are participating in a beta program, click **Analyze in Pre-Production**.

The system displays the policy classifier in a new tab. The classifier breaks down the policy to illustrate whether each rule will perform as expected in the WSS.

![Policy Classifier Overview](image)

5. Review the classifier recommendations:
   - Examine the information displayed in the **Overview** tab. If the policy is not 100% enforceable on the WSS, click the **Recommendations** tab for more information.
   - If necessary, refer to the **Migration**, **Policy**, and **Dependencies** tabs for additional information.
Management Center Configuration & Management

- The **WSS** tab provides general information about the WSS. Use this information to inform your policy edits.

6. Open the VPM:

   a. Navigate back to the policy editing page and click **Launch VPM Editor**. When the system displays the following message, click **Run**.

   ![Security Warning](image1)

   b. If you see a Security Warning, check the IP address and click **Continue**.

   ![Security Warning](image2)

   The web console displays the Visual Policy Manager.

7. Keeping both the classifier and VPM open, edit your policy rules.

   ![Security Warning](image3)

   **For each rule, specify whether it should apply only to appliances (**Appliance**), both appliances and the WSS (**Universal**), or the **WSS** only.**

   If you use Windows, use **ALT+Tab** to switch between the VPM editor and the analysis tab. Displaying each application in a separate monitor also works well.
For details on enforcement domains, refer to "The Visual Policy Manager" chapter in the 6.7.1.1 Visual Policy Manager Reference.

8. Save your VPM changes.
9. As you save your changes, the classifier notes that the data is stale, prompting you to refresh. Click Refresh to update the classifier to reflect your changes.

10. Review the new results. If the policy requires modification, repeat step 6.
11. Repeat steps 7 through 9 until you are satisfied with your changes.

You are now ready to add targets and install the universal VPM policy.

**Deploy Universal CPL Policy**

Any CPL policy object can be used for universal policy, as described below.

1. Create a new CPL policy object or edit an existing CPL policy object.
2. Analyze the CPL policy.
3. Make changes to optimize the on-premise and WSS portions of the policy.
4. Repeat steps 2 and 3 until you are satisfied with the policy.

Each policy rule can apply only to on-premises users, only to remote users (Web Security Service - WSS), or to both (universal policy). These categories are called enforcement domains. Before uploading the rules to the WSS, you must analyze the policy to ensure it will run as expected.

**Analyze the CPL Universal Policy**

1. Select Configuration > Policy.
2. Click the policy name hyperlink or highlight the row and click Edit. Verify that you are in the Editor tab.
3. Click the cloud icon and select Analyze Policy > Analyze in Production to open the policy classifier.

   If you are participating in a beta program, click Analyze in Pre-Production.
The system displays the policy classifier in a new tab. The classifier breaks down the policy to illustrate whether each rule will perform as expected in the WSS.

4. Review the classifier recommendations:
   - Examine the information displayed in the **Overview** tab. If the policy is not 100% enforceable on the WSS, click the **Recommendations** tab for more information.
   - If necessary, refer to the **Migration**, **Policy**, and **Dependencies** tabs for additional information.
   - The **WSS** tab provides general information about the WSS. Use this information to inform your policy edits.

5. Using what you have learned from the classifier, edit your CPL policy. For example, if you think a section should apply only to on-premise appliances, do the following:
   a. Highlight the section.

   ```xml
   <proxy "Web Filter">
   <url domain="playboy.com" FORCE_DENY
   category="News_White">
   category="gambling, hacking, games, newa" exception="content_filter_denied"
   </url>
   <url domain="fantasyfootball.com" ALLOW>
   <proxy "Restricted Acess">
   group=execs, managers url.domain="fantasyfootball.com" ALLOW
   </proxy>
   </proxy>
   ```

   b. Select **Operations > Insert > Insert On-Premises Segment**.
The system then applies the on-premise enforcement rule to the highlighted text.

```
<proxy "Web Filter">
  url_domain=playboy.com FORCE_DENY
  category=News_Whitelist ALLOW
  category=(gambling, hacking, games, news) exception(content_filter_denied)
  #if enforcement=appliance
  <proxy "Restricted Access">
    group=execs, managers url_domain=fantasyfootball.com ALLOW
  #endif

  
  
  
  
  
  
  
  
  
  
  
```

6. As you save your changes, the classifier notes that the data is stale, prompting you to refresh. Click Refresh to update the classifier to reflect your changes.

You do not have to save your CPL policy to view changes in the classifier. Policy marked for on-premises use is not shown in the classifier.

7. Repeat steps 4 through 6 until you are satisfied with your changes.

You are now ready to add targets and install the universal CPL policy.

**Select Reference Device for Universal CPL Policy**

You must associate a reference device with your universal CPL policy before you can install it to the Web Security Service Production Network.
Management Center Configuration & Management

1. Select **Configuration > Policy**. From the Policy Objects list, select the CPL policy. Click **Edit**.

   A default reference device is not automatically populated. Associate a least one deployed device with the policy or manually configure a reference device to enable editing.

2. Select the cloud button > **Add Reference Device**.

3. To associate a reference device, from the Select Device dialog, select the check box by the device that you want to use as a reference. The selected device automatically displays in the Selected view. Click **OK**.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy universal policy.</td>
<td>&quot;Apply a Single Policy to Both On-Premises and Cloud Users&quot; on page 291</td>
</tr>
<tr>
<td>Add or remove devices associated with the policy.</td>
<td>&quot;Add or Remove Devices Associated with Policy&quot; on page 326</td>
</tr>
<tr>
<td>Restore a version of the policy.</td>
<td>&quot;Restore a Version of Policy &quot; on page 335</td>
</tr>
<tr>
<td>Import a policy configuration from a device.</td>
<td>&quot;Import Policy or Shared Objects&quot; on page 308</td>
</tr>
</tbody>
</table>

**Install or Import Policy**

To install or import policy, refer to the following.

"Preview Policy Before Installing It" below

"Install Policy" on page 302

"Install Multiple Policies" on page 307

"Import Policy or Shared Objects" on page 308

"Import External Policy " on page 315

**Preview Policy Before Installing It**

Management Center deploys policy to devices as it appears in the Policy Editor, and does not attempt to compile or otherwise validate your CPL. To make sure that the CPL is correct and that the ProxySG appliance will process the policy as intended, you can preview the policy for specific devices before installing it.
If the policy includes substitution variables, the policy preview displays the specific values that replace the variables for each associated device.

1. Create policy (Create the Content Policy Language) or edit existing policy (Refine Existing CPL Policy).
2. (If policy includes substitution variables) On the Basic Information tab when creating policy, or on the Info tab when editing policy, select Replace substitution variables.
3. Click Targets. The web console displays devices associated with the policy.
4. Select the device for which you want to preview policy.
5. Click Preview. The web console displays the CPL in a Preview dialog.

Inspect the CPL for any errors and edit it if needed. If the policy includes substitution variables, all variables are replaced with appropriate values (except for cases where no value is available). For more information, see "Use Substitution Variables in Policies and Scripts" on page 202.
Install Policy

When you create policy, you do not have to install it to devices immediately; you can save it, continue to edit and test it, and then deploy it to devices when it is complete and working as expected.

You cannot install a shared object. Shared objects are used to augment policy, not to replace policy. See "Create Shared Objects" on page 336.

You can only install the latest version of policy; if you want to install an earlier version, restore that version first. See "Restore a Version of Policy" on page 335.

Policy Installation Methods

Install policy using one of the methods described in the following table.

<table>
<thead>
<tr>
<th>Type</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Install...&quot; below</td>
<td>Configuration &gt; Policy</td>
<td>Install policy using job wizard. You can select more than one script to install in the same job.</td>
</tr>
<tr>
<td>&quot;Install to All...&quot; on page 306</td>
<td>Configuration &gt; Policy &gt; Policy_Name &gt; Edit &gt; Targets</td>
<td>Install policy using job wizard.</td>
</tr>
<tr>
<td>&quot;Install to Target&quot; on page 306</td>
<td>Configuration &gt; Policy &gt; Policy_Name &gt; Edit &gt; Targets</td>
<td>One click policy installation. Does not use the job wizard.</td>
</tr>
</tbody>
</table>

Install...

1. Select Configuration > Policy. Select the policy name.
2. From the targets shown, select the device(s) to install the policy.
3. Click Install.... Fields marked with an asterisk (*) are required. The name of the policy is automatically filled in the required field, though you can change it.
4. (Optional) Add a description. Click **Next**.

5. From **Select Policies to Install**, select the Object Selector 📋. To choose the policies to install, click the check box associated with each policy. This action immediately populates the **Selected** list. Click **OK**. Choose the Force installation check box. Click **Next**.
6. Click **All Predefined Targets** to install the policy to all target devices or click **Selected Targets** to exclude some target devices. Click **Next**.

If you select **Selected Targets**, you can select some members of a group and not others for policy installation. You do not have to install policy to all group members.
7. Choose a schedule to install the policy. Click **Finish**.

The web console displays the following messages:

- **Job Started**
  Execution of job "Install Policy: Data Loss Prevention" has begun.

- **Job Completed**
  Execution of job "Install Policy: Data Loss Prevention" has completed. Click here for complete details.

Depending on how many targets you selected, policy installation can take up to 60 seconds. During this time, the web console displays a Job Progress: Install Dialog.
Install to All...

1. Select **Configuration > Policy**.
2. Select the policy name and click **Edit**.
3. Click the **Targets** tab and click **Install to All...**
4. Follow steps 3 to 6 in "Install..." on page 302

Install to Target

1. Select **Configuration > Policy**.
2. Select the policy name and click **Edit**.
3. Click the **Targets** tab and click **Install to Target**.
Install Multiple Policies

When you create policy, you do not have to install it to devices immediately; you can save it, continue to edit and test it, and then deploy it to devices when it is complete and working as expected. You can create multiple policies without having to install the policies right away. This is particularly useful for large deployments of policies to multiple devices or device groups.

You can schedule multiple policies to deploy to device groups, as long as the following are true:

- Each policy does not have unsaved changes. To ensure that the latest policy changes are installed, click **Save Changes** in the Editor.
- Any devices you want to associate with the policy have been added and activated in Management Center.

It is a best practice to only schedule installation of policies that are the latest version. However, you can Force Installation of Policies, by selecting the **Force Installation** check box. During installation of policies, Management Center ignores the following installation warnings:

- Mismatched on-box policy object
- Mismatched OS versions

By forcing the Installation, you are ensuring that large deployments of policies DO NOT fail when encountering devices that may have the above issues.

1. From the **Jobs** tab select the **Scheduled Jobs** section. Click **Add Job**. The Add Job Wizard displays the **Add Job: Basic Info** dialog. Fields marked with an asterisk (*) are required.
2. Enter a unique **Name** (*) for this large policy deployment. Enter a Description.
   
   For example, the unique Name can be Install Policies on All Active ProxySG Appliances, and the Description can be Deploy policies to all activated ProxySG appliances.
3. Click **Next**. The Add Job wizard displays the **Add Job: Operation** dialog.
4. From the Operation drop-down, select **Install Policy**. The policy marked with a red asterisk is a mandatory policy and is installed regardless of the other policies you select.
5. From **Select Policies to Install**, select the Object Selector 📃. To choose the policies to install, click the check box associated with each policy. This action immediately populates the **Selected** list. Click **OK**. Choose the Force installation check box. Click **Next**. The Add Job wizard displays the Add Job: Targets dialog.

Each selected policy will be installed to targeted devices (excluding devices that are not active).

![Add Job wizard](image)

You cannot choose targets at this point. If you are not sure of the devices targeted by the selected policies, click **Back**. Management Center has built in intelligence, so that only properly configured policies can only be applied to appropriate targets.

6. Click **Next** to choose a **Schedule**. See "Add a Job" on page 430 and "Install Policy" on page 302.

**Import Policy or Shared Objects**

You can import policy into Management Center. For example, if a knowledge base article includes sample policy, you could import it directly into Management Center. You could also share policies between Management Center instances.

You can import policy into Management Center in the following ways:

- "Import Policy from a File (Policy or Shared Objects Grid)" on the facing page
- "Import Policy from a File (Object Edit)" on page 312
If you import a policy without a reference ID, the system assigns a reference ID with the format `auto_generated_id_1`. You can change the ID after importing the file.

**Import Policy from a File (Policy or Shared Objects Grid)**

You can import policy from the following file types:

- Management Center (.json)
- Content Policy Language (.cpl, .bpf, .txt)
- Visual Policy Manager (.xml)

**Procedure**

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.
2. Click **Import**.

The system displays the Import Policy wizard.

3. Drag and drop the file into the **Select File** dotted-line area. Alternatively, browse to the file.
4. Click **Next**.

---

[^Note]: Management Center Configuration & Management
[^Note]: “Import Policy from a Device” on page 313
5. If the imported file contains multiple policies, you might want to exclude some from import. To do this, clear the Import Policy check box.

In the preceding example, the VPM policy has been excluded from import.

6. Choose whether to create a new policy or to update an existing policy.
The wizard displays only policy objects that are relevant to the file type. If the policy uuid or reference ID in the import file matches a policy already on the system, **Update existing policy** is the default (with the matching policy prepopulated in the Policy field under **Update Existing Policy**). Otherwise, **Create new policy** is the default.

- To create a new policy, click **Create new policy** and enter a meaningful name.
- To update an existing policy, ensure that **Update existing policy** is selected. Clear the **Import Policy** check box for any policies you do not want to change.
- To update a different policy than the one shown, click the pencil icon, select the policy or policies to
7. Click **Import**. The system displays the results of the import.
8. Click **Close** to exit the wizard.

**Import Policy from a File (Object Edit)**

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.
2. Select the policy object and click **Edit**.
3. Click **Import > From File**... or **Operations > Import > From File**... (CPL or CPL Fragments).
4. Drag and drop the file into the **Select File** dotted-line area. Alternatively, browse to the file.
5. Click **Import**.

**Import Policy from a Device**

Importing policy from a device is useful in the following situations:

- You want to use a device’s currently installed policy as the starting point for a managed policy.
- A device has a policy configuration that you want to use as a policy template to deploy on other like device(s).

**Universal VPM Policy Considerations**

Although you can import universal VPM policy from a source that does not have enforcement domains enabled, you cannot deploy the policy unless you launch the VPM Editor and save a new revision of policy. This generates the CPL with enforcement domains enabled.

**Import from Device**

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.
2. Select a policy object or CPL fragment and click **Edit**.
3. Click **Import > From Device...** or **Operations > Import Policy > From Device...** The web console displays the Import Policy wizard.
4. From the **Source Device** drop-down list, select the device from which to import the policy configuration and click **Next**.
5. Select the policy that you want to import. Depending on whether the policy is a VPM or CPL policy, the deployment type is shown next to the policy:

- **VPM** - This policy contains policy created by the Visual Policy Manager and is deployed in the V slot.

- **Central** - This policy contains policy common to your entire organization and is deployed in the C slot.

- **Local** - This policy contains policy specific to your organizational structures, such as departmental policies or local (geographic-specific) policies and is deployed in the L slot.

- **Forward** - This policy contains forwarding rules for the policy and is deployed in the "F" slot.

- **Landlord** - Policy rules for tenant determination.

- **Default tenant** - Policy rules for all requests where tenancy cannot be determined during the initial connection.

- **Tenant** - Policy specifically for tenants.

For details on tenant policy, refer to the *Multi-Tenant Policy Deployment Guide*.

- **WSS** - Used for WSS targets *(universal VPM policy)* only.

6. Select **Import Policy**.

   The web console prompts you to confirm the overwrite of the existing policy in Management Center.

7. Click **Import and Overwrite** to accept the import.

8. (Optional) Click **Compare** to view the differences between an earlier version of a policy and the current version. See "Compare Different Versions of the Same Policy" on page 331.

9. Enter a comment for the commit operations and click **Save**. The comment that you enter is saved as metadata.

## Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export policy</td>
<td>&quot;Export Policy or Shared Objects to Local Disk&quot; on page 333</td>
</tr>
<tr>
<td>View existing policy information</td>
<td>&quot;View Existing Policy Information&quot; on page 319</td>
</tr>
<tr>
<td>Restore a version of the policy</td>
<td>&quot;Restore a Version of Policy&quot; on page 335</td>
</tr>
<tr>
<td>Deploy the policy, as is, to devices</td>
<td>&quot;Install Policy&quot; on page 302</td>
</tr>
</tbody>
</table>
**Import External Policy**

You can create a job to import a CPL fragment created in an external tool into Management Center. The job can be executed immediately, manually, or on a schedule. This is useful if you want to regularly sync the policy with the version on an external server.

Before you import an external policy, you need to create a policy object in Management Center into which to import the file.

**Prerequisites**

Before you create the Import External Policy job, you need to perform the following tasks:

1. Create the CPL in an external tool.
2. Create a policy object in Management Center. You will be importing the external file into this policy. See "Create a CPL Policy Object" on page 189.
3. (Optional) If you intend to use the URL as an absolute path to the policy target file:
   a. Edit the policy object and go to the Info tab. Record the Unique ID; you must name the external CPL file with this ID.
   b. Name the external policy file with the Unique ID of the Management Center policy.

   **Example:** 7B6F26F9–94FB–453C–B56F–8AE433ABDBBE.bpf

4. Store a file that contains the contents of the policy on a web, FTP, or SCP server.
5. Make note of the URL path to the file; you will need to specify the URL when defining the Import External Policy job.

*When the URL is used as an absolute path to the policy target file, Management Center attempts to fetch a file at the URL and store it as the content for the policy target(s) selected. If you have more than one target policy selected for the job, all the targets will be updated with the same content of the file.*

The Management Center default treats the URL as a directory and attempts to fetch files that match one of the IDs of the policy target(s). When the job executes, Management Center appends {id}.bpf to the URL for each of the policy targets in the job.

**Procedure**

To create a job for importing an external policy:

1. Click **Jobs > Scheduled Jobs**.
2. Select **New Job**. The web console runs the New Job wizard. An asterisk denotes fields that are mandatory.
3. Enter a **Name(*)** and **Description**.
4. Click **Next**. From the **Operation(*)** drop-down list, select **Import External Policy**.
5. Specify the location of the external policy file:

   - **Import from URL**: The path to the file on the external web, FTP, or SCP server.
     - **Directory URL Example**: ftp://company.com/policies/
     - **Absolute Path to File Example**: ftp://company.com/policies/7B6F26F9–94FB–453C–B56F–8AE433ABDBBE.bpf
   - **Username**: If authentication to the server is required, enter the name of user with permission to access the server.
   - **Password**: Enter the user's password.
Use URL as absolute path to file: This option is not selected by default.
- Leave this unselected if you want to load a large number of policies and do not wish to manage separate jobs for each.
- Select this option to treat the URL as an absolute path to the policy target(s).

If you have more than one target policy selected for the job, all the targets will be updated with the same content of the file.

7. For the Target, select the name of the policy object you created as a container for the imported external policy.
8. Click Next. Define a schedule to run the Import External Policy job. See “Job Scheduling Options” on page 436.

View Policy

To view policy, refer to the following.

"Preview Policy Before Installing It" on page 300
"View Existing Policy Information" on page 319
"View Deployed Policy for each Device Slot" on page 323
"View Devices Associated with Policy" on page 324

View Policy Versions

Management Center enables you to view CPL or VPM policy versions.

A policy file can have up to 99999 versions. By default, Management Center keeps an unlimited number of versions. In practice this will become an issue as storage is limited and eventually you would run out. So we have a housekeeping script to delete old version. It was limited to 999 and we changed it to 9999

1. Select Configuration > Policy.
2. From the Policy Objects list, select the policy name.
   - If needed, search for the policy object; see “Filter by Attributes and Keyword Search” on page 167.
3. With the policy selected, click Edit. The system displays the editor.
4. Select the Versions tab.

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Admin23</td>
<td>12/7/16 2:52 PM</td>
<td>asd</td>
</tr>
<tr>
<td>1.0</td>
<td>Admin23</td>
<td>12/7/16 2:51 PM</td>
<td>Initial revision</td>
</tr>
</tbody>
</table>
5. Select the policy version you want to view.

6. Click View. The Preview dialog displays.

CPL example:

![CPL example preview](image)

VPM example:
7. (Optional) To compare policy versions, see "Compare Different Versions of the Same Policy" on page 331.
8. (Optional) To restore an earlier version of the policy, See "Restore a Version of Policy " on page 335.
9. Click Close.
View Existing Policy Information

Whenever you create a version of policy, Management Center automatically saves information about it. This information is called metadata.

1. You can view metadata by selecting Configuration > Policy.
2. Select a policy and click Edit.

View Policy Object Information

1. Click the Info tab. The Version Control page displays all versions of the selected policy. An asterisk denotes fields that are mandatory.
2. Under General Information, the Overview displays the information you entered when creating the policy object:
   - **Policy name**(*)—The name of the Policy that you gave it when you created it
   - **Policy type**(*)—The Policy type can either be CPL or VPM.
   - **Description**—This is the Description that you entered when you created the policy. If you edit this field, make sure to click Save before leaving the Info tab.

   - **Replace substitution variables**

     Variable substitution is powerful and can be applied to policies and scripts. See "Use Substitution Variables in Policies and Scripts" on page 202.

3. Metadata displays under Latest Revision:
Management Center Configuration & Management

View Available Policy Versions

1. Click the **Versions** tab. The Version Control page displays all versions of the selected policy. When a policy object is created it is assigned the Version number 1.0. Every time that add attributes or edit it in any way, the version increases by increments of 0.1.

2. Select an early version of policy to compare.
3. Press and hold the Ctrl key while selecting the later version of policy to compare.

Version Number—When a policy object is first created, its version is 1.0. Each subsequent time the object is modified—for example, if the object properties are edited or when policy is added to it—the version number increments by 0.1. For example, when you add policy to an object and save it, the version becomes 1.1.

Date—The time and date stamp indicates when the policy was last updated.

Author—The author is the user who saved the current version of the policy.

Comments—If the author entered comments about the policy, they are displayed here. Metadata displays automatically-generated comments as follows:

- **Policy Object created**—When the policy container is initially created and policy has not been added yet.
- **Name changed**—When the policy name is edited.
- **Description changed**—When the policy description is edited.
- **Name and description changed**—When both the name and description are edited.

Of these metadata, the comments are usually the most important in helping you and other users understand the purpose and intent of creating the specific policy version. Symantec recommends that you always enter clear, helpful comments when creating policy.

View Associated Policy Attributes

1. Select the **Attributes** tab. The Attributes page displays all attributes currently assigned to this Policy. The attributes are custom attributes that you created. See "Add Attributes" on page 401 or "Edit Attributes" on page 404.
2. You can edit the Associated attributes. If you do, you need to save your changes. Click **Save**. Doing this actually increases the version number by an increment of 0.1.

Set the Maximum Number of Policy Versions to Store in Management Center

Each time you edit or import a policy, a revision of the policy is stored. By default, Management Center keeps an unlimited
number. However, this can result in storage issues so you are able to specify the number of revisions of policy to store before Management Center begins to prune. You can specify up to 9999 revisions.

1. Select the Administration > Settings. Click General. General fields display on the right. An asterisk denotes fields that are mandatory.
2. Select Maximum number of policy revisions to store.
3. Enter a number (limit) from 0 to 9999. If the you leave the value at 0, Management Center does not prune.
4. Do one of the following:
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server.
   - Click Activate to cause the server to load and apply the currently saved configuration.
**View Deployed Policy for each Device Slot**

1. From the **Network** tab, select a device.
2. Click **Edit**.
3. From the Edit Device wizard, select the **Policies** tab.

The deployment slots are not editable.

**Policies** are assigned to slots in the following ways:

- **Direct assignment** - The policy was installed directly to the slot and not inherited from the device group to which the device belongs.
- **Inherited from** [Device Group Name] - The policy was inherited from the device group to which the device belongs.

**Notes:**

- **Local**, **Central**, and **Forward** are CPL policy slots.
- **VPM Tenant** and **Landlord** can be either CPL and VPM.
- Policy deployed to the Landlord slot overrides any previous policy deployed to the Landlord slot.
View Devices Associated with Policy

You can view the devices that are associated with a policy.

1. Select Configuration > Policy. From the Policy Objects list, select the policy you want to view. If needed, filter on attributes. See "Filter by Attributes and Keyword Search" on page 167.

2. Click Edit. Select the Targets tab.

- Only those devices that can support the policy selected are displayed. This helps to know which policies can be installed on which devices.

3. For each device listed, verify the following:
   - **Enabled**—If selected, the policy that is installed on the device is enabled.
   - **Name**—The name that was entered in Management Center during device registration.
   - **Device Count**—The number of devices available.
   - **Device Model**—The device hardware model.
   - **Installed Version**—The version of policy installed on the device. If no version is listed, the device is still associated with policy, but policy has not been installed.
   - **OS Type**—The operating system on the device.
   - **State**—Displays historical association data for devices (whether deleted or not).
## Configure Policy

Configuring policy for specific devices or multiple devices at once involves several methods of creating, testing, and updating policy.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>What you can do</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write new policy; the behavior that you want is not yet expressed in policy in Management Center.</td>
<td>Create policy, which involves first creating a policy object.</td>
<td>&quot;Create a CPL Policy Object&quot; on page 189</td>
</tr>
<tr>
<td>Create a policy using the Visual Policy Manager.</td>
<td>Create a VPM Policy Object.</td>
<td>&quot;Launch Visual Policy Manager&quot; on page 210</td>
</tr>
<tr>
<td>Create rules to route traffic to the proper tenant.</td>
<td>Create tenant determination rules.</td>
<td>&quot;Specify Tenant Determination Rules &quot; on page 138</td>
</tr>
<tr>
<td>Specify rules to protect your WAF applications.</td>
<td>Create a WAF Application object.</td>
<td>&quot;Configure WAF Application Objects&quot; on page 145</td>
</tr>
<tr>
<td>Remove devices from policy or add devices to policy; you want to keep the policy but change the devices that use it.</td>
<td>Associate devices with, or disassociate devices from, a specific policy.</td>
<td>&quot;Add or Remove Devices Associated with Policy&quot; on the next page</td>
</tr>
<tr>
<td>Modify existing CPL policy because it does not behave as intended or has to be improved.</td>
<td>Refine the existing policy.</td>
<td>&quot;Refine Existing CPL Policy&quot; on page 193</td>
</tr>
<tr>
<td>Verify information about existing policy.</td>
<td>Check information about an existing policy.</td>
<td>&quot;View Existing Policy Information&quot; on page 319</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Add or Remove Devices Associated with Policy

Use the following procedure to add targets to associate with the selected policy.

Web Security Service (WSS) Target Considerations

Consider the following if you plan to add WSS as a target.

- You cannot add WSS and other devices (for example, a Content Analysis) as targets in the same operation because they have different deployment types. You must add WSS devices in a separate operation.
- Management Center must have a connection to the reference device at the time of installation. When installing policy, Management Center fetches data from the reference device, including non-policy configuration items like ICAP server data, and exception pages referenced by policy.
- For universal policy, appliance-only rules are blanked out before sending to the WSS. The rules are replaced with blank lines.

Add Targets

1. Select Configuration > Policy. From the Policy Objects list, select the policy you want to add to devices. If needed, search for the object; see "Filter by Attributes and Keyword Search" on page 167.
2. Select the policy name. Click Edit.
3. Click the Targets tab. To add targets to associate with the selected policy, click Add Targets.
4. From the Add Targets wizard, select the Devices tab. Select the checkbox by the device(s) name (or click Add to add a new device).

Only those targets that can support the policy selected are shown. This helps to know which policies can be installed on which targets (devices).
5. (Optional) To associate device groups with the policy, click the **Groups** tab and select **Devices**. This action immediately populates the **Selected** list.

6. To remove the selected devices, click **Unselect** or **Unselect All**. Click **Next**. The Add Targets wizard displays the **Add Targets: Configure Deployment** dialog.

7. From the **Deployment Type** drop-down list, select one of the following:
   - **VPM Slot** - Generated CPL (and the XML markup which persists the state of the VPM UI) pushed to the target’s VPM slot.
   - **Policy Slot** - The ProxySG appliance’s Local, Central, or Forward policy file.
   - **WSS** - Used for WSS targets (universal VPM policy) only.
   - **Landlord Slot** - Policy rules for tenant determination.
   - **Tenant Slot** - Policy specifically for tenants.

   **Note:** If you select **Tenant Slot** and a tenant is not configured, a "Tenant not configured" warning appears in the Deployment column on the Targets tab.

8. (If you selected Policy Slot) From the **Slot** drop-down list, select **Local**, **Central** or **Forward**.

9. Click **Finish**. A web console message displays the following:
Remove Targets

To remove devices associated with a policy, select the device name and click **Remove Targets**. You are asked to confirm that you want to remove the associated device(s). Click **Yes** or **No**.

---

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>View associated devices (targets)</td>
<td>&quot;View Devices Associated with Policy&quot; on page 324</td>
</tr>
<tr>
<td>Compare policy versions</td>
<td>&quot;Compare Different Versions of the Same Policy&quot; on page 331</td>
</tr>
<tr>
<td>Install a policy</td>
<td>&quot;Install Policy&quot; on page 302</td>
</tr>
<tr>
<td>Compare the policy version installed on the device, with the most current version saved in Management Center</td>
<td>&quot;Compare the Device Policy Version with Current Policy Version&quot; on page 332</td>
</tr>
<tr>
<td>Schedule a policy installation</td>
<td>&quot;Add a Job&quot; on page 430</td>
</tr>
<tr>
<td>Install multiple policies to multiple devices</td>
<td>&quot;Install Multiple Policies&quot; on page 307</td>
</tr>
</tbody>
</table>
Check Consistency between Policy and Devices

You can check if the policy saved in Management Center is different from the policy installed on devices.

1. To check the consistency of the installed policy with the devices, select Configuration > Policy and select a policy object.
2. Select the option by the policy name. Click Edit, and then click the Targets tab.
3. Select the device that you want to check for consistency against the policy stored in Management Center. Click Check Consistency. Select the base policy version by selecting the The latest policy version or the Version check box.

   If you don't select any devices, or you select a few and click Check Consistency, a consistency check is done on those devices, not just one. No selection of a device is required.

4. Click Check Consistency.

   ![Consistency Check](image)

   If you receive a Mismatch error for a device, the policy is inconsistent: either the policy was changed in Management Center and not installed to the device with the error, or the policy on the device was changed outside of Management Center.

5. You can click Compare Policy to determine what has changed.
6. (Optional) For each device listed, verify the following:

- The Management Center license contains all of the features for which you have purchased a subscription.
- The documentation covers all features, including ones that you may not have purchased.

- Policy is enabled (if Enabled is selected).
- Device Name—The name that was entered in Management Center during device registration.
- Device Count—The number of managed devices is shown in the banner.
- Device Model—The device hardware model.
- Installed Version—The version of policy installed on the device. If no version is listed, the device is still associated with policy, but policy has not been installed.
- OS Type—The operating system on the device.
- State—The status of the device. See "About Color-Coded Status Indicators" on page 34.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove associated devices.</td>
<td>&quot;Add or Remove Devices Associated with Policy&quot; on page 326</td>
</tr>
<tr>
<td>Compare different versions of the same policy.</td>
<td>&quot;Compare Different Versions of the Same Policy&quot; on the facing page</td>
</tr>
<tr>
<td>Install a policy or policies.</td>
<td>&quot;Install Policy&quot; on page 302 or &quot;Install Multiple Policies&quot; on page 307</td>
</tr>
<tr>
<td>View policy information.</td>
<td>&quot;View Existing Policy Information&quot; on page 319</td>
</tr>
</tbody>
</table>


**Compare Different Versions of the Same Policy**

As a troubleshooting step or as part of performance evaluation, you might want to identify the changes between an earlier version and a later version of policy. Management Center shows the changes made.

1. Select **Configuration > Policy**. From the **Policy Objects** list, select the policy name. If needed, search for the policy object; see "Filter by Attributes and Keyword Search" on page 167.
2. Select the **Versions** tab.
3. Select the versions of policy to compare (press and hold the Ctrl key while selecting the policy versions).
4. Click **Compare**. The system displays the Compare Policy dialog.

   - **CPL Example.**

   ![Compare Policy Example](image)

   - **VPM Example.**

   Starting in Management Center 1.6, you can diff the source code of VPM policy. To switch between the
Generated CPL and XML views, select the appropriate window.

The two policies are displayed side-by-side; the web console displays the version you selected first (earlier version) on the left and your second selection (later version) on the right.

- Policy highlighted in red exists in the former version and was removed in the later version.
- Policy highlighted in yellow indicates that a line exists in both versions of policy, but there are differences in the line.
- Policy marked in green does not exist in the former version and was added in the later version.
- Policy highlighted in white means the two copies are identical.

5. (Optional) To restore an earlier version of the policy, See "Restore a Version of Policy " on page 335.
6. Click Close.

**Compare the Device Policy Version with Current Policy Version**

You can compare the policy version installed on the device with the current policy version that is stored in Management Center.
Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>View all of the details about an existing policy, including policy object information, the policy version, and the associated attributes.</td>
<td>&quot;View Existing Policy Information&quot; on page 319</td>
</tr>
<tr>
<td>Compare different versions of the same policy.</td>
<td>&quot;Compare Different Versions of the Same Policy&quot; on page 331</td>
</tr>
</tbody>
</table>

Export Policy or Shared Objects to Local Disk

You can export policy objects from the **Policy** or **Shared Objects** grid. The policy is exported in JSON format. If you export multiple policy objects, they are collected and exported in a single JSON file.

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.
2. Select one or more policy objects.
3. Click **Export**.
4. Depending on your browser settings, you may be prompted to view or save the file. Click Save if prompted. In other cases, the file is automatically saved to local disk (typically, the Downloads folder).
Restore a Version of Policy

After time, you might find that the policy pushed to devices needs improvement or must change because of changes in business requirements or practices. In such situations, you can modify policy as needed, or revert to an earlier version of policy that is appropriate. When you have determined which version of policy to restore, you can restore it using the version history.

1. Select **Configuration > Policy**. From the **Policy Objects** list, select the policy name. If needed, search for the object; see "Filter by Attributes and Keyword Search" on page 167.
2. Click **Edit**. Click the **Versions** tab. Versions of the policy are listed in descending numerical order.
3. From the **Version Control** page, verify that the version you want to restore is the correct one. Perform one or both of the following as required.
   - Check the version metadata. See "View Existing Policy Information" on page 319.
   - Compare versions of policy. See "Compare Different Versions of the Same Policy" on page 331
4. After you identify the version to restore, select it and click **Restore**. The web console displays the Restore dialog.
5. In the **Comment** field, specify the reason for the restore.
6. Click **Restore**.
   The restored version of the policy is incremented to the latest version in the **Policy** list, and the comment you entered in step 6 is displayed in the **Comments** column.
7. To install the restored policy to associated devices, select the policy and click **Install Policy**. See "Install Policy" on page 302.

Use Specific Attribute Values to Control Access to Policy

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Attributes are custom metadata used to refine and edit devices, device groups policy, and scripts. These attributes can be used to control access to policy, as described below.

Procedure

1. **Create** the **Policy** attribute.
2. Associate the attribute with a policy object.
   a. Select **Configuration > Policy**.
   b. Select the policy name and click **Edit**.
      The system displays the policy editor.
   c. Select the **Attributes** tab.
   d. Select the attribute and click **Save**.
3. Add the permission rule to a new or existing role.
   a. Select **Administration > Roles**.
   b. Select an existing role and click **Edit** or click **Add Role**.
   c. If this is a new role, provide a name and description, and click **Next**.
   d. **Symantec recommends that you enter a list of the permissions for the defined role in the Description field. This helps you and other users understand the permissions of a user's role including the intent of their job function.**
In the Add Role: Permissions dialog, click Add Permission.

f. In the Object list, specify Policy.

g. In the Action list, select All operations or a specific operation.

h. In the Filter section, click the Add Filter icon.

i. In the Filter Type section, select Attribute has specific value.

j. Select the attribute and assign a value to it.

k. Click Save, then Finish.

Create Shared Objects

Shared objects are policy elements that can be referenced by multiple policy objects. A shared object cannot be deployed by itself; it must be included in another policy type, such as CPL or a WAF Application.

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit ${include} and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

Users are warned if they attempt to delete a shared object currently assigned to a policy object. The error message lists all policies to which the shared object is assigned. When presented with the message, the user must confirm the deletion by selecting I understand that once I choose to delete the Object above, this action cannot be undone.

Create CPL Fragments

CPL policy fragments are reusable building blocks of CPL policy. Because fragments are not complete CPL policy, you do not deploy them to devices but include them within policy that you deploy to devices.

"Create a CPL Policy Fragment" on page 223
Create a Category List

A category list is a named set of URL categories that can be easily referenced in policy, allowing you to assign an allow or deny condition to all the categories in one simple rule, or reuse the list in multiple policy rules.

Create a Category List Template

A category list template provides a starting point for defining which categories to include in a category list. The template contains a subset of the complete list of WebPulse categories, typically used to restrict the categories a less-privileged user can select when creating a category list.

Create a URL List

URL lists allow you to easily create URL exceptions to your policy. The URL list can be easily included in your existing policy.

Create an IP Address List

Easily create IP address lists for use on the SSL Visibility appliance.

Manage List Triggers

When you create a URL or category list, Management Center includes subconditions and associated triggers optimized for the type of URL or category entered. These triggers are enabled by default but you have the option to disable some of them.

Create WAF Security Profile

A WAF Security Profile is a shared object that defines the Web Application Firewall settings for the associated WAF application object. The WAF Security Profile is assigned to one or more WAF applications that can be installed on ProxySG appliances to set WAF policy.
When defining users, groups, roles and grant permissions, refer to the following for important information.

"Reference: Permissions Interdependencies" on the facing page

"Reference: Permissions Filters Object and Attributes" on page 393

"Reference: Understanding Job Permissions" on page 352
Reference: Permissions Interdependencies

When adding permissions to roles, remember that users can access an object as long as they have a role with the required permission. For example, if a user is added to a role which allows access to only one device group and a role that has View permissions for all devices, the user can see all devices in all groups.

Refer to the following permission objects to determine specific dependencies.

The View permission is implied in all higher permission levels except for Add. To reduce the number of permissions in a role, you can remove the View permission if a higher-level permission for the same object exists in the role. For example, if a role already has the Policy - Update permission for importing policy, you do not have to add the Policy - View permission for adding policy jobs.

### All objects

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all functions in all areas of the web console</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View all areas of the web console</td>
<td>None</td>
</tr>
</tbody>
</table>

### Attribute Definition

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Add, delete, and edit attributes</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Add attributes</td>
<td>Attribute Definition - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete attributes</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Edit attributes</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View attributes</td>
<td>None</td>
</tr>
</tbody>
</table>

### Audit

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all audit log functions</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to audit log records</td>
<td>None</td>
</tr>
</tbody>
</table>

Backup Image
### Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Import, export, delete, and restore image backups</td>
<td>Management Center - View  Management Center - Update</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete backups</td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Export backups</td>
<td></td>
</tr>
<tr>
<td>Import</td>
<td>Import backups</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Restore backups</td>
<td>Management Center - View  Management Center - Update</td>
</tr>
<tr>
<td>View</td>
<td>View information about existing backups</td>
<td></td>
</tr>
<tr>
<td>View Contents</td>
<td>View the backup contents</td>
<td></td>
</tr>
</tbody>
</table>

### Device

When using filters with a specified value, make sure that the value exactly matches the value in the device properties. See "Set User-Defined Device Attributes for Access Control" on page 405 and "Reference: Permissions Filters Object and Attributes" on page 393.

<table>
<thead>
<tr>
<th>Permission Action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All device functions</td>
<td>Hierarchy - View</td>
<td>To see the effective policy for a device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To change membership in device properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Group - Change Membership</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To see groups to which the device belongs (not needed if assigning Change Membership):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Group - View</td>
</tr>
<tr>
<td>Add</td>
<td>Add devices</td>
<td>Hierarchy - View</td>
<td>To add devices by importing from a file:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - Change Membership</td>
<td>Device - Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td>Device - Update</td>
</tr>
<tr>
<td>Backup</td>
<td>Back up devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup Image - Update</td>
<td></td>
</tr>
<tr>
<td>Permission Action</td>
<td>Allows access to these areas/functions</td>
<td>Requires these permissions to be useful</td>
<td>Grant these permissions for more functions</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td>Install Policy</td>
<td>Install policy to devices</td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td>Manage</td>
<td>Activate and deactivate devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restore</td>
<td>Restore configuration backups to devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup Image - Update</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Edit device basic information, connection parameters, and attributes</td>
<td>Hierarchy - View</td>
<td>To change membership in device properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td>Device Group - Change Membership</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To add devices by importing from a file:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device - Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device - Update</td>
</tr>
<tr>
<td>View</td>
<td>View device information</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
</tbody>
</table>

**Device Group**

When using filters with a specified value, make sure that the value exactly matches the value in the device group properties. See "Set User-Defined Device Attributes for Access Control" on page 405 and "Reference: Permissions Filters Object and Attributes" on page 393.
### Management Center Configuration & Management

#### Permission action

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all device group functions</td>
<td>Hierarchy - View</td>
<td>To see the devices in groups: Device - View</td>
</tr>
<tr>
<td>Add</td>
<td>Add device groups</td>
<td>Hierarchy - View</td>
<td>To associate devices while adding a group: Device - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - Change Membership</td>
<td>To add device groups or hierarchies by importing from a file: Device Group - Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - Update</td>
<td></td>
</tr>
<tr>
<td>Change Membership</td>
<td>Change associated groups in device properties</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - Update</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Delete device groups</td>
<td>Hierarchy - View</td>
<td>To add device groups or hierarchies by importing from a file: Device Group - Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Edit device groups’ basic information and attributes</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to device groups</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
</tbody>
</table>

### Device Script

#### Permission action

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All functions related to script</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Add script objects</td>
<td>Device - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete script objects</td>
<td>None</td>
</tr>
<tr>
<td>Edit Metadata</td>
<td>Edit script object attributes and information</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Edit and execute script content</td>
<td>Device - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - Manage</td>
</tr>
<tr>
<td>View</td>
<td>View script</td>
<td>None</td>
</tr>
</tbody>
</table>

**Note:** "Compare Versions of the Script" on page 160 is available at this level.
### Hierarchy

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for ancillary functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Add, delete, and edit hierarchies</td>
<td>Device Group - All operations</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add hierarchies</td>
<td>Hierarchy - View</td>
<td>To add device groups or hierarchies by importing from a file:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - All operations</td>
<td>Device Group - Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Group - Update</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete hierarchies (except for the predefined hierarchies)</td>
<td>Device Group - Delete</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Edit hierarchies</td>
<td>Device Group - Update</td>
<td>To add device groups or hierarchies by importing from a file:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Group - Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Group - Update</td>
</tr>
<tr>
<td>View</td>
<td>View hierarchies</td>
<td>Device Group - View</td>
<td>To see devices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device - View</td>
</tr>
</tbody>
</table>

### Management Center

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all Management Center functions.</td>
<td>None</td>
</tr>
<tr>
<td>Backup</td>
<td>Perform Management Center backup and restore.</td>
<td>None</td>
</tr>
</tbody>
</table>

### Policy

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All functions related to policy</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add policy objects</td>
<td>Policy - View</td>
<td>To assign targets while adding a policy object:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy - Assign Target</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission action</td>
<td>Allows access to these areas/functions</td>
<td>Requires these permissions to be useful</td>
<td>Grant these permissions for more functions</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Assign Targets</td>
<td>Add and remove target devices</td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td>CPL - Add Section</td>
<td>Add policy sections to existing policy objects</td>
<td>None</td>
<td>To add policy sections while adding a new policy object: Policy - Add</td>
</tr>
<tr>
<td>CPL - Delete Section</td>
<td>Delete policy sections</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CPL - Edit Default</td>
<td>Edit the default sub-section in policy sections</td>
<td>* CPL - Edit Override - Consider granting this permission to senior roles only. Granting this permission allows users to edit the Override sub-section in all policy sections, which could have unintended results.</td>
<td></td>
</tr>
<tr>
<td>CPL - Edit Mandatory</td>
<td>Edit the mandatory sub-section in policy sections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPL - Edit Override*</td>
<td>Edit the override sub-section in policy sections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPL - Move Section</td>
<td>Move policy sections within policy objects</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CPL - Update Section</td>
<td>Edit the name and purpose of sections</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Delete policy objects</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Edit Contents</td>
<td>Restore previous versions of policy and edit policy</td>
<td>None</td>
<td>To select a reference device: Device - View</td>
</tr>
<tr>
<td>Edit Metadata</td>
<td>Edit policy object attributes and information</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Import</td>
<td>Import policy from devices</td>
<td>Device - View</td>
<td>Policy - Update</td>
</tr>
</tbody>
</table>

**Note:** Because Management Center imports policy as one section, it might be useful to grant some policy section permissions in some cases (for example, to allow users to break down the imported policy into sections and sub-sections).
### Permission action

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish</td>
<td>Install policy on target devices</td>
<td>None</td>
<td>To add/remove target devices to policy before installing:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device - Manage</td>
</tr>
<tr>
<td>View</td>
<td>View policy</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Edit &gt; Check Consistency is available at this level.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Report

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all Appliance Monitoring reports and functions</td>
<td>None</td>
<td>To filter reports and report widgets by device or device group:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Group - View</td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to reports</td>
<td>None</td>
<td>Device - View</td>
</tr>
</tbody>
</table>

### Role

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All role functions</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Users can add roles</td>
<td>Role - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Users can delete roles</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Users can update roles</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to roles</td>
<td>None</td>
</tr>
</tbody>
</table>

### Scheduled Job

Job permissions are distinct from the operational permissions. If you have unexpected results or 'access denied' errors when running jobs, see "Reference: Understanding Job Permissions" on page 352.
<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Add, edit, delete, enable, disable, and run jobs; view job progress, current jobs, and job history</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add jobs</td>
<td>Scheduled Job - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Caution: Scheduled Job - Add is an elevated permission. See &quot;Reference: Understanding Job Permissions&quot; on page 352.</td>
<td>Device - View</td>
<td>(For policy jobs) Policy - View</td>
</tr>
<tr>
<td>Cancel Running Job</td>
<td>Cancel all active, running jobs</td>
<td>Scheduled Job - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td>(For policy jobs) Policy - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete jobs</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Run Manually</td>
<td>Run jobs manually using the Run Now option</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Edit jobs' information and schedule; enable/disable jobs</td>
<td>None</td>
<td>To view devices and add/remove targets:</td>
</tr>
<tr>
<td></td>
<td>Caution: Scheduled Job - Update is an elevated permission. See &quot;Reference: Understanding Job Permissions&quot; on page 352.</td>
<td></td>
<td>Device - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To add/remove policies from a job: Policy- View</td>
</tr>
<tr>
<td>View</td>
<td>View all scheduled and current jobs and job history</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: All users can see the Jobs tab in the web console, even if they do not have a Scheduled Job - View permission.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Session**

Session permissions are specifically to control access to user sessions.

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>View, kill, disable logins</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View active sessions</td>
<td>None</td>
</tr>
</tbody>
</table>
### Permission action

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kill Session</td>
<td>Kill an active session</td>
<td>None</td>
</tr>
<tr>
<td>Disable Logins</td>
<td>Enable or Disable logins to Management Center</td>
<td>None</td>
</tr>
</tbody>
</table>

### Settings

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all settings functions in Administration Settings (Hardware Diagnostics is always read-only)</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Edit Management Center Settings</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View Management Center Settings, and Hardware Diagnostics</td>
<td>None</td>
</tr>
</tbody>
</table>

### User

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all user functions</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add users and specify basic information</td>
<td>User - View</td>
<td>To assign roles while adding a user: Role - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete users</td>
<td>None</td>
<td>To add or remove roles from a user: Role - View</td>
</tr>
<tr>
<td>Update</td>
<td>Update users' basic information and change/expire user passwords</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>View users</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

### User Group
### Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all user group functions</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add user groups</td>
<td>User Group - View</td>
<td>To add or remove group roles while adding a user group: Role - View To add or remove group roles while adding a user group: User - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete user groups</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Update user groups’ basic information</td>
<td>None</td>
<td>To add/remove users from groups: User - View</td>
</tr>
<tr>
<td>View</td>
<td>View user groups</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Reference: Permissions Filters Object and Attributes**

Although you are not restricted to the user-defined system attributes of **Location** and **Rack**, the following helps to determine which filters to use for the Device and Device Group permissions.

**Set Filters for Device Object**

Specify Rack and Location attributes. See "Set User-Defined Device Attributes for Access Control" on page 405 for information.

<table>
<thead>
<tr>
<th>Select the Attributes type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute has specific value</td>
<td>Attribute: Select Rack. Value: Specify the rack. Click Save. The Filter field displays &quot;Rack is '&lt;value&gt;'&quot;.</td>
<td>Devices specified with this rack in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Attribute: Select Location. Value: Specify the location. Click Save. The Filter field displays &quot;Location is '&lt;value&gt;'&quot;.</td>
<td>Devices specified with this location in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

348
<table>
<thead>
<tr>
<th>Select the Attributes type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute has any value</td>
<td>Attribute: Select <strong>Rack</strong>. Click <strong>Save</strong>. The Filter field displays &quot;<strong>Rack</strong> is not empty&quot;.</td>
<td>Devices specified with any rack specified in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td></td>
<td>Attribute: Select <strong>Location</strong>. Click <strong>Save</strong>. The Filter field displays &quot;<strong>Location</strong> is not empty&quot;.</td>
<td>Devices specified with any location in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Specific Device</td>
<td>Device: Select a device from the drop-down list. Click <strong>Save</strong>. The Filter field displays &quot;Specified Device&quot;.</td>
<td>This selected device.</td>
</tr>
<tr>
<td>Members of specific group</td>
<td>Hierarchy: Select a hierarchy. Your selection determines the values for device group. Device Group: Select the device group. Click <strong>Save</strong>. The Filter field displays &quot;Members of specified group&quot;.</td>
<td>All devices in the specified group or its sub-groups.</td>
</tr>
</tbody>
</table>
### Set Filters for Device Group Object

Specify Primary Contact and Location attributes. See "Set User-Defined Device Attributes for Access Control" on page 405 for information.

<table>
<thead>
<tr>
<th>Select the Filter type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute has specific value</td>
<td>Attribute: Select <strong>Primary Contact</strong>&lt;br&gt;Value: Specify the contact.&lt;br&gt;Click <strong>Save</strong>. The Filter field displays &quot;Primary is '{value}'&quot;.</td>
<td>Groups specified with this primary contact in group properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Attribute has any value</td>
<td>Attribute: Select <strong>Primary Contact</strong>&lt;br&gt;Click <strong>Save</strong>. The Filter field displays &quot;Primary Contact is not empty&quot;.</td>
<td>Groups specified with any primary contact in group properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Specific Device Group</td>
<td>Hierarchy: Select a hierarchy. Your selection determines the values for device group.&lt;br&gt;Device Group: Select the device group.&lt;br&gt;Click <strong>Save</strong>. The Filter field displays &quot;Specified Device Group&quot;.</td>
<td>The specified device group.</td>
</tr>
<tr>
<td>Members of specific group</td>
<td>Hierarchy: Select a hierarchy. Your selection determines the values for device group.&lt;br&gt;Device Group: Select the device group.&lt;br&gt;Click <strong>Save</strong>. The Filter field displays &quot;Members of specified group&quot;.</td>
<td>The sub-groups of the specified group (but not the group itself).</td>
</tr>
</tbody>
</table>

### Set Filters for Policy Object

Filter permissions for specific policies. See "Edit Attributes" on page 404.
### Set Filters for Scheduled Job

Filter permissions for scheduled jobs. Limits the user to working with specific jobs or all jobs created by a user.

<table>
<thead>
<tr>
<th>Select the Filter type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner (Created by)</td>
<td>Select Current User or Specific User. Click <strong>Save</strong>.</td>
<td>All jobs from created by the specified user.</td>
</tr>
<tr>
<td>Specific Scheduled Job</td>
<td>Select a specific, scheduled job. Click <strong>Save</strong>.</td>
<td>The specified job.</td>
</tr>
</tbody>
</table>

For more information about user-defined attributes, see "Manage Attributes" on page 400.
Reference: Understanding Job Permissions

A job is distinct from the operation (such as backing up devices and installing policy) that the job executes. When a user creates a job, he/she defines its operation, targets, and schedule. If a user has permissions to add or update jobs, he or she can configure and save any job.

Users can run jobs in Management Center in the following ways.

User runs a job immediately after configuring it or manually using Run Now

- The job executes as the user.
- The Audit Log displays the event as a Job Execution and lists the username as the Operating User.
- The job information shows that it was started by the user.

As long as the user has the job permissions, running a job immediately or manually always results in a completed job. In the previous scenario, if the user has permissions to perform the operation, the job completes without errors; if the user has insufficient permissions to perform the operation, the job completes with errors.

User configures a job scheduled in the future

- The job executes as the system.
- The Audit Log displays the event as a Job Execution and lists SYSTEM as the Operating User.
- The job information shows that it was started by the system.

Because the job executes as the system, which can perform all operations, users with permissions to schedule jobs can create jobs for an operation that they do not have permissions to perform. Allowing more users than necessary to schedule jobs is thus a potential security risk.

Consider granting the Scheduled Job - Run Now permission to most users who require the ability to run jobs. Reserve the Scheduled Job - Add and Scheduled Job - Update permissions for the most senior users.
Configure Users, Roles, and Attributes

As the Management Center administrator, you can specify the following global settings after you set up Management Center for the first time or when needed.

"Manage Management Center Users" on the next page
"Define Roles " on page 386
"Filter Devices or Device Groups in a Permission" on page 393
"Manage Attributes" on page 400
"Preview or Download Logs" on page 409
"Customize the Audit Log" on page 562
Manage Management Center Users

The Users tab allows you to manage access Management Center. Before adding users, make sure you have defined roles.

See the following topics for details:

- "Add Local Users" on page 357
- "View, Edit, or Delete User Accounts" on page 372
- "Manually Reset a User's Web Console Password" on page 378
- "Expire a User's Web Console Password" on page 378

Add Users and Grant Permissions

Management Center employs a role-based security model for access control, which consists of defining roles and then adding users to roles rather than granting explicit rights to features and functions.

You should create a role structure that ensures:

- Users have enough access—and no more—to perform their day-to-day jobs.
- Only authorized users can access sensitive features and data.
- The permissions that a defined role requires.
- Enforcement of your organization’s access control policies.

To configure access control in Management Center, create a role structure that meets your technical and business requirements. As your organization changes, you may need to change role definitions and assignments to be certain that users continue to have appropriate access.
Users (based on their role) should only manage specific devices, including reports on those devices.

User roles control the actions that individuals within an organization should perform on devices for which they have access.

Users roles should be organized into a hierarchical control model to conform to an organization's IT structure.

Define Roles and Users

To control access to Management Center, you should first create each role to allow access to specific areas and the operations that users can perform there; then, you can assign these roles in accordance with users’ functions and responsibilities.

1. Define roles to provide access to different areas and functions in the Management Center.
   - To create a new role, see "Define Roles" on page 386.
   - To duplicate an existing role, see "Duplicate an Existing Role" on page 388
   - (Optional) "Edit an Existing Role" on page 388.

2. "Add Local Users" on page 357 after you have created a role structure and defined roles.

   (Optional) "Add User Groups" on page 381. If multiple users require the same type of access to Management Center, user groups make it easy to apply roles and permissions to a large number of users at one time. User groups contain users that control access to Management Center; you should first create each role to allow access to specific areas and the operations that users can perform there; then, you can assign roles in accordance with users’ functions and responsibilities.

Grant Permissions

To grant permissions to Management Center that a role requires, you should understand how permissions work with roles. Grant permissions to users based on the actions you need them to perform on specific objects. See "Reference: Permissions Interdependencies" on page 339.

- "Grant Permissions" on page 390 to users. See "Reference: Permissions Filters Object and Attributes" on page 393.
- (Optional) Grant job permissions to users. See "Reference: Understanding Job Permissions" on page 352

(Optional) Filter Devices in Permissions

(Optional) Filter devices or device groups in permissions. Some permissions allow access at the device and device group levels.

- To specify devices or device groups in specific permissions, see "Filter Devices or Device Groups in a Permission" on page 393.
- To specify object filters, see "Reference: Permissions Filters Object and Attributes" on page 393.

(Optional) Add Users from External Directory Services

To authenticate users using RADIUS, LDAP or Active Directory services, see Add Users from an Existing Directory Service. Available directory services to which you can authenticate users include:
- "Authenticate Users Against Active Directory LDAP" on page 363
- "Authenticate Users Against LDAP" on page 360
- "Authenticate Users Against RADIUS" on page 365
Add Local Users

Use these settings to provide Management Center access to local users.

Security Considerations

The following items are supported today:

- Management Center logs all access attempts to the audit log and syslog.
- Administrators can manually expire a user’s password and force them to enter a new one.
- Starting with 1.7, Management Center tracks the last access attempt in the user record and displays the record when viewing the user’s details (Administration > Users).
- Starting with 1.7, Management Center tracks the number of login failures a user has had in a row.

The following items are not supported:

- Management Center does not enforce password strengths.
- Passwords do not expire automatically. You can manually expire them.
- Management Center does not automatically disable accounts if the user does not enter their password correctly after $n$ attempts.
- Management Center does not track password history.

If the unsupported features are important to you, use an external authentication service like LDAP, Active Directory LDAP, or RADIUS instead.

Add Roles First

You can add local users to Management Center at any time, but it is good practice to set up the role structure before you start adding users. After roles have been added, you can assign users the specific roles that they require to perform their jobs. It is best practice to assign the most restrictive permissions possible so that users do not have more access than they need. To import users from Active Directory, LDAP or RADIUS, see Authenticate Users and User Groups using Existing Directory Service.

When you select an existing user record, user details open in the right pane. In the title bar, under the user name, the local user account indicates a user that you manually added and the imported user account indicates a user that you imported using an existing directory service.

To understand more about how permissions and filters work with users and roles in Management Center, see "Reference: Permissions Filters Object and Attributes" on page 393 and "Reference: Permissions Interdependencies" on page 339.

Add Users

Before you start adding users, devise the naming convention for usernames. Once a username is saved, it cannot be changed. This does not apply to imported users—their usernames are set in LDAP, Active Directory, or RADIUS and are thus read-only.
1. Select **Administration > Users**.

2. Click **Add User**. The Add User: Basic Info dialog displays. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username *</td>
<td>Usernames are case-sensitive and cannot be changed.</td>
</tr>
<tr>
<td>Note:</td>
<td>Although the username/password combination successfully authenticates if the</td>
</tr>
<tr>
<td></td>
<td>username has a mixture of cases, Management Center recognizes the users as</td>
</tr>
<tr>
<td></td>
<td>different users. For example: A user signs in as “joe” and access is setup</td>
</tr>
<tr>
<td></td>
<td>using that specific case for username. Then later the user signs in as “Joe”.</td>
</tr>
<tr>
<td></td>
<td>The login using “Joe” will have no access because the account created is for</td>
</tr>
<tr>
<td></td>
<td>the user “joe”.</td>
</tr>
<tr>
<td>Password *</td>
<td>Example: admin1234</td>
</tr>
<tr>
<td>Verify Password *</td>
<td>Example: admin1234</td>
</tr>
<tr>
<td>Password expired on:</td>
<td>Does not expire</td>
</tr>
<tr>
<td>First Name</td>
<td>The actual first name that the person uses.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The actual last name that the person uses.</td>
</tr>
<tr>
<td>Email</td>
<td>The Email associated with this user and organization. Example <a href="mailto:joe@heremail.com">joe@heremail.com</a></td>
</tr>
<tr>
<td>Phone</td>
<td>The Phone number associated with this user and organization (including</td>
</tr>
<tr>
<td></td>
<td>extension, if any)</td>
</tr>
<tr>
<td>Mobile</td>
<td>The personal mobile or cell number associate with this person.</td>
</tr>
<tr>
<td>Description</td>
<td>1024 character description can include anything from what town she resides</td>
</tr>
<tr>
<td></td>
<td>to average commute time to security certifications in this user’s possession.</td>
</tr>
</tbody>
</table>

3. In the **Add User: Basic Info** screen, enter the user’s information.

4. Click **Next**. From the Add User: Assign Roles dialog, select a role from **Available Roles** and add it **Assigned Roles**. The default roles are Administrator (with administrator rights) and viewOnly (with only viewing rights). You must assign a role or the user will be unable to login to Management Center. See "Define Roles " on page 386 or "Edit an Existing Role" on page 388.

5. Click **Finish**. The new user displays in the Users list and has access to Management Center based on their defined role.
Add Users from an Existing Directory or Service

As the Management Center administrator, you can add from an existing directory or service.

"Authenticate Users Against LDAP" on the next page

"Authenticate Users Against Active Directory LDAP" on page 363

"Authenticate Users Against RADIUS" on page 365
Authenticate Users Against LDAP

These options configure LDAP or LDAPS (LDAP over SSL) authentication in Management Center.

A secondary failover LDAP server can be configured in case the primary LDAP server cannot authenticate. If the secondary LDAP server cannot authenticate, authentication can only occur through Active Directory LDAP or RADIUS (if configured).

Prerequisites

If you are configuring LDAPS and the LDAP server SSL key uses a self-signed certificate or a certificate signed by a non-trusted root certificate authority, you must import that certificate into Management Center. To import the certificate, use the `security ssl import external-certificate` command.

Configure General Settings

1. Select Administration > Settings.
2. Click LDAP on the left. The web console displays fields on the right. An asterisk denotes fields that are mandatory.
3. Specify general LDAP settings as described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must have permission</td>
<td>A user must have a role with permissions or be a member of a group with a role that has permissions in order to log in.</td>
<td>false</td>
</tr>
<tr>
<td>Role attribute</td>
<td>Specify the roles to assign to imported users. Use the same name that exists in LDAP, ensuring that the spelling and case are identical.</td>
<td>businessCategory</td>
</tr>
<tr>
<td>Display name attribute</td>
<td>Specify the format of user names.</td>
<td>displayName</td>
</tr>
</tbody>
</table>

Configure Primary Server Settings

1. Select Administration > Settings.
2. Select LDAP. The web console displays fields on the right. An asterisk denotes fields that are mandatory.
3. Enter the Primary Server Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable LDAP authentication.</td>
<td>false</td>
</tr>
<tr>
<td>LDAP URL*</td>
<td>The URL used to connect to the LDAP directory server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify the LDAP host, port, and root. Example: ldap://localhost:10389/dc=example,dc=com LDAPS example ldaps://ldapservr1:3269/dc=example,dc=com</td>
<td></td>
</tr>
</tbody>
</table>
Configure Secondary Server Settings

You can also configure a **Secondary LDAP Server** to take over in case the Primary Server fails. The settings under **Secondary Server** are specific to the Secondary LDAP Server only. The settings under **Secondary RADIUS Server** are specific to the secondary server only.

1. Select **Administration > Settings**.
2. Select **LDAP**. The web console displays fields on the right. An asterisk denotes fields that are mandatory.
2. Enter the Secondary Server Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login user</td>
<td>If required, enter the username used for browsing.</td>
<td>Specify the username.</td>
</tr>
<tr>
<td>Login password</td>
<td>If required, enter the password used for browsing.</td>
<td>Specify the password.</td>
</tr>
</tbody>
</table>

Configure Search Settings

1. Select **Administration > Settings**.
2. Select **LDAP**. The web console displays fields on the right. An asterisk denotes fields that are mandatory.
2. Configure the LDAP Search Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable LDAP authentication.</td>
<td>false ☐</td>
</tr>
<tr>
<td>LDAP URL*</td>
<td>The URL used to connect to the LDAP directory server.</td>
<td>Specify the LDAP host, port, and root. Example: ldaps://localhost:10389/dc=example,dc=com</td>
</tr>
<tr>
<td>Login user</td>
<td>If required, enter the username used for browsing.</td>
<td>Specify the username.</td>
</tr>
<tr>
<td>Login password</td>
<td>If required, enter the password used for browsing.</td>
<td>Specify the password.</td>
</tr>
</tbody>
</table>
Setting | Description | Input Value/Format
--- | --- | ---
**Base DN for group search** | Specify where in the LDAP directory tree to initiate the username search. | Example: ou=groups
**Attribute to read group name** | Specify the group name attribute. Use the same name that exists in LDAP, ensuring that the spelling and case are identical. | Example: cn
**Search sub-tree** | Specify whether to search sub-tree. | false|true

**Finalize Your Changes**

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

After setting your configuration options, you must do one of the following:

1. Reset or commit your changes.
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server. If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

2. Instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.

**Supported LDAP Servers**

<table>
<thead>
<tr>
<th>Server Types</th>
<th>Configuration Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache DS</td>
<td>Apache Directory Studio™ user interface</td>
</tr>
<tr>
<td>Novell eDirectory</td>
<td>Novell ConsoleOne user interface</td>
</tr>
</tbody>
</table>

**Add LDAP Users**

After LDAP is configured, have users log in with their LDAP credentials. The first time the user logs in, Management Center adds them to the system. You cannot add external users at this time.
Authenticate Users Against Active Directory LDAP

Set up Active Directory LDAP authentication in Management Center. A secondary failover Active Directory LDAP server can be configured in case the primary Active Directory LDAP server cannot authenticate. If the secondary Active Directory LDAP server cannot authenticate, authentication can only occur through LDAP or RADIUS (if configured).

Prerequisites for enabling **Sync the role membership** and **Sync the group membership**:

- To sync role membership, you must define the role in Management Center before users assigned to the role in Active Directory authenticate.
- To sync group membership, you must define the group in both Management Center and Active Directory. The group names must match in order to map correctly.

After you define the roles and groups, and when a user authenticates in Management Center, the appropriate roles and/or group memberships are set up in Management Center.

Specify General Active Directory LDAP settings.

1. Select **Administration > Settings**.
2. Select **Active Directory LDAP**. The web console displays fields on the right. An asterisk denotes fields that are mandatory.
3. Enter the General Active Directory LDAP Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sync the role membership</strong></td>
<td>Specify whether to assign users to roles that match the Role Attribute setting. No roles are synchronized if the Role Attribute is not set.</td>
<td>false</td>
</tr>
<tr>
<td><strong>Sync the group membership</strong></td>
<td>Specify whether to assign users to a user group that matches a group in Active Directory. The spelling and case must be identical to match.</td>
<td>false</td>
</tr>
<tr>
<td><strong>User must have permission</strong></td>
<td>A user must have a role with permissions or be a member of a group with a role that has permissions in order to log in.</td>
<td>false</td>
</tr>
<tr>
<td><strong>Role attribute</strong></td>
<td>Specify the roles to assign to imported users. Use the same name that exists in Active Directory, ensuring that the spelling and case are identical.</td>
<td>Specify the department to which the role is assigned.</td>
</tr>
<tr>
<td><strong>Display name attribute</strong></td>
<td>Specify the format of user names.</td>
<td>displayName</td>
</tr>
</tbody>
</table>

Specify Primary Server Settings

1. Select **Administration > Settings**.
2. Select **Active Directory LDAP**. The web console displays fields on the right. An asterisk denotes fields that are mandatory.
3. Enter the Primary Server Settings described in the following table.
### Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Is the authenticator enabled</strong> *</td>
<td>Enable AD authentication.</td>
<td>false</td>
</tr>
<tr>
<td><strong>LDAP URL</strong> *</td>
<td>The host URL for LDAP authentication.</td>
<td>Example: ldap://localhost:389</td>
</tr>
</tbody>
</table>

### Specify Secondary Server Settings

You can also configure a **Secondary Active Directory Server** to take over in case the Primary Server fails. The settings under **Secondary Server** are specific to the Secondary Server only. The settings under **Secondary RADIUS Server** are specific to the secondary server only.

1. Select **Administration > Settings**.
2. Select **Active Directory LDAP**. The web console displays fields on the right. An asterisk denotes fields that are mandatory.

2. Enter the Secondary Server Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Is the authenticator enabled</strong> *</td>
<td>Enable AD authentication.</td>
<td>false</td>
</tr>
<tr>
<td><strong>LDAP URL</strong> *</td>
<td>The host URL for LDAP authentication.</td>
<td>Example: ldap://localhost:389</td>
</tr>
</tbody>
</table>

### Finalize Your Changes

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

After setting your configuration options, you must do one of the following:

1. Reset or commit your changes.
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server. If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

2. Instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.
Authenticate Users Against RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. Authentication using a RADIUS server acts much like authenticating against LDAP and runs in the application layer.

Refer to How to Set Up Cisco ACS for Management Center for an example RADIUS implementation.

Prerequisites

Prerequisites for enabling Sync the role membership and Sync the group membership:

- To sync role membership, you must define the role in Management Center before users assigned to the role authenticate.
- To sync group membership, you must define the group in both Management Center. The group names must match in order to map correctly.
- Install Symantec’s latest dictionary of VSAs for Symantec on the RADIUS server. The latest version of the dictionary file is available with the Management Center image on the Symantec Support site.
- Define the Symantec attributes, as in the following example:
  - Blue-Coat-Group = "mc_group_1"
  - Blue-Coat-Role = "mc_role_1"

where mc_group_1 and mc_role_1 are the names you specify for the group and role, respectively, in Management Center.

After you define the VSAs, and when a user authenticates in Management Center, the appropriate roles and/or group memberships are applied to the permission set in Management Center.

Set up RADIUS authentication in Management Center.

1. Select Administration > Settings.
2. Select RADIUS. The web console displays fields on the right. An asterisk denotes fields that are mandatory.
3. Configure general RADIUS settings.

<table>
<thead>
<tr>
<th>RADIUS Settings</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable RADIUS authentication.</td>
<td>false</td>
</tr>
<tr>
<td>Sync the role membership</td>
<td>Specify whether to assign users to roles that match the Blue-Coat-Role VSA.</td>
<td>false</td>
</tr>
<tr>
<td>Sync the group membership</td>
<td>Specify whether to assign users to roles that match the Blue-Coat-Group VSA.</td>
<td>false</td>
</tr>
<tr>
<td>User must have permission</td>
<td>A user must have a role with permissions or be a member of a group with a role that has permissions in order to log in.</td>
<td>false</td>
</tr>
</tbody>
</table>

Configure Secondary RADIUS Server
Supported RADIUS Servers

<table>
<thead>
<tr>
<th>Server Types</th>
<th>Configuration Interface</th>
<th>Example User Credentials and Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steelbelted</td>
<td>Windows XP VM</td>
<td>user1/1resu</td>
</tr>
<tr>
<td></td>
<td>Note: Restart Windows services after making any modifications.</td>
<td>mcuser1/1resu (FirstName=MC1, LastName=User1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mcuser2/2resu (Role=Role_administrator)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mcuser3/3resu (Group=MCAdministrator)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mcuser4/4resu (No vendor-specific attributes defined)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Important: The group and role attribute values should match the Blue-Coat-Group and Blue-Coat-Role VSAs, respectively.</td>
</tr>
<tr>
<td>Safeword</td>
<td>Windows XP VM</td>
<td>user1/password shown on token</td>
</tr>
<tr>
<td>RSA</td>
<td>Web - Use Internet Explorer 11 Linux VM</td>
<td>user2/2resu (fixed password)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure users with a hardware or software token.</td>
</tr>
</tbody>
</table>

Finalize Your Changes

If you have unsaved changes, the edited settings are marked with a red triangle. See the “Pending changes” text at the top left of the dialog as an example.

After setting your configuration options, you must do one of the following:

1. Reset or commit your changes.
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server. If you are unable to save your changes, make sure that all required settings are specified.
   - Click Activate to cause the server to load and apply the currently saved configuration.
2. Instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.

Authenticate Users with SSL Mutual Authentication

In mutual SSL authentication, an SSL connection between a client and a server is established only if the client and server validate each other’s identity during the SSL handshake. The server and the client must each have their own valid X.509 certificate and the associated private key in order to perform SSL mutual authentication.

Certificates and private keys can be stored in multiple locations. On the client, one such location is a Common Access Card (CAC). However, a CAC card or reader is not required for SSL mutual authentication, you can install the certificates on your browser and into Management Center’s truststore.

The following example describes an SSL mutual authentication transaction.
1. The user requests access to the Management Console.
2. Management Center presents its certificate to the browser.
3. The browser validates Management Center’s certificate. This includes the following checks:
   - The certificate subject must match the appliance’s hostname.
   - The certificate must be issued by a CA listed in the browser’s Trusted Root Certificate store.
4. The browser confirms that the appliance has the certificate’s private key by challenging the appliance to sign random data. The browser validates the signature using the appliance’s certificate.
5. If appliance authentication succeeds, the browser accesses the client certificate and private key using the installed certificate or CAC. It then presents the certificate to the appliance.
6. The appliance validates the certificate that the browser presents. This includes the following checks:
   - The certificate must be issued by a CA included in Management Center’s truststore.
   - The appliance confirms that the browser has the certificate’s private key by challenging the browser to sign random data. The appliance validates the signature using the browser’s certificate.
   - The certificate must have a valid signature and not be expired.
7. If authentication succeeds, the appliance grants access to Management Center.
8. (If applicable) The appliance presents a Notice and Consent banner. The user provides consent.

Prerequisites

Before using SSL mutual authentication, you must meet the following prerequisites:

- The browser must have an X.509 certificate installed that will pass Management Center’s trust validation. That is, if the client is using its own Root Certificate Authority (CA) or a different CA, that CA must first be installed into Management Center’s truststore.
- The appliance certificate must be from a CA listed in the browser’s Trusted Root Certificate store. Install any missing client certificates or custom root CA certificate into the browser. For browser installing instructions, refer to http://wiki.cacert.org/FAQ/BrowserClients and select your browser of choice.

Set up SSL Mutual Authentication
1. Import the root CA certificate(s) and any intermediate certificate(s) required to validate the client certificates into Management Center’s truststore.
   
   # security ssl import external-certificate <name> <URL>  
   # security ssl import server-certificate <URL>  

2. Verify installation with the appropriate command:
   
   # security ssl list external-certificate all  
   # security ssl list external-certificates system  
   # security ssl list external-certificates user  
   # security ssl list server-certificates  
   # security ssl view external-certificate <name>  

   See "# security" on page 617 for more information on the certificate viewing commands.

3. Determine the client authentication method, mandatory or optional; client authentication is off by default.

4. Issue one of the following commands:
   
   # security ssl client-authentication set-mandatory  
   # security ssl client-authentication set-optional  

   See "# security" on page 617 for more information on the client-authentication commands.

The flowchart below depicts the prerequisites, setup, and authentication process for mandatory and optional SSL mutual authentication.
Note

- When SSL mutual authentication is enabled, all devices using Management Center as the host require X.509 certificates. For example, to access file services and API's in a mandatory setting, a certificate is required.
- Browsers retain the certificate used. If you have more than one X.509 certificate installed and you want to use a different certificate, you must close and reopen your browser to change certificates.

Allow Users to Bypass Password if Certificate is Valid

Starting with 1.9.1.1, you can use the following CLI commands to configure Management Center to trust X.509 certificates so users do not have to enter their passwords after successful authentication:

```
# security ssl client-authentication password-requirement disable
# security ssl client-authentication set-regex
```
When the password requirement is disabled, a user does not have to enter a password to access Management Center if the system determines the certificate is valid, and finds the user in the local user database or LDAP system, if configured. The user is then automatically logged in with the permissions defined for that user in Management Center.

To validate certificates, you must create a regular expression to evaluate the information in the certificate’s SubjAltName field. The subjectAltName data is compared to a regex set by the security ssl client-authentication set-regex command, which is used to extract the portion of the value to use as the user’s identity. That value is then used to find the user in the local or LDAP authentication service. Refer to "Use Certificate Subject Alternative Name Data for Certificate Validation" below and "# security" on page 617 for more information.

This method only supports the local or LDAP authentication schemes. You can use active directory but only if you set it up using the LDAP settings (Administration > Settings > LDAP). This is because a service account is needed to look up users because the system no longer has the user password.

**HTTP Strict Transport Security (HSTS)**

Starting with Management Center 1.7.1, HSTS support is included to make web browsers interact with the servers using HTTPS connections. To enable HSTS:

1. Have a DNS name (domain) for your Management Center appliance.
2. Purchase a HTTPS certificate from a trusted CA (using the DNS above) and have it installed.
3. Be able to access Management Center using HTTPS without any warnings or errors. In Chrome, you need to have a green lock icon, showing the certificate is valid.
4. To enable the HSTS, use the CLI Command `# security ssl hsts enable`, or to disable, use `# security ssl hsts disable`.

With the HSTS activated, any attempted access using HTTP port 8080 gets an error instead of being rerouted to HTTPS port 8082. If you deactivate it, the domain must be removed from the HSTS in each browser. See How to Clear HSTS Settings in Major Browsers for more information.

If you change the SSL certificate, statistics monitoring will fail unless you install the certificate on your monitored appliances. See Statistics Monitoring Over HTTPS for more information.

**Use Certificate Subject Alternative Name Data for Certificate Validation**

Management Center can search the certificate Subject Alternative Name (SAN) data so that it can be matched against a regular expression to validate the certificate and user. SAN is a X.509 extension that allows data to be associated with a security certificate using a subjectAltName field. SAN data can include:

- Email addresses
- IP addresses
- URIs
- DNS names
- Directory names
- Object identifier (OID) followed by a value

Management Center scans the `subjectAltName` field for OID data. The format of the `subjectAltName` field data is as follows:

```
{oid}, [[{ASN.1 value type code}]{value}
```

For example:

```
1.3.6.1.4.1.311.20.2.3, [0]1309382685121005@gov
```

The `subjectAltName` data is compared to a regex set by the `security ssl client-authentication set-regex` command, which is used to extract the portion of the value to use as the user's identity. That value is then used to find the user in the local or LDAP authentication service.

This enables Management Center to validate the certificate and allow users to bypass the password requirement, if the system determines the certificate is valid and finds the user in the local user database or LDAP system. Refer to "Authenticate Users with SSL Mutual Authentication" on page 366 for more information.

For example:

```
# security ssl client-authentication set-regex
"'^1\\..6\..1\..4\..1\..311\..20\..2\..3\..s\[0\]\.(.*?}\""
```

Refer to "# security" on page 617 for more information about the `client-authentication set-regex` command.
View, Edit, or Delete User Accounts

This topic describes the following tasks:

- "View User Information" below
- "View User Permissions" below
- "Edit User" below
- "Delete a User" on the facing page

View User Information

To view user information, expand the Overview section.

```
Overview
```

View User Permissions

The Permissions section lists the user's permissions. Click Expand All to view the permissions and roles associated with the selected user.

- To view duplicate assignments, click Expand All and select Highlight all duplicated permissions and roles.
- To modify the assigned roles, click the Actions icon.
- To view group inheritance information, click the hyperlink associated with the group. (Direct assignment has no group link.)

```
Permissions
```

Edit User

To modify the user details (first name, last name, email address, phone numbers, description) or change the user's role (both local and imported), use the Edit User wizard.

1. Select Administration > Users.
2. In the list of users on the left, select the username to edit.
3. Click Edit. The web console displays the Edit User wizard.
4. Change desired information on the Basic Info tab. Note that you cannot change the username.
5. Click the Assign Roles tab to modify the user's role.
6. Click **Save**.

---

### Delete a User

Organizations typically implement processes to deactivate and remove access to internal accounts—such as mailboxes, intranet, and applications—when users leave the organization. As a best practice, include deleting the user account in Management Center to the exit procedures that your organization uses to reduce the risk of a security breach.

Deleting an imported user does not remove that user from Active Directory, LDAP or RADIUS.

1. Select **Administration > Users**.
2. In the list of users on the left, select the user you want to delete.
3. Click **Delete**. A Delete User dialog displays, prompting you to confirm the deletion.

4. Verify that it is the correct user, and then click **Delete User**. The user no longer displays in the Users list and is not a registered user of Management Center.
## Change and Reset Passwords

Select the topic for the applicable situation.

<table>
<thead>
<tr>
<th>Situation</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>User knows his/her password and wants to change it</td>
<td>&quot;Change Your Password&quot; on the next page</td>
</tr>
<tr>
<td>User forgot his/her password</td>
<td>&quot;Reset Password&quot; on page 376</td>
</tr>
<tr>
<td>Admin wants to automate the password resetting process</td>
<td>&quot;Automate Password Reset Process&quot; on page 570</td>
</tr>
<tr>
<td>Admin needs to manually change a user’s password because user forgot</td>
<td>&quot;Manually Reset a User’s Web Console Password&quot; on page 378</td>
</tr>
<tr>
<td>answer to security question or password reset process isn’t automated</td>
<td></td>
</tr>
<tr>
<td>Admin wants to expire a user’s web console password.</td>
<td>&quot;Expire a User’s Web Console Password&quot; on page 378</td>
</tr>
<tr>
<td>Admin forgot admin account password</td>
<td>&quot;Reset or Restore Admin Account Password&quot; on page 380</td>
</tr>
</tbody>
</table>
Change Your Password

You can change the password that you use to log into the web console.

If you log in to the web console using your LDAP or Active Directory credentials, you cannot change your password.

1. In the web console banner, click and select your username.

   The username for the default admin login is “Management Center.”

The web console displays the Profile dialog. Fields marked with an asterisk (*) are required settings.

2. Click Change Password.
3. In the Current Password field, enter your current password.
4. In the first New Password field, enter a new password.
   As you type your password, the Password Strength meter indicates the strength of the password. Because the system assesses the strength of the password with each character, the meter might fluctuate while you are typing.
   Symantec recommends that you use a password with at least Secure strength. You can try a number of different passwords until the Password Strength meter indicates Secure or higher.
5. In the Retype New Password field, enter your new password again.
6. Click Save.
   The next time you log into the web console, use your new password.
Reset Password

If you have forgotten your password to log in to the Management Center web console, you can request a password reset. This capability requires that the administrator has enabled the Management Center password reset feature; see "Automate Password Reset Process" on page 570. The password reset is only good for the web console and not for the CLI console.

The password resetting process requires that you answer a security question, using the exact upper/lowercase you entered when you initially defined it in your user profile. You also must have the correct email address in your profile. If you forget the answer to your security question, or failed to define an email address, you will not be able to use the automated password reset process.

1. If you have forgotten your password when logging in, click Reset Password.

2. Enter your Username and click Next.

3. In the Answer field, enter the answer to the Security Question, using the exact spelling and upper/lowercase you entered when defining it. Click Next.
4. Check your email to retrieve your temporary password.
5. The next time you log in to the Management Center web console, use the temporary password.
6. Change your password because the temporary password will expire.

Automate Password Reset Process

As an administrator on Management Center, you need to configure settings so that users can request a password reset if they forget their password.
1. Select Administration > Settings > General.
2. Set the Is Reset Password enabled? field to true.
3. For Reset Password Email Subject, modify the email subject line, if desired.

4. For Reset Password Email Message, modify the body of the email that is automatically sent to users when they click the Reset Password link. For example, you can add a person's name to the signature instead of the generic Management Center.

   The message contains two substitution variables: {fullname} and {password}. Management Center automatically replaces {fullname} with the user's first and last name and replaces {password} with a temporary password.

5. Click Save to store the settings on the server.
6. Make sure an email server is configured. See "Configure Mail Settings" on page 528.

When the email is sent with the temporary password, the user’s account is marked so the administrators know that the password is only temporary. The temporary password will expire.
**Manually Reset a User's Web Console Password**

If users forget their web console password, you can manually reset the password for them. (Alternatively, if you have automated the process, the user can request a password reset when logging in. See "Automate Password Reset Process" on page 570.) Even if you have automated the process, you may still need to manually change someone’s password if the user has forgotten the answer to his/her security question.

1. Select Administration > Users.
2. In the list of users on the left, select the username whose password you want to change.
3. Click Edit. The web console displays the Edit User wizard.

   You cannot change the password for users authenticated against LDAP, Active Directory, or RADIUS (authenticated users have the following icon: 🔒).

4. From the Basic Info tab, click the Change password link. The system displays two new fields: New Password and Verify New Password.
5. Enter a new password. If you do not enter identical text in both fields, you receive an error message.
6. Click Save. The dialog closes and the web console banner displays an alert indicating that the user's password was saved.
7. Communicate the new password to the user and recommend a password change as soon as possible.

**Expire a User's Web Console Password**

For security reasons, you should regularly prompt users to change their passwords. You can expire a user’s password, as described below. You must have administrative privileges to expire passwords.

1. Select Administration > Users.
2. In the list of users on the left, select the username whose password you want to change.
3. Click Edit. The web console displays the Edit User dialog.

   You cannot expire the password for users authenticated against LDAP, Active Directory, or RADIUS (authenticated users have the following icon: 🔒).
4. From the Basic Info tab, click Expire password. The system displays the expiration time and date.

![Edit User: John Smith](image)

Username: Test2

Password: Change password  Expire password

Password expired on: 11/29/16 3:56 PM UTC

After the password is expired, the user is prompted to change their password the next time they log in. If the user does not log in within the next 24 hours, they are locked out of their account and instructed to contact their administrator. You can then change the password for the user and allow them to log in again.
Reset or Restore Admin Account Passwords

You can reset the password for the CLI (serial console). You can also restore the default password for the admin UI (web console). The admin account to access the CLI versus the admin account to access the web console are different accounts (and thus the passwords are not the same).

To reset the CLI admin account password, use `#security reset-password`. This command is only available through the serial console for hardware appliances and Management Center VMware console for virtual appliances.

1. "Access the Management Center CLI" on page 594.
2. Enter privileged mode by typing `enable` at the command prompt. See "Privileged Mode Commands" on page 602.
3. Enter your enable password and press Enter.
4. At the '#' prompt, type `restore-defaults reset-admin` and press Enter.

The CLI prompt displays the following:

```
This operation will restore admin password on UI to default. Management Center service will be unavailable during this operation.

Are you sure you want to restore UI admin password? [y/N]
```

Resets the UI admin password to admin/admin.
Manage User Groups

To reduce the time and effort involved in assigning roles to users, you can create a user group, add users to it, and then assign roles to the group. Creating user groups also helps ensure consistency among users who require the same access. Before adding user groups, make sure you have defined roles.

Use the Groups tab to add, edit, and delete user groups. See the following topics for details:

- "Add User Groups" below
- "Edit a User Group" on page 383

Add User Groups

Although you can add users and assign roles to them individually, doing so can be labor-intensive if there are many users in the system who require the same permissions. To reduce the time and effort involved in assigning roles to users, you can create a group, add users to it, and then assign roles to the group. Creating user groups also helps ensure consistency among users who require the same access.

Users inherit the roles and permissions assigned to them individually and to the groups in which they are members. If users inherit permissions that seem to conflict, keep in mind that they can access an object as long as they have a role with the required permission. For example, if one of a user's groups has a role with the View permission for policy objects but another group has no policy permissions, the user can view policy objects.

Groups cannot be members of other groups.

1. Select Administration > Groups.
2. From the Groups section, click Add Group. The web console displays the Add Group wizard.
3. In the Add Group: Basic Info page, enter the group's information. An asterisk denotes fields that are mandatory. Enter a Name for your group. This group name displays on the dashboard and other areas in the web console.

Before you start naming user groups, devise a naming convention. For example, a user group name can be based on an organization, job function or geographical location.

4. In the Add Groups: Basic Info page, add a description (even though it is not required).

Although entering a description is optional, the description helps you and other users understand the purpose or function of the group. This helps to understand the correct roles and permissions to apply within the group. Symantec recommends that you always enter a clear, helpful description.

5. Click Next.
6. In the Add Group: Members dialog, select users from the Available Users and add them to the Members list using the arrow buttons. Click Next.
7. In the Add Group: Assign Roles dialog, select a group role from the Available Roles it to the Assigned Roles list. See "Define Roles " on page 386.
8. Click **Finish**. The system displays the group that you just created in the left pane.
Edit a User Group

To modify the user group details (name or description), add or remove group members, or change the role(s) assigned to the group, you can use the Edit Group wizard.

1. Select Administration > Groups.
2. In the list of groups on the left, select the group to edit.
3. Click Edit or click the edit icon in the Action column. The web console displays the Edit Group wizard.
4. Change desired information on the Basic Info tab.
5. To add a user to the group:
   a. Click the Members tab.
   b. Select the username in the Available Users list.
   c. Click the right arrow button to add the user to the Members list.
   d. Repeat for other users you want to add to the group.
6. To remove a user from the group:
   a. Click the Members tab.
   b. Select the username in the Members list on the right.
   c. Click the left arrow button to remove the user. The user moves over to the Available Users list.
   d. Repeat for other users you want to remove.
7. Click the Assign Roles tab to modify the role(s) associated with the group.
8. Click Save.

View Group Permissions and Roles

To view the permissions and roles associated with a group click the + icon. Expand or collapse the roles and associated permissions using the expand buttons.

Modify a role by selecting the role and clicking the edit role icon in the Action column.

View Group Members

To view the members in a group, you can edit the group or hover over the profile icon in the Actions column.
User Groups

If a group has more than 4 members, click the profile to view the complete list.

Delete a User Group

Deleting a group does not remove the members in the group.

1. Select Administration > Groups.
2. In the list of groups on the left, select the group you want to delete.
3. Click Delete. A Delete Group dialog displays, prompting you to confirm the deletion.
4. Verify that it is the correct group, and then click Delete Group. The group no longer displays in the Groups list.

You can also select multiple groups and click Delete.

Deleting a group does not delete any associated members or permissions. They are only disassociated from that group.
Management Center Configuration & Management

Manage User Sessions

Management Center tracks and logs each user session. Administrators can view and manage current user sessions from Administration > User Sessions. As a super admin, the ability to log in will not be affected by what you do in this dialog. You can delete (kill) any user session which will immediately log the user out of the Management Center web console.

As a best practice, Symantec recommends that all users log out of the web console after completing their tasks. As a Management Center administrator, you may need to enforce this practice. If a user has changed roles or has accepted a new job that may change their access rights, you can manage all active or stored user sessions.

1. From the web console banner, select Administration > User Sessions.
2. To prevent users from logging in to the web console, select the Disable user login to Management Center check box.
3. (Optional) To delete a user session:
   a. Select a user session. Green denotes your session (you), not an active session.
   b. Click Kill Session.
   c. Confirm that you want to kill the session.
Define Roles

Roles are not necessarily associated with jobs or job titles; rather, each role should contain the permissions required to perform a specific task or set of tasks. Managing roles based on tasks is easier than managing permissions attached to features or functions. Because multiple users in organizations often perform the same task (for example, two teams of 20 support engineers require a Device Admin role), and tasks are shared even across different teams (five product engineers also require 'Device Admin'), the number of roles you need to define is in principle much lower than the number of users in the system. See "Edit an Existing Role" on page 388 and "Duplicate an Existing Role" on page 388.

About Roles

The role structure in Management Center has two predefined levels:

- **administrator**, which has all permissions for all objects. The default *admin* account has the administrator role.
- **viewOnly**, which has the view permission for all objects.

You can create other roles that allow view access to some objects, add or update access to some objects, or a mix of different permissions as shown in the example below.

Symantec recommends that you create roles—with all necessary permissions and filters—*before* adding users.

Procedure

1. Select **Administration > Roles** and click **Add Role**.
2. In the **Add Role: Basic Info** dialog, enter a name for the role.
   If you authenticate users against LDAP, Active Directory or RADIUS, create a role in sync with the directory service.
3. (Optional) Enter a description.

Symantec recommends that you enter a list of the permissions for the defined role in the Description field. This helps you and other users understand the permissions of a user’s role including the intent of their job function.

4. Click Next.
5. In the Add Role: Permissions dialog, click Add Permission.
6. From the Object drop-down list, select All objects or a specific object.
7. From the Action drop-down list, select All operations or one or more individual actions.
8. (Optional) In the Filter drop-down list, select a filter to apply to both the action and the object.
   See "Grant Permissions" on page 390 for information on objects, actions, and filters.
9. To add more permissions, repeat steps 6 through 8.
11. Click Finish.

For information about managing roles, see "Edit an Existing Role" on the facing page and "Duplicate an Existing Role" on the facing page.
**Duplicate an Existing Role**

To avoid spending an excessive amount of time on defining roles with similar permissions, you can define a role based on a role that already exists in the system. For example, if you have already created a role that allows access to device groups, you can base other roles on it with different attributes.

1. Click the Administration tab and select Roles.
2. Select the role on which you want to base the new role.
3. Click Duplicate. Use the Duplicate button or the icon in the Action column, as shown below.

![Roles Tab](image)

The Roles tab displays the new role, with the name of the original role followed by (1). For example, if you duplicated the viewOnly role, the new role’s name is viewOnly (1).

4. Select the role you just created and click Edit. The web console displays the Edit Role dialog containing two tabs:
   - Basic Info
   - Permissions
5. Update the name and description to reflect the purpose of the new role.
6. Click Permissions.
7. Edit the permissions for the new role; see "Grant Permissions" on page 390 for instructions.
8. Click Save. The role is saved and the Roles tab displays it with the new name and description.

**Edit an Existing Role**

Use the settings on the Administration > Roles page to edit an existing role. From the Roles page you can perform the following actions:

- Edit role
- Delete role
- Refresh view
- Add role
- Duplicate role

You cannot directly assign permissions to users; thus, you must always edit a role to change a permission. You can edit a role’s basic information or the permissions that the role comprises.
Management Center Configuration & Management

Roles

To view the permissions associated with a role click the + icon. Expand or collapse the roles and associated permissions using the icons.

Edit: Update basic information

1. Select Administration > Roles.
2. Select the role whose information you want to update and click Edit. The web console displays the Edit Role dialog.
3. On the Basic Info tab, edit the name of the role or the description as required. Click Save.

Edit: Update permissions

1. Select Administration > Roles.
2. Select the role whose permissions you want to update and click Edit (or click the edit icon in the Action column). The web console displays the Edit Role dialog containing two tabs:
   - Basic Info
   - Permissions
3. Click the Permissions tab. The web console displays the list of permissions.
4. To change only part of a permission, select the value in the Object or Action column. See "Reference: Permissions Interdependencies" on page 339. Do one or more of the following as needed:
   - In the Object drop-down list, double-click and specify All objects or a specific object.
   - In the Action drop-down list, double-click and select All operations or a specific operation.
   - (If applicable) In the Filter drop-down list, click the plus sign (+) and select a filter. See "Filter Devices or Device Groups in a Permission" on page 393.
5. Add or remove an existing permission:
   - To add a permission, click Add Permission. See steps 7 through 10 in "Define Roles " on page 386 for instructions.
   - To remove a permission, select it and click Remove Permission. The permission is removed from the list.
6. Click Save.
Control Roles and Permissions through user sessions. If you edit a role's permissions while users are logged in to the web console, users must log out and log in again to see the effects of the change. See "Manage User Sessions" on page 411.

Delete Role

Select Administration > Roles. Select the role and click Delete or use the trash icon in the Action column.

Refresh View

Select Administration > Roles. Click to refresh the role.

Grant Permissions

You can add, remove, and edit permissions for any role. A role must have at least one permission for the role to take effect.

1. Select Administration > Roles.
2. Select a role and click View. The web console displays the View Role dialog.
3. Click Permissions. You can add, remove, and edit permissions on this tab.

A permission consists of:

- The object, which describes the area, feature, or function that the user can access, such as devices and global settings.
- The action, which is the scope of access to an object. It details what actions a user can do with the object, such as the ability to add and edit devices, or view global settings. The actions that are available depend on the selected object. Starting in Management Center, 1.6.x, you can add multiple actions per object.
- A filter, which dictates permissions to a sub-set or specific area of the object, such as certain attributes about a device or policy. Filters are available for devices and device groups; for instructions on specifying filters, see "Filter Devices or Device Groups in a Permission" on page 393.

The available filters correspond to the specified actions. That is, if multiple actions are defined, the filters list includes all possible filters for those actions. If an action is subsequently deleted, the corresponding filter will also be deleted if it does not apply to any remaining actions.

If the View permission for an object is not included in a role, users with the role are unable to see the object when they log in to the web console. For example, if a role does not include a permission for the Device object, users added to the role do not see the Network tab.

See "Define Roles " on page 386 for more information about setting roles and permissions.
Update Access When a User's Job Changes

When a user's job changes, you can adjust their information to reflect their new job or responsibilities.

1. Select Administration > Roles.
2. (If applicable) Update a user's roles to reflect changes in position or responsibilities.
3. (If applicable) Update the user's basic details.
4. (If applicable) Update a role to apply changes to all users who have the role. See "Edit an Existing Role" on page 388.

Update a User's Roles

When a user has a new job or responsibilities within the organization, you might have to update their roles to ensure that they can perform their new tasks.

1. Select Administration > Users.
2. In the Users left pane, select the user whose roles you want to change. The user's details display.
   
   Imported users have the following icon:

   ![Icon](image)

3. Click Edit. The web console displays the Edit User dialog.
4. Click Assign Roles. The dialog displays a list of all the roles in the system. Roles to which the user is not assigned are listed under Available Roles. Roles to which the user is currently assigned are listed under Assigned Roles.

5. Update roles:
   
   - To add a role, select it from Available Roles and using the arrow, add it to the Assigned Roles list.
   - To remove a role, select it from Assigned Roles and using the arrow, add it to Available Roles list.
6. Click Save. The web console banner displays an alert indicating that the user was saved.
Roles are linked to user sessions. If you edit users’ roles while they are logged in to the web console, instruct them to log out and log in again to see the effects of the change.

Filter Devices or Device Groups in a Permission

You can control access to devices and device groups (folders) on a more granular level than with other objects in Management Center using permission *filters*. These filters are based on the attributes that you specify in device and device group properties. See "Set User-Defined Device Attributes for Access Control" on page 405 for information.

1. Perform one of the following:
   - Add a permission. See "Grant Permissions" on page 390.
   - Edit a permission. See "Edit an Existing Role" on page 388.
2. In the Add/Edit Role dialog, select the permission and click the plus sign (+) in the Filter field. The Add/Edit Filter dialog displays.
3. Select a filter from the Filter Type drop-down list and specify filter values. See "Reference: Permissions Filters Object and Attributes" below.
4. Click Save. The filter displays in the Filter field.

Reference: Permissions Filters Object and Attributes

Although you are not restricted to the user-defined system attributes of Location and Rack, the following helps to determine which filters to use for the Device and Device Group permissions.

Set Filters for Device Object

Specify Rack and Location attributes. See "Set User-Defined Device Attributes for Access Control" on page 405 for information.

<table>
<thead>
<tr>
<th>Select the Attributes type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute has specific value</td>
<td>Attribute: Select Rack. Value: Specify the rack. Click Save. The Filter field displays &quot;Rack is '&lt;value&gt;'&quot;.</td>
<td>Devices specified with this rack in device properties under Attributes &gt; User-Defined.</td>
</tr>
<tr>
<td></td>
<td>Attribute: Select Location. Value: Specify the location. Click Save. The Filter field displays &quot;Location is '&lt;value&gt;'&quot;.</td>
<td>Devices specified with this location in device properties under Attributes &gt; User-Defined.</td>
</tr>
<tr>
<td>Select the Attributes type</td>
<td>Specify the Attributes</td>
<td>What a user can access</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Attribute has any value</td>
<td>Attribute: Select <strong>Rack</strong>. Click <strong>Save</strong>. The Filter field displays &quot;<strong>Rack</strong> is not empty&quot;.</td>
<td>Devices specified with any rack specified in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td></td>
<td>Attribute: Select <strong>Location</strong>. Click <strong>Save</strong>. The Filter field displays &quot;<strong>Location</strong> is not empty&quot;.</td>
<td>Devices specified with any location in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Specific Device</td>
<td>Device: Select a device from the drop-down list. Click <strong>Save</strong>. The Filter field displays &quot;<strong>Specified Device</strong>&quot;.</td>
<td>This selected device.</td>
</tr>
<tr>
<td>Members of specific group</td>
<td>Hierarchy: Select a hierarchy. Your selection determines the values for device group. Device Group: Select the device group. Click <strong>Save</strong>. The Filter field displays &quot;<strong>Members of specified group</strong>&quot;.</td>
<td>All devices in the specified group or its sub-groups.</td>
</tr>
</tbody>
</table>
Set Filters for Device Group Object

Specify Primary Contact and Location attributes. See "Set User-Defined Device Attributes for Access Control" on page 405 for information.

<table>
<thead>
<tr>
<th>Select the Filter type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
</table>
| Attribute has specific value | Attribute: Select **Primary Contact**  
Value: Specify the contact.  
Click **Save**. The Filter field displays "Primary is '<value>'". | Groups specified with this primary contact in group properties under **Attributes > User-Defined**. |
| Attribute: **Select Location**  
Value: Specify the location.  
Click **Save**. The Filter field displays "Location is '<value>'". | Groups specified with this location in group properties under **Attributes > User-Defined**. |
| Attribute has any value | Attribute: Select **Primary Contact**  
Click **Save**. The Filter field displays "**Primary Contact** is not empty". | Groups specified with any primary contact in group properties under **Attributes > User-Defined**. |
| Attribute: **Select Location**  
Click **Save**. The Filter field displays "**Location** is not empty". | Groups specified with any location in group properties under **Attributes > User-Defined**. |
| Specific Device Group | Hierarchy: Select a hierarchy. Your selection determines the values for device group.  
Device Group: Select the device group.  
Click **Save**. The Filter field displays "Specified Device Group". | The specified device group. |
| Members of specific group | Hierarchy: Select a hierarchy. Your selection determines the values for device group.  
Device Group: Select the device group.  
Click **Save**. The Filter field displays "Members of specified group". | The sub-groups of the specified group (but not the group itself). |

Set Filters for Policy Object

Filter permissions for specific policies. See "Edit Attributes" on page 404.
### Management Center Configuration & Management

#### Select the Filter type | Specify the Attributes | What a user can access
---|---|---
Specific Policy | Policy: Select a policy. All policy objects that exist in Management Center are displayed here. Click **Save**. The Filter field displays Policy Attributes. | The specified policy. |
Attribute has specific value | Select an attribute. You must create an attribute and associate it with policy before using this option. Click **Save**. The Filter field displays Policy Attributes. | The policy matching the attribute details. |

### Set Filters for Scheduled Job

Filter permissions for scheduled jobs. Limits the user to working with specific jobs or all jobs created by a user.

#### Select the Filter type | Specify the Attributes | What a user can access
---|---|---
Owner (Created by) | Select **Current User** or **Specific User**. Click **Save**. | All jobs from created by the specified user. |
Specific Scheduled Job | Select a specific, scheduled job. Click **Save**. | The specified job. |

For more information about user-defined attributes, see "Manage Attributes" on page 400.

### Restrict Access to Reporter Reports

When creating or editing roles, you can set permissions to limit the Reporter report fields the role has access to. The choices you make limit the reports that users in that role are able to view and also preclude them from adding corresponding widgets to a dashboard.

**Procedure**

1. Select **Administration > Roles**.
2. Select a role and click **Edit**.
3. Click the **Reporter Permissions** tab.
4. Click **Add Permission**.
5. Select the Reporter database to apply permissions to.

If you select a database that includes All Databases in the title, the permissions you set will apply to all databases (present and future) on that device. If you select All Reporters - All Databases, the permissions you set will globally apply to all databases on all devices.

If you've already applied permissions to a database, it will not display in the Reporter-Database list.

6. Click Next. The system displays the Add Report Permissions - Restricted Fields, Reports dialog.
7. Restrict report fields.
8. To view the reports affected by your choices, select **Show Restricted Reports**.

9. When you are satisfied with your choices, click **Close**.
10. Click **Finish**, then **Save**.

Users in the specified role are now precluded from viewing reports in the selected fields.

**Users Associated With Multiple Roles**

If a user is associated with more than one role (or by group association), all applicable roles are displayed. For example, when viewing reports, the user can choose a role and a corresponding database from the menu on the **Reports > Reporter** page. If a role has no access to a database, that role does not display in the **Role** drop-down menu.

<table>
<thead>
<tr>
<th>Role:</th>
<th>test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database:</td>
<td>RP-V50 - ProxyS</td>
</tr>
</tbody>
</table>
Manage Attributes

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Because you have different devices and appliances to manage, those devices require and are often restricted to certain attributes. Attributes are custom metadata used to refine and edit devices, device groups policy, and scripts. Attributes can be used to filter on specific devices, device groups or objects.

1. Select Administration > Attributes.
2. From the Manage Attributes list, select one the following:
   - Device
   - Device Group
   - Policy
   - Device Script
3. To add an attribute, click Add Attribute. See "Add Attributes" on the next page.
4. To edit an attribute, select the attribute name and click Edit. See "Edit Attributes" on page 404.
5. To enable group inheritance, see Enable Attribute Group Inheritance.

View and Sort the Following Attributes Lists

- **Name**
- **Display Name**—The attribute name (with no spaces).
- **Type**—The format that users must enter or select values.
- **Default Value**—Select the default value that displays in the Attributes list. Default values can be substituted by other variables. See "Use Substitution Variables in Policies and Scripts" on page 202.
- **Mandatory**—The value of attributes that are marked as mandatory is required when you create a new or add a device, device group, create a policy, and create a script.
- **Inheritable**—Applies specifically to devices and device groups. When this is selected, the device or device group inherits attributes from its parent device group.
- **Description**—Describes the attribute and must be specific to the device, device group, policy, or script to which you are applying the attribute.

You are able to search for specific objects based on the attributes you define. See "Filter by Attributes and Keyword Search" on page 167.
Add Attributes

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Attributes are custom metadata used to refine and edit devices, device groups, policy, and scripts. Because you have different devices and appliances to manage, those devices require, and are often restricted to, certain attributes. Use these attributes to filter on specific devices, device groups or objects.

1. Select Administration > Attributes.
2. Select one of the following from the Manage Attributes list:
   - Device
   - Device Group
   - Policy
   - Device Script
3. Click Add Attribute. Define the properties of the attribute that you are creating. An asterisk denotes fields that are mandatory.
4. Click **Save**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description or Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name (*)</td>
<td>Name that displays throughout Management Center.</td>
</tr>
<tr>
<td>Name (*)</td>
<td>This is the name with no spaces.</td>
</tr>
<tr>
<td>Type (*)</td>
<td>The format in which users must enter or select attribute values.</td>
</tr>
<tr>
<td>Available Values (*)</td>
<td>The Available Values depend on the Type you selected.</td>
</tr>
<tr>
<td>Default Value</td>
<td>If this attribute has a default value, it is displayed here.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>All attributes that you check as mandatory will appear as options when you create a new policy, device, device group, or device script. All mandatory attributes can be filtered on when you &quot;Filter by Attributes and Keyword Search&quot; on page 167.</td>
</tr>
<tr>
<td>Inheritable</td>
<td>This attribute applies to devices and devices groups. Attributes that are checked as inheritable can &quot;inherit&quot; their attributes from a parent device group.</td>
</tr>
</tbody>
</table>
Mandatory Attributes

Attributes are metadata that you can apply to objects. Nothing changes to the existing devices, device groups, policy, or scripts when an attribute is marked mandatory. However, marking an attribute as mandatory means that whenever you create a new or add a device, device group, policy or device script object, you will be forced to enter a value for that mandatory attribute.

When you mark an attribute as mandatory, then the attribute's value is required. You can enable variable substitution only if you save the attribute with a default value. See "Use Substitution Variables in Policies and Scripts" on page 202.
Edit Attributes

After you have defined an attribute, you can refine and edit that attribute to apply to any of the devices, device groups, policy and device scripts within your network. Editing an attribute changes the way devices, device groups, policy or script objects can be filtered and searched.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

1. Select the Administration > Attributes section.
2. From the Manage Attributes list, select an attribute to edit from the following attribute types:
   - Device
   - Device Group
   - Policy
   - Device Script
3. Select an attribute from the list and click Edit.
4. Change the properties for the attribute. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description or Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name (*)</td>
<td>Name that displays throughout Management Center.</td>
</tr>
<tr>
<td>Name (*)</td>
<td>This is the name with no spaces.</td>
</tr>
<tr>
<td>Type (*)</td>
<td>The format in which users must enter or select attribute values.</td>
</tr>
<tr>
<td>Available Values(*)</td>
<td>The Available Values depend on the Type you selected.</td>
</tr>
<tr>
<td>Default Value</td>
<td>If this attribute has a default value, it is displayed here.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>All attributes that you check as mandatory will appear as options when you create a</td>
</tr>
<tr>
<td></td>
<td>new policy, device, device group, or device script. All mandatory attributes can be</td>
</tr>
<tr>
<td></td>
<td>filtered on when you &quot;Filter by Attributes and Keyword Search&quot; on page 167.</td>
</tr>
<tr>
<td>Inheritable</td>
<td>This attribute applies to devices and devices groups. Attributes that are checked as</td>
</tr>
<tr>
<td></td>
<td>&quot;inherit&quot; their attributes from a parent device group.</td>
</tr>
<tr>
<td>Displayed as a default</td>
<td>When enabled, the attribute displays as a column in the Policy Object grid, Script</td>
</tr>
<tr>
<td>column (*)</td>
<td>Object grid, or Network dashboard. Even if this option is not enabled, you can still</td>
</tr>
<tr>
<td></td>
<td>display the attribute by right-clicking the column header, selecting Columns and</td>
</tr>
<tr>
<td></td>
<td>selecting the attribute to display. See Customize the Network View.</td>
</tr>
<tr>
<td>Description</td>
<td>Give a useful description of this attribute to distinguish it from the others when</td>
</tr>
<tr>
<td></td>
<td>viewing all of the attributes in a list.</td>
</tr>
</tbody>
</table>

5. Click Save.
Set User-Defined Device Attributes for Access Control

User-Defined attributes can either be custom attributes that you create from the Administration tab (or if you edit the attributes system attributes of Location and Rack). System attributes contain values that Management Center collects for reporting purposes.

- **Connection Parameters** - IP or hostname, Username, Password, Enable Password and SSH Port number.
- **Name** - Device Name
- **Membership** - The hierarchy and device group that the device belongs. See "Configure Hierarchy for Devices and Device Groups" on page 113.
- **Attributes** - Customized Location and Rack attributes or new custom attributes (or metadata) that administrators can create. See "Add Attributes" on page 401.

2. Use the up/down arrows to specify a Bandwidth Cost. "Set Bandwidth Cost for Reports" on page 523.

The bandwidth cost is a multiplier and is thus not expressed in a specific currency unit. For example, you can specify a value to represent on average how you pay per gigabit for data usage on your network.

3. If the User-Defined attribute has a red asterisk * it is required. You must specify a value before continuing.

Administrators can create attributes in addition to the user-defined attributes of Location and Rack. To define your own device and device group attributes, see "Add Attributes" on page 401 and "Edit Attributes" on the previous page.

For more fine-grained control of a device or device group, you can add permissions for the specified attributes. See "Reference: Permissions Filters Object and Attributes" on page 393.
Attributes

What are the values of system and user-defined attributes for this device?

System

Bandwidth cost: 

User-Defined

Location: 

Rack: 

Sub-group: 
Filter and Keyword Search

Apply filters to any object within Management Center. Objects can include:

- Attributes
- Audited Objects
- Authentication
- Devices
- Policy Objects
- Policy Device Assignment
- Roles
- Script Objects

Filter on attributes and then use the keyword search. When you are managing hundreds or thousands of policies across multiple devices, it is important to be able to find a particular policy or configuration quickly.

You are not limited to the Filter fields displayed. You can customize your filters.

Procedure

Default fields are dependent upon the type of object that you are filtering. For example:

- Name - Filters by the object name
- Type - Filters by the object type
- Description - Filters by the object Description
- Author - Filters by who created the object

1. To filter by a particular type of policy, click the Type drop-down list. Select a Policy Type:
   - CPL
   - CPL Fragment
   - VPM
2. Click **Apply Filters**.
3. The Object list displays all of the Objects by Type. After you have applied filters, search for specific objects using the Keyword Search.
4. From the Policy Objects listed by Type, search for a specific Policy using the Keyword Search.

The logic is Filter *and* Keyword Search.

Search by Keyword

When searching, Management Center breaks text into keywords and then searches for keywords entered. Management Center's index system has a special case for dot. Although Management Center sees dots as separating letters within a word (i.e. Management Center considers dots as a part of a word).

You cannot search on special characters such as ^ % | ~.

Colons are treated like other non-letters by splitting keywords apart. IPv4 and IPv6 addresses work differently because of colons.

The wildcard symbol is *. Management Center automatically appends an * at the end of your search term but if you want to start with a wildcard search, you have to enter it yourself.
Can quotes be used in a search?

Use quotes when non letters are part of the search term. For example, your search term includes a colon. The exception to this search rule is the use of a dot because a dot that is NOT followed by white space is considered part of the keyword.

How do you search for whole words?

Enter the whole word. If there is more than one word, separate each word with a space. If using special characters, enclose each word in double quotes.

How do you search for partial words?

Enter the partial term, and Management Center attempts to complete the search. For example, enter hi and Management Center matches that to both highlight and high.

Example Searches

IPv4 127.0.0.1
- 127.0.0 - matches any IPv4 starting with 127.0.0
- *.0.0.1 - matches any IPv4 ending in 0.0.1

IPv6 *:0:0:0:0:1*

Use quotes for IPv6 addresses because IPv6 uses colons instead of dots as the separator.

- "0:0:0" - matches any IPv6 start with 0:0:0
- "*:0:1" - matches any IPv6 ending with 0:0:1

Hostnames
- abc.com - matches a host named abc.com
- *.com - matches a hostname ending in .com
- "*:8080" - matches a hostname with :8080 as the port

Search

1. From the Keyword Search field, enter your search term.
2. Press Enter or click the magnifying glass icon.

What if the search finds no match?

If the search finds no match, the right pane displays a message indicating that objects match the keyword filter. You can search again using a different keyword.

What if the search succeeds in finding matches?

If the search finds matches, the results display in alphabetical order in the Objects list.

How do you clear the search results?

To clear search results and display all objects in the system, click the X in the search field.
Preview or Download Logs

You can sort and preview a log by file name or log type. You can preview one log or download multiple logs.

1. Select Administration > Logs.
2. Select a log to view. Click Preview. For example, to view the localhost_access.log in a text viewer, click Preview.
3. To download multiple logs, select the check boxes of logs that you want to download and then click Download. Management Center downloads a .zip archive file to the default download location.

Available Logs

The following table lists the available logs.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost_access.log</td>
<td>WEB-ACCESS</td>
<td>Tracks users requests to the Management Center UI. These logs roll over weekly for a maximum of 4 weeks.</td>
</tr>
<tr>
<td>log.log</td>
<td>WEB</td>
<td>Primary Management Center log. The primary Management Center log rolls over when it reaches 10 MB and maintains a maximum of 9 history logs for a total of 1 GB.</td>
</tr>
<tr>
<td>debug.log</td>
<td>DEBUG</td>
<td>This log provides diagnostics information to help with debugging. The log only displays if a user enables debug diagnostics (Administration &gt; Settings &gt; Diagnostics). The DEBUG logs roll over when it reaches 10 MB and maintains a maximum of 9 history logs for a total of 1 GB.</td>
</tr>
<tr>
<td>journal.txt</td>
<td>PDM</td>
<td>Primary log for the performance data collector of Management Center. This log is useful for determining why performance data is not showing up in Management Center or is being delayed. These logs roll over weekly for a maximum of 4 weeks.</td>
</tr>
<tr>
<td>device.log</td>
<td>SYSTEM</td>
<td>Internal CLP OS log. These logs are very small and roll over every day for a maximum of 30 days.</td>
</tr>
<tr>
<td>clp_services.log</td>
<td>SYSTEM</td>
<td>Internal CLP OS log. These logs are very small and roll over every day for a maximum of 30 days.</td>
</tr>
</tbody>
</table>

There are also debug logs for each type of device. For example, cas.log.

Rollover Log Formats

Rollover log formats are similar to the following:

- name.zip
- name.log-data
**Log Types**

The following table describes the log types.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEB</td>
<td>Logs related to Management Center and its operation.</td>
</tr>
<tr>
<td>WEB-ACCESS</td>
<td>Logs that track user requests to Management Center web UI.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>As the name implies, these are debugging logs.</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>Internal core OS logs.</td>
</tr>
<tr>
<td>PDM</td>
<td>Performance Data processing logs. These correspond to anything related to the <code>appstat</code> processing of PDM logs from the ProxySG or other systems.</td>
</tr>
</tbody>
</table>
Manage User Sessions

Management Center tracks and logs each user session. Administrators can view and manage current user sessions from Administration > User Sessions. As a super admin, the ability to log in will not be affected by what you do in this dialog. You can delete (kill) any user session which will immediately log the user out of the Management Center web console.

As a best practice, Symantec recommends that all users log out of the web console after completing their tasks. As a Management Center administrator, you may need to enforce this practice. If a user has changed roles or has accepted a new job that may change their access rights, you can manage all active or stored user sessions.

1. From the web console banner, select Administration > User Sessions.
2. To prevent users from logging in to the web console, select the Disable user login to Management Center check box.
3. (Optional) To delete a user session:
   a. Select a user session. Green denotes your session (you), not an active session.
   b. Click Kill Session.
   c. Confirm that you want to kill the session.
Receive Error Notifications

Configure how you will be notified when errors occur in Management Center.

<table>
<thead>
<tr>
<th>Description</th>
<th>Message Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware monitor warnings or critical errors.</td>
<td>&lt;monitor_name&gt; has exceeded &lt;level_name&gt; level of &lt;#&gt;%, current usage is &lt;#&gt;%.</td>
</tr>
<tr>
<td>Database disk quota warning.</td>
<td>Statistics Monitoring DB exceeded allowed disk quota. Collector to reject upload requests.</td>
</tr>
<tr>
<td>Critical repository messages.</td>
<td>Unable to create/start the repository, &lt;repository_name&gt;. The system is stopping.</td>
</tr>
<tr>
<td></td>
<td>Unable to initialize the &lt;repository_name&gt; repository.</td>
</tr>
<tr>
<td>Internal critical errors.</td>
<td>Subscription URLs are not installed.</td>
</tr>
<tr>
<td>Errors with auditing user actions.</td>
<td>Unable to write audit record, user: &lt;username&gt;, event: &lt;action&gt;.</td>
</tr>
<tr>
<td>Management Center license errors due to duplicate serial or server avoidance.</td>
<td>License error &lt;message_string&gt;.</td>
</tr>
<tr>
<td>Migration errors during an upgrade.</td>
<td>Migration step: &lt;step_name&gt; failed. Changes made by the step have been rolled back, but migration steps that have completed successfully have been retained. Subsequent steps have been canceled.</td>
</tr>
<tr>
<td>Statistics monitoring exceeds the disk quota.</td>
<td>Statistics Monitoring DB exceeded allowed disk quota. Collector to reject upload requests.</td>
</tr>
<tr>
<td>Raise alert whenever a device’s license (or any of its sub-components) are about to expire. The warning shows within 30 days of the expiration.</td>
<td>License component &lt;component_name&gt;, for device &lt;device_name&gt; has, or will, expire on &lt;date&gt;.</td>
</tr>
<tr>
<td>If a device license expires, the warning alert closes to open an error alert.</td>
<td>State changed from NEW to CLOSED. System closed alert because license expired.</td>
</tr>
</tbody>
</table>
### Description

<table>
<thead>
<tr>
<th>Description</th>
<th>Message Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>If a device license, in the warning state, is renewed, the warning alert</td>
<td>State changed from NEW to CLOSED. System closed alert because license was</td>
</tr>
<tr>
<td>closes because of subscription renewal.</td>
<td>renewed.</td>
</tr>
<tr>
<td>If a device license, in the error state, is renewed, the error alert</td>
<td>State changed from NEW to CLOSED. System closed alert because license was</td>
</tr>
<tr>
<td>closes because of subscription renewal.</td>
<td>renewed.</td>
</tr>
</tbody>
</table>

### Manage Alerts

Management Center provides an area for administrators to store and manage various alerts. The settings on the Administration > Alerts page enable you to change the state of an alert, change the owner, provide feedback, or find a specific alert.

This is different from the message viewer. To view messages in the Recent Messages pane, see "Read Messages and Alerts" on page 577.

Go to the Alerts management page using one of the following methods:

- Select Administration > Alerts.
- Click the Alert Notification 📣 icon. This shows the number of open (or unresolved) alerts.

### Overview

The landing page shows the current alerts and the options available for management.

- **Sorting** options allow you to view the alerts based on various criteria.
  - Severity  
  - Priority  
  - Message  
  - Category  
  - State  
  - Received  
  - Acknowledged  
  - Owner
- **Details and Filters Tabs** give quick information about the alert(s).
- **Navigation** options at the bottom allow you to go to specific pages.
- **Management** options allow you to take action on specific alert(s).

### Sorting Alerts

The primary element on the landing page is the list of available alerts. These can be sorted by different columns.

*Indicates columns that are NOT shown by default*
Sort and view the alerts with these options:

- Adjust the length of columns by hovering between two columns to get the adjustment cursor.
- To sort the list, you have two options:
  - Click on a column header. The first click sorts the list by that column in ascending order. A second click sorts it in descending order.
  - Hover over a column header, then select **Menu Arrow > Sort Ascending** or **Sort Descending**.
- To customize which columns show, hover over any column header, then select **Menu Arrow > Columns**.
- To reset the columns back to the default columns and width, hover over any column header, then select **Menu Arrow > Reset Columns**.

### Details and Filters Tabs

Get an overview of a specific alert or use filter options in order to find specific alerts.

---

If you need more space to view the alerts list, collapse this pane by clicking the arrow tab on the left of it. See **Filters Panel** for an example image.
Preview Details Panel

Gives a brief summary of the selected alert. If you need to view more details, such as the history of the alert, see Editing Alerts.

ℹ️ Select only one alert to preview the details.

Filters Panel

Find specific alerts with various filters. Once applied, the Filters tab shows how many active filters there are. Example: (Active 3).
Apply/Clear
Save or delete any filter changes selected.

Customize
Select the filters that show in the Filter Panel.

Time Range
Select the time range you want to search in.

<table>
<thead>
<tr>
<th>Hour Options</th>
<th>Day Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 1 Hr</td>
<td>Last 24 Hrs</td>
</tr>
<tr>
<td>Last 12 Hrs</td>
<td>Last 3 Days</td>
</tr>
<tr>
<td>Last 24 Hrs</td>
<td>Last 7 Days</td>
</tr>
</tbody>
</table>

State
Select the alert current status(es).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>New or unworked issues.</td>
</tr>
<tr>
<td>Pending</td>
<td>Already known issue, but resolution hasn't started.</td>
</tr>
<tr>
<td>Assigned</td>
<td>Assigned to a specific user.</td>
</tr>
<tr>
<td>In Progress</td>
<td>A resolution has been started.</td>
</tr>
<tr>
<td>Resolved</td>
<td>The issue has been resolved.</td>
</tr>
<tr>
<td>Closed</td>
<td>The issue has been closed. This can be used whether or not the issue has been resolved.</td>
</tr>
</tbody>
</table>
Management Center Configuration & Management

**Acknowledge**
Select the receipt status(es).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledge</td>
<td>Alert received by owner.</td>
</tr>
<tr>
<td>Unacknowledge</td>
<td>Alert not received by owner.</td>
</tr>
</tbody>
</table>

**Category**
Select the element(s) affected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy specific.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Scripts, Shared Objects, Tenants, and Files.</td>
</tr>
<tr>
<td>License</td>
<td>Device license status.</td>
</tr>
<tr>
<td>Operational</td>
<td>Alerts related to the function of a device or Management Center.</td>
</tr>
<tr>
<td>System</td>
<td>Networks linked to Management Center, including files, software, hardware, and firmware.</td>
</tr>
<tr>
<td>Security</td>
<td>Security related alerts.</td>
</tr>
<tr>
<td>Other</td>
<td>For an issue not listed in any other category.</td>
</tr>
</tbody>
</table>

**Priority**
Select the importance level of resolution.

<table>
<thead>
<tr>
<th>Priority Level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Urgent</td>
<td></td>
</tr>
</tbody>
</table>

**Owner**
Select the current owner.

> Alerts that are **not assigned** (in the Owner sorting column) will not show up if an owner is selected.
Keyword Search

Next to the Preview/Filter pane is the keyword searching option. If you know keywords in the alerts you are looking for, enter them into the search box and click the magnifying glass or press Enter. To clear the search terms, click the (×) within the search box.

Navigation

Navigate between pages and set navigation options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginning</td>
<td>&lt;&lt;</td>
<td>Go to the first page.</td>
</tr>
<tr>
<td>Back</td>
<td>&lt;&lt;</td>
<td>Go back a page.</td>
</tr>
<tr>
<td>Page Number</td>
<td>Page 1 of 1</td>
<td>Current page number and total page count.</td>
</tr>
<tr>
<td>Forward</td>
<td>&gt;&gt;</td>
<td>Go forward a page.</td>
</tr>
<tr>
<td>End</td>
<td>&gt;&gt;</td>
<td>Go to the last page.</td>
</tr>
<tr>
<td>Refresh</td>
<td></td>
<td>Refresh the list.</td>
</tr>
<tr>
<td>Page Size</td>
<td>Page Size 50</td>
<td>Number of alerts displayed per page.</td>
</tr>
</tbody>
</table>

Alert Management

Create, edit, delete, or acknowledge receipt of alert(s).

Creating New Alerts

Use Raise Alert to create a new alert.
Management Center Configuration & Management

Raise Alert

**Raise Alert**

**Message:**
Enter in the message for the alert. *This field is required.*

**Severity**
The impact level on the affected category. *Indicates default*

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Severity Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info*</td>
<td>📢</td>
<td>Low</td>
<td>Little or no impact.</td>
</tr>
<tr>
<td>Warning</td>
<td>🚧</td>
<td>Medium</td>
<td>Potential to cause errors.</td>
</tr>
</tbody>
</table>
## Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Severity Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td><img src="Image" alt="Error" /></td>
<td>High</td>
<td>Errors found.</td>
</tr>
<tr>
<td>Fatal</td>
<td><img src="Image" alt="Fatal" /></td>
<td>Critical</td>
<td>System failure.</td>
</tr>
</tbody>
</table>

### Priority

The importance level of resolving the alert. *Indicates default

<table>
<thead>
<tr>
<th>Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low*</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Urgent</td>
</tr>
</tbody>
</table>

### State

The current status of the alert. Alerts are either considered open or closed. *Indicates default

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>New or unworked issues.</td>
<td>Open</td>
</tr>
<tr>
<td>Pending</td>
<td>Already known issue, but resolution hasn't started.</td>
<td>Open</td>
</tr>
<tr>
<td>Assigned*</td>
<td>Assigned to a specific user.</td>
<td>Open</td>
</tr>
<tr>
<td>In Progress</td>
<td>A resolution has been started.</td>
<td>Open</td>
</tr>
<tr>
<td>Resolved</td>
<td>The issue has been resolved.</td>
<td>Closed</td>
</tr>
<tr>
<td>Closed</td>
<td>The issue has been closed. This can be used whether or not the issue has been resolved.</td>
<td>Closed</td>
</tr>
</tbody>
</table>

### Owner

The administrator currently logged in is set as the default owner. You may assign it to a different owner as long as the person has previously been added as a user. See "Add Local Users" on page 357.

Alerts created by the system will show as **not assigned** in the **Owner** sorting column.

### Category

The element affected by the alert. *Indicates default
Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Option</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy specific.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Scripts, Shared Objects, Tenants, and Files.</td>
</tr>
<tr>
<td>Operational</td>
<td>Alerts related to the operation of a device or Management Center.</td>
</tr>
<tr>
<td>System</td>
<td>Networks linked to Management Center, including files, software, hardware, and firmware.</td>
</tr>
<tr>
<td>Security</td>
<td>Security related alerts.</td>
</tr>
<tr>
<td>Other*</td>
<td>For an issue not listed in any other category.</td>
</tr>
</tbody>
</table>

Description
(Optional) Enter a more detailed description of the alert and/or the reasons for it.

If you forget any information for the detailed description, you can always Edit it or add note to the Journal tab at a later time.

Save/Cancel
Save or Cancel the new alert.

Editing Alerts

You can edit the alerts using one of two methods:
- To edit all the information for an alert, select a message and then click Edit. Alternately, right-click a message to get the Edit option. Only one message can be selected for editing at a time.

Edit Details Tab

The basic information, normally set in Raise Alert, can be edited in the Details tab. A summary of the current saved status of the alert shows in a box below the editable details. The action buttons include:

- Save Alert for any changes you make.
- Acknowledge or Unacknowledge the receipt of the message.
- Discard any changes.
- Take Ownership to instantly assign it to yourself.
Journal Tab

A history of the changes made to the alert are logged in the Journal tab beneath the Notes field. Actions you can take include:

- Add more information in the Notes field.
- Add Note to the alert.
- Clear any information typed.

Back

Return to the list of alerts. Alternately, you can click on the Alerts link above the Back button to return to the list.

- Select message(s) to access the available quick Operations. These allow you to edit information on an alert without having to open the Edit screen.

Assign Users

Select a user to have ownership. You may assign it to a different owner as long as the person has previously been added as a user. See "Add Local Users" on page 357.

Alerts created by the system will show as not assigned in the Owner sorting column.

Take Ownership

Instantly assigns the alert to yourself.

Change State

The current status. Alerts are either considered open or closed.

* Indicates default
### Option | Description | Status
--- | --- | ---
New | New or unworked issues. | Open
Pending | Already known issue, but resolution hasn’t started. | Open
Assigned* | Assigned to a specific user. | Open
In Progress | A resolution has been started. | Open
Resolved | The issue has been resolved. | Closed
Closed | The issue has been closed. This can be used whether or not the issue has been resolved. | Closed

#### Change Priority

The importance level of resolution. *Indicates default*

<table>
<thead>
<tr>
<th>Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low*</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Urgent</td>
</tr>
</tbody>
</table>

#### Other Alert Management Options

- Select message(s) to **Delete** them. Alternately, right-click the message(s) to get the **Delete** option.
- Messages are automatically removed by the system after a set time. The default is 120 days. See "Configure Housekeeping Settings" on page 564 for more information.

To change the amount of days alerts are retained:

1. Select **Administration > Settings > Housekeeping**.
2. Change the value in **Number of days of closed alert records to keep**.
3. Click **Save**.
4. (Optional) Click **Activate** to push your changes to the server immediately.

- Select message(s) to **Acknowledge** or **Unacknowledge** the receipt of them. Alternately, right-click the message(s) to get the acknowledgment options.

  Only messages of the same receipt status can be selected at the same time for the button to work.  
  Example: Under the **Acknowledged** column, all messages marked **not yet**.

- **Refresh** the list of available alerts.
Configure SMTP Alerts

Configure the mail server for sending health monitoring notifications from Management Center and specify which administrators receive the alerts.

1. Select **Administration > Settings**.
2. Click **SMTP Alerts** on the left. SMTP fields display on the right. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>What to send*</td>
<td>Specify OFF to turn off e-mail notification or ERROR when errors occur with mail delivery.</td>
<td>OFF</td>
</tr>
<tr>
<td>Mail Server*</td>
<td>The SMTP mail server to use for outgoing mail.</td>
<td>Example: smtp.organization.com</td>
</tr>
<tr>
<td>Send to address*</td>
<td>E-mail addresses to which alerts are sent. For example, enter administrators’ e-mail addresses or a distribution list.</td>
<td>A comma-separated list of valid e-mail addresses.</td>
</tr>
<tr>
<td>From address*</td>
<td>The e-mail address from which e-mails are sent.</td>
<td>Example: <a href="mailto:bccm@organization.com">bccm@organization.com</a></td>
</tr>
</tbody>
</table>

4. Perform one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server.
     - If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.
Configure SNMP Alerts

By using the SNMP protocol, alerts can be sent by Management Center to other computers. An SNMP trap is sent each time an alert is generated by Management Center. These traps are sent in the Management Information Protocol (MIB) format.

The Simple Network Management Protocol (SNMP) itself does not define which variables a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs).

Restrictions

- SNMPv1 traps are not supported in Management Center 1.10.1.1 and later.
- Content Analysis 2.2 SNMP trap settings are not backed up and restored.

Configure SNMP settings for Management Center. If you want to enter a password for the SNMP traps, see "Configure the SNMP Agent Password" on page 529.

The MIBs are available on the Downloads page. Refer to the Management Center Release Notes for information on MIBs.

1. Select Administration > Settings.
2. Select SNMP Alerts. SNMP fields display on the right. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>What to send*</td>
<td>Specify OFF to turn off SNMP notifications or ERROR when errors occur with the SNMP traps.</td>
<td>OFF</td>
</tr>
<tr>
<td>SNMP Destination IP*</td>
<td>Specify an IP address for the listener.</td>
<td>Example: 192.0.2.0</td>
</tr>
<tr>
<td>SNMP Destination port*</td>
<td>Specify the port for the listener.</td>
<td>Example: 155</td>
</tr>
<tr>
<td>SNMP Version*</td>
<td>Specify the protocol version for the SNMP listener.</td>
<td>2</td>
</tr>
<tr>
<td>Community</td>
<td>A password that allows access to a device's statistics (transmitted in plaintext).</td>
<td>Enter the password. See &quot;Configure the SNMP Agent Password&quot; on page 529.</td>
</tr>
<tr>
<td>Engine ID</td>
<td>The unique SNMP engine ID based on the device IP. This engine ID is associated with the specific Management Center installation and displays in each SNMP packet to identify the source of the packet. Applies to SNMPv3 only.</td>
<td>Click generate to generate the engine ID.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Input Value/Format</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Security</td>
<td>Use name used to access the management module.</td>
<td>Enter the username.</td>
</tr>
<tr>
<td></td>
<td>Applies to SNMPv3 only.</td>
<td></td>
</tr>
<tr>
<td>Auth Protocol</td>
<td>The authentication protocol algorithm to use.</td>
<td>SHA</td>
</tr>
<tr>
<td></td>
<td>SHA is the default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Applies to SNMPv3 only.</td>
<td></td>
</tr>
<tr>
<td>Auth Passphrase</td>
<td>Passphrase to use for authentication.</td>
<td>Enter the passphrase.</td>
</tr>
<tr>
<td></td>
<td>Applies to SNMPv3 only.</td>
<td></td>
</tr>
<tr>
<td>Priv Protocol</td>
<td>The protocol to use for SNMP message privacy.</td>
<td>AES</td>
</tr>
<tr>
<td></td>
<td>AES is the default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Applies to SNMPv3 only.</td>
<td></td>
</tr>
<tr>
<td>Priv Passphrase</td>
<td>Passphrase to use when encrypting messages.</td>
<td>Enter the passphrase.</td>
</tr>
<tr>
<td></td>
<td>Applies to SNMPv3 only.</td>
<td></td>
</tr>
</tbody>
</table>

4. Perform one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server.
     - If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.
Customize the Audit Log

Because the Audit Log records all transactions on multiple levels, the log can grow very quickly—especially if you many devices are managed in Management Center and there is a high level of user activity. Although the Audit Log is designed to make it easy for you to locate the records you want, you can customize the display further to help you locate specific records, isolate records from a certain date or time, filter records pertaining to specific users or objects, and more.

Use the following methods in conjunction to customize the Audit Log display to suit your purposes.

When you make the following changes in the Audit Log Viewer, the changes do not persist beyond the current browser session; the next time you log in to the web console, you must go through the same steps to change the viewer again.

Show or hide columns

You can show columns that you hid, or columns that are not visible by default, such as Record Type and Info 3 through Info 5. You can hide some columns if you want a more general look at the log or if your screen size is limited.

To see all information available in the Audit Log and ensure that you can see an appropriate level of detail, you can show all columns first and then choose which ones, if any, you want to hide.

1. On any column header, click the arrow. The web console displays a list of options.
2. Select an option to show the column.
   - Clear an option to hide the column.
3. Click anywhere outside of the list to close it.
   - The Audit Log shows/hides the columns you specified.

Sort columns

Because the Audit Log displays records in descending chronological order by default, you can re-arrange them to analyze the data more effectively. By default, the records are sorted in descending order of Operation Time (latest to earliest).

1. Click the header of the column you want to sort.
   - If the header displays an up arrow, the data is arranged in ascending order (A-Z, earliest to latest).
   - If the header displays a down arrow, the data is arranged in descending order (Z-A, latest to earliest).
2. Click the header again to reverse the sort order.

In the following example the columns are sorted by Operation Type, so all Authentications are displayed first.

Filter records

To limit the amount the data that the log displays and focus only on specific records, apply filters using the drop-down lists on the right. Depending on the transaction level, you may need to filter pages of records. The filters limit the record type. To narrow the search, apply one or more filters.
If applying a filter results in too few records or not the right records, remove or change some filters. To reset the filters to default, click Clear.
Create and Manage Jobs

Management Center allows you to create jobs for running a variety of operations on a defined schedule. For example, you can create jobs for backing up Management Center each day, installing policy on a group of ProxySG appliances immediately, or executing a ProxySG script on a monthly basis. Jobs don’t necessarily need a precise schedule, though; if you don’t define a schedule for a job, you can run the job manually. In addition, you may override the defined schedule for a job and run it immediately.

Scheduling a job and running an operation require different permissions. See "Reference: Understanding Job Permissions" on page 352.

1. Plan the job:
   - Determine which operation you want to create a job for. See "Job Operations" on page 432.
   - Which devices do you want to perform the operation on? These will be the targets of the job.
   - Decide how often the job should run. This will be the job schedule. See "Job Scheduling Options" on page 436.
2. Create the job. See "Add a Job" on the next page.
4. Monitor jobs as they are running. See "View Current Jobs" on page 440.
5. View job history. See Job History.
Add a Job

The Management Center New Job wizard prompts you for information required to create a job: name, operation, targets (individual devices or groups), and schedule. The fields vary for each type of operation.

The basic steps for adding a job are described below.

1. Select Jobs > Scheduled Jobs.
2. Click New Job.
3. In the Basic Info section, enter a name for your job.
4. Enter a description of the job. Good descriptions help to differentiate jobs when they have similar names.
5. (Optional) Email the job results. Click Email results and select the condition. Then, enter the email(s) of the recipient(s) and click Next.
6. In the Operation section, select Single Job or Multistep Job.
   - Single Job:
     a. Select an operation from the menu.
     b. Additional fields may display, depending on which operation you select. See "Job Operations" on page 432.
     c. After filling in the fields required for the operation you selected, click Next.
   - Multistep Job:
     a. Click Select Jobs.
     b. Select the jobs to add to the execution list, then click Apply.
   
   Only single jobs are available to embed into a multistep job. Management Center does not allow nested multistep jobs.

   c. (Optional) Use Remove, Move Up, and Move Down to edit the available jobs and their execution order.
   d. (Optional) Select Stop on Fail for any job to stop the execution of the rest of the multistep job should a specific job produce an error. Jobs are executed in the order listed, so you can select as many jobs to stop on as you would like.

7. In the Targets section, do one of the following depending on what the system displays:
   - Select the Devices or Group tab. Add multiple devices or device groups by selecting the check box next to the names of devices or device groups. All selected targets appear in Selected Targets. When you have added all of the targets for the job, click Next.
   - Select All Predefined Targets or Selected Targets. The system displays this dialog when targets have already been assigned. Choose Selected Targets if you want to execute a job on some targets but not others. You can choose to execute the job on individual devices within a group or some groups but not others, etc.

   For a Multistep Job, no targets are selected in this step. Multistep jobs are system jobs and run single jobs that have their own targets.

8. In the Schedule section, define a schedule for the job. See "Job Scheduling Options" on page 436 for more information.
Schedule jobs to run when network performance is not impacted or jobs that recur often. Scheduling a job and executing a job (run now) apply different permissions. See "Reference: Understanding Job Permissions" on page 352.

The Jobs tab is one way to add a job in Management Center. Some operations have alternative methods for creating jobs. See the topics in the table below.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute Script</td>
<td>&quot;Execute Scripts&quot; on page 162</td>
</tr>
<tr>
<td>Export Backups</td>
<td>&quot;Export Device Backups&quot; on page 98</td>
</tr>
<tr>
<td>Install Policy</td>
<td>&quot;Install Policy&quot; on page 302</td>
</tr>
</tbody>
</table>
Job Operations

When defining a job, additional fields may display, depending on which operation you select. The list below describes each operation and its associated fields.

* designates a required field

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
</table>
| Backup Devices          | Backs up the configuration of the selected device(s) on a defined schedule; any supported type of device can be backed up.                                                                             | Backup Name *  
Backup Description *  
Include Private Data  
Encrypt Backup |
|                         | Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored. |                                                                          |
|                         | See also "Back Up Device Configurations" on page 89.                                                                                                                                                    |                                                                          |
| Backup Management Center| Stores a backup of the Management Center configuration to the specified server on a defined schedule.                                                                                                   | Export to Server - Select the check box.  
Server URL * - Supported protocols include scp, ftp/ftps, and http/https.  
Encryption Phrase * - 1 or more characters, alphanumeric.  
User name  
Password |
| Change Monitoring State | Activate or deactivate devices. Management Center actively monitors the health status of activated devices.                                                                                              | Change Health Monitoring state - Select the radio button and Activate Devices or Deactivate Devices.  
Change Statistics Monitoring state - Select the radio button and Enable Statistics Monitoring collection or Disable Statistics Monitoring collection. |
|                         | Deactivated devices are not monitored. Whether you choose to activate or deactivate a device depends on your business requirements.                                                                      |                                                                          |
|                         | You can also disable statistics monitoring without deactivating a device.                                                                                                                                  |                                                                          |
|                         | See also "Monitor Device Health and Statistics" on page 103.                                                                                                                                               |                                                                          |
| Check Consistency       | Checks whether the policy installed on selected devices matches the reference policy.                                                                                                                     | Policy* - Click to select the reference policy to use for comparison.  
Select policy version* - Select the radio button for either The latest policy version or specify a previous Version. |
<p>|                         | See also &quot;Check Consistency between Policy and Devices&quot; on page 329.                                                                                                                                    |                                                                          |</p>
<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect Sysinfo</td>
<td>Extracts the Sysinfo data from the selected ProxySG appliances and outputs it to a file. If the job executes successfully, the files are saved to <strong>Jobs &gt; Archived Files</strong> as a zip file.</td>
<td>During job creation, ensure that <strong>Email Results</strong> or <strong>Generate Archive</strong> are selected.</td>
</tr>
<tr>
<td>Execute a Script</td>
<td>Runs the designated script on the selected target ProxySG appliances on a defined schedule. See also &quot;Execute Scripts&quot; on page 162.</td>
<td><strong>Device Script</strong> - Click 🖋️ to select the script to execute.</td>
</tr>
<tr>
<td>Export Backups</td>
<td>Saves backup files of the selected target device(s) to the specified server on a defined schedule. Exporting device backups is necessary to save space and is mandatory if you are upgrading the device to a new image.</td>
<td><strong>Export to Server</strong> - Select the check box. <strong>Server URL</strong> * - Supported protocols include scp, ftp/ftps, and http/https. <strong>Encryption Phrase</strong> * - 1 or more characters, alphanumeric. <strong>User name</strong> <strong>Password</strong> <strong>Prune Backups</strong> - Select this check box if you want to remove the backup from the backup slot when you export the backup. <strong>Retention Count</strong> ^ - Enter the number of backups to keep. <strong>Prune Pinned</strong> - Select this check box if you want to prune backups that have been pinned (or saved).</td>
</tr>
<tr>
<td></td>
<td>Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See also &quot;Export Device Backups&quot; on page 98.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Center supports the following key exchange algorithms for SSH/SCP connections: DHGex, DHG, and Curve25519. If a user attempts to export a backup to a server via SCP and the target server does not support the at least one of those key exchange algorithms, the export may fail with the message: <strong>A connection could not be established or The secure handshake failed during key exchange.</strong> This also applies to other Management Center operations that use SSH/SCP.</td>
<td></td>
</tr>
<tr>
<td>File Transfer</td>
<td>Transfers a file to the system. If you have previously downloaded a file, such as a configuration, image, license, text, or other file, and you want it on the new system, this option loads it.</td>
<td><strong>Server URL</strong> * - Enter the URL of the file. Supported protocols include http/https. <strong>File Type</strong> - Specify the file type. <strong>If the file already exists</strong> - Choose what to do if the file already exists.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>Description</td>
<td>Fields</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Import External Policy        | Imports the designated ProxySG policy or policy fragment from a web, FTP, or SCP server and merges it into the selected target policy fragment in Management Center.  
See "Import External Policy " on page 315.                                                                                               | Import from URL * - Supported protocols include scp, ftp/ftps, and http/https. The filename must be the ID assigned to the target policy.  
Username  
Password  
Policies* - Click 🔄 to select the policies to install.  
Force Installation - Select this check box to override any warnings.                                                                 |                                                                                                                                               |
| Install Policy                | Runs the designated policy on the selected target ProxySG appliances on a defined schedule.                                                                                                               | System Image - Select the image to install. The file will only be listed here if it has been uploaded to Management Center (Configuration > Files).  
No additional fields.                                                                                                              |                                                                                                                                              |
| Install System Image          | Upgrades the selected device to the specified image. The file must be uploaded to Management Center (Configuration > Files) and the device type must be specified.  
See Remove Unused Tenant Policy.                                                                                                          |                                                                                                                                               |
| Remove Unused Policy          | Removes tenant policy when there is no policy assigned to the tenant on the appliance.                                                                                                                      | Registered | Not Registered * - Use Not Registered if using Reporter 9.x or higher. You can manually enter the credentials to connect.  
Reported (*) - Select the Reporter device to run the report on.  
Database (*) - Select the database from which to run the report.                                                                  |                                                                                                                                              |
<p>| SWG-VR Data Collection        | Used to capture specific information associated with the Value Reporting service offered by Symantec. This job will capture specific information from your SGs attached to a Reporter instance and return a payload suitable for emailing to your SE for analysis. Consult with your SE for more information on this service. This saves the report as an archived file (Jobs &gt; Archived Files). |                                                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
</table>
| Summary Report    | Runs a summary report. This saves the report as an archived file (Jobs > Archived Files). See also Run a Summary Report. | **Cover Title** * - Add a title for the cover page of the report.  
**Sections** - Select the sections you want to add to the report on.  
**Database** (*) - Select the database from which to run the report. The database is only required for some sections and is inaccessible for the others.  
**Filename** (*) - Change the filename of the archived PDF, if wanted. This is automatically populated by what you enter for the Cover Title.  
**Description** - Add a description of the scheduled report. |
| Synchronize Devices | Synchronizes configuration settings from one device (the source) to one or more similar devices running the same or later OS versions. Management Center supports synchronization of the following device types: SSL Visibility, Content Analysis, and Malware Analysis. See also “Synchronize Devices” on page 110. | **Source Device** * - Select the device whose settings you want to copy to other devices.  
**What to synchronize** (*) - Varies by source device. |
Job Scheduling Options

Define a schedule for each job that you create or edit from the Schedule dialog in the Job wizard.

Verify that the time zone is configured for the region in which the job will occur. See Synchronize the System Clock using NTP.

Consider the following scheduling options.

**Immediate**

If you select **Immediate**, the job runs immediately after you finish creating or editing the job. To have the job listed on the Scheduled jobs page, select **Save this job in Scheduled Jobs**.

The job displays in Job History and Scheduled Jobs (if you selected the check box).

**No Schedule**

To run a on-demand job or to define the schedule later, select **No Schedule**.

Although the job does not have a schedule, it still displays in the Scheduled Jobs section. When you are ready to run the job, initiate the job manually by selecting Run Now. Management Center displays the **Are you sure you want to run the selected job now?** message. Click Yes. The Job History page displays the completed job.

**Run Once Only**

Certain jobs only need to be run once (for example, when you install policy to a device).

Select **Run Once Only** and then specify the date and time to run the job:

- In the Run at field enter the time (using a 24-hour clock) you want to run the job, or use the arrows to adjust the time.
- Click the calendar icon and select the day.

The job is listed in the Scheduled Jobs section until it runs at the scheduled time.
Periodic

You can schedule a job to run periodically, such as every two weeks or every three days. To specify a periodic schedule, you indicate the frequency the job should run and when you want the first job to run:

- **Run every** (number) of (minutes, hours, or days)
- **Starting at** (time) on (a specific date). Enter the time using a 24-hour clock.

The job will be listed in the **Scheduled Jobs** section.

Daily

You can schedule a job to run every day at a certain time. Specify the time using a 24-hour clock:

- **Run at** (hh): (mm)

The job will be listed in the **Scheduled Jobs** section.

Monthly

You can schedule a job to run monthly. To specify a monthly schedule, you indicate which day of the month to run the job as well as the time of day:

- **Run on the** (first, second, third, fourth, fifth) (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) of the month.
- **Run on day** (1-31) of the month.
- **Run on the last day of the month**.
- **Run at** (hh): (mm) Enter the time using a 24-hour clock.

The scheduled job will display in the **Scheduled Jobs** section.

It is important to remember that if the job that you are scheduling is big (meaning it will take a lot of time and resources), it is recommended you schedule the job to run during off-hours or on weekends.
Monitor Jobs

Scheduled Jobs list all the jobs that have been created and are either scheduled to run or have no schedule and must be run manually. Use this screen to see when scheduled jobs will run next, when jobs have last run, how many times each job has run, and who created the job.

1. Select Jobs > Scheduled Jobs.

2. From this list of scheduled jobs, you can select a job and perform any of the following tasks on the job:
   - **Edit**—Change any of the job parameters (basic information, operation parameters, targets, schedule). See "Edit a Job" on the facing page.
   - **Delete**—Permanently remove the job from the list of scheduled jobs
   - **Enable**—Re-enable a job that has been disabled
   - **Disable**—Disable the job so that it will not run as scheduled
   - **Run Now**—Initiate the operation of the job; any job can be manually run — unscheduled as well as scheduled

You can also right-click a job and select the task from the menu.

By default, jobs are sorted alphabetically by name. To sort by a different column:

1. Hover the mouse on the column heading you want to sort by, on the right edge of the column.
2. Click the triangle and select **Sort Ascending** or **Sort Descending**.
Edit a Job

You can edit any job listed on the Scheduled Jobs page.

1. Select Jobs > Schedule Jobs.
2. Select the name of the job that you want to edit. Click Edit. The web console displays the Edit Job Wizard.
3. Edit the information on each tab as needed to complete the job:
   - **Basic Info**—Change the job name, description, and whether to email job results. An asterisk denotes fields that are mandatory.
   - **Operation**—
     - For a Single Operation job, you can change any of the fields specific to the operation. (See "Job Operations" on page 432 for details.) However, you cannot modify the operation itself; if you want to change the operation, you will need to create a new job.
     - For a Multistep Operation job, you can add more jobs (Select Job), Remove jobs, Move Up/Move Down jobs in the execution order, and/or select the job to Stop on Fail for a specific job.

   This requires you to first create the Single Operation jobs you want to execute before they can be used in a Multistep Operation job.
   - **Targets**—Based on the operation, you can either add or remove targets, or a message displays stating that the job will run on the targets already specified.
   - **Schedule**—From Schedule, you can choose from the following schedule types. (See "Job Scheduling Options" on page 436).
     - Immediate
     - No Schedule
     - Run Once Only
     - Periodic
     - Daily
     - Weekly
     - Monthly

4. Click Save.
View Current Jobs

The Current Jobs section displays all currently running jobs. To view jobs that have already occurred, "View and Manage Job History" on page 442. To view all scheduled jobs, see "Monitor Jobs" on page 438. To cancel a currently running job, see "Cancel a Currently Running Job" on the facing page.

1. Select Jobs > Current Jobs. The top pane displays the following details:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This is the name you gave the job when you created it. See &quot;Add a Job&quot; on page 430.</td>
</tr>
<tr>
<td>Status</td>
<td>This is the current status of the job. The status of a job changes from Running to Complete.</td>
</tr>
<tr>
<td>Progress</td>
<td>This progress bar is constantly updating. You can view in real-time the progress of the current job. The color of the progress bar correlates with the top of the web console banner.</td>
</tr>
<tr>
<td>Start Time</td>
<td>This shows the start time (in a 24-hour clock format) of the current job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The shows the end time (in a 24-hour clock format) of the current job.</td>
</tr>
<tr>
<td>Description</td>
<td>This is the description you gave the job when you created it. Although entering a description is optional, the description (and name) help differentiate versions of the similar jobs. For example, a common job is &quot;Backup&quot;, but without a good description it is difficult to see which devices are currently being backed up.</td>
</tr>
</tbody>
</table>

Each time you start a job manually a Job Progress window displays. If you want to run the script in the background (and get rid of the window) while you do other tasks in Management Center, click Continue in Background.

2. If you select a name of a currently running job in the top pane, the details of that job appear in the two bottom panes.

3. The Job Progress Summary pane includes filters for the device on which the job is currently running. To cancel a currently running job, click Cancel.

If you have too many jobs going to keep track of, you can filter the results by:

- **Complete** = Green
- **Error** = Red (Hover your mouse over all jobs with errors to view the details of the error)
- **Warning** = (Hover your mouse over all jobs with warnings to view the details of the warning)
- **Running** = Grey (Grey signifies inactivity)

For more information on colors and status indicators, see "About Color-Coded Status Indicators" on page 34.
Cancel a Currently Running Job

To cancel a currently running job, select **Jobs > Current Jobs**.

1. Select the job you want to cancel.
2. Click **Cancel**.

Some steps of a job that are currently in progress will run to completion instead of being canceled.

3. Ensure that the job running is canceled by checking the **Status** column and the **Job Results** pane. Check for errors, which appear with a red exclamation mark in the Status column:

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>✉️ Error: The operation has</td>
</tr>
</tbody>
</table>

4. All jobs that you successfully cancel are obvious in the web console. Canceled jobs appear as such in the Status column.

Some jobs have multiple commands running on multiple devices. The more complex a job is, the more errors may occur when you choose to cancel a running job.
View and Manage Job History

View all past jobs and their status. The Job History section is similar to the Current Jobs list, but the Job History displays thousands of results of jobs that have already occurred. The Current Jobs section displays currently running jobs. To view currently running jobs, see "View Current Jobs" on page 440. To view all scheduled jobs, see "Monitor Jobs" on page 438. You can view more details of a completed job from Job History.

1. Select Jobs > Job History.
2. The Job History top pane displays the following details about each completed job:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This is the name you gave the job when you created it. See &quot;Add a Job&quot; on page 430.</td>
</tr>
<tr>
<td>Status</td>
<td>This is the status of the job. More details are available about the job.</td>
</tr>
<tr>
<td>Progress</td>
<td>This progress bar is displays completed jobs, with the latest job that was run always on top.</td>
</tr>
<tr>
<td>Start Time</td>
<td>This shows the start time (in a 24-hour clock format) of the selected job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The shows the end time (in a 24-hour clock format) of the selected job.</td>
</tr>
<tr>
<td>Description</td>
<td>This is the description you gave the job when you created it. Although entering a description is optional, the description (and name) help differentiate versions of the similar jobs. For example, a common job is &quot;Backup&quot;, but without a good description it is difficult to the different backups that occurred.</td>
</tr>
</tbody>
</table>

3. If you select a name of a job in the top pane, the details of that job appear in the two bottom panes. The job Name and the Job Results are detailed in the bottom panes. You can copy and paste the text in these panes. The text in the Status field is especially useful for debugging.

Management Center can be down while a job is running. The jobs that run while Management Center is down never appear in Current Jobs but they will appear in Job History when Management Center is back up and running.

4. To delete any jobs from the history, select the job(s) from the main list and click Delete.

View and Filter Job Progress

The Job Progress Summary pane includes filters for the device on which the jobs have run or are currently running. If you need to filter the Job History results, you can filter the results by:

- **Job Name**: Any part of the name of the job(s), such as searching for any job that includes "Backup" in the title.
- **Description**: Any keywords that may be in the description of the job(s).
- **Owner**: The current owner of the job(s).
- **Started by**: The user who first initiated the job(s).
- **Job Status**: The specific status of available jobs. The available statuses include:
  - Canceled
  - Complete
  - Failed to start
  - Interrupted
Each status also includes a colored icon, indicating the progress through the task.
  - **Complete** = Green (Green indicates that the job is running or has already run successfully)
  - **Error** = Red (Red signifies that the job did not run because of an error. Select the job name to drill down for the details)
  - **Warning** = Yellow (Yellow signifies the job ran, but issues occurred. Select the job name to drill down for the details)
  - **Running** = Green or Grey (Grey signifies inactivity)

**Step Status:** The specific status of step(s) within multistep jobs. Step statuses include:
  - Canceled
  - Complete
  - Continue Error
  - Error
  - Pending
  - Running
  - Skipped

**Date:** The start and/or end date for the range desired.

---

When the Job Progress window displays a currently running job that is taking a long time, you have the option to **Continue in Background**.

For more details on the use of color and status indicators, see “About Color-Coded Status Indicators” on page 34.

You cannot delete a job from Job History, you can only "Cancel a Currently Running Job" on page 441.
Management Center Reports

Management Center allows you to consolidate data from all, or a group of, ProxySG appliances you have added as managed network devices. Management Center offers Statistics Monitoring and Reporter reports.

Statistics Monitoring Reports

Statistics Monitoring reports consolidate statistics from your managed ProxySG devices. There are two categories of Statistics Monitoring reports:

- **Devices**: a variety of reports about the network traffic seen by a single ProxySG device, ProxySG appliances in a device group, or all ProxySG devices
- **WAN Optimization**: reports for ProxySG appliances with a Proxy or MACH5 Edition license.

"View Statistics Monitoring Reports" on page 501

For descriptions of each report, refer to "Reference: Statistics Monitoring Reports in Management Center" on page 502.

Reporter Reports

If you have integrated Symantec Reporter into Management Center, additional sets of reports are available to you. Reporter reports are grouped into the following categories:

- **Security**: reports that reveal activity on the network that may pose security or liability concerns.
- **Web Applications**: reports that provide insight into the web applications being accessed on your network, as well as the riskiness of these applications.
- **User Behavior**: reports that give you insight into the websites and categories of web traffic users are viewing or are blocked from viewing, and the amount of web traffic for different time periods.
- **Bandwidth Usage**: reports that analyze hourly, daily, and monthly bandwidth usage on the network, and estimate the time and data cost of that usage.

"Integrate Reporter into Management Center" on page 446

For descriptions of each of these reports, see "Reference: Report Descriptions" on page 465.

View Consolidated Reports

When using Management Center to manage and monitor ProxySG devices, you can produce reports that consolidate the data from all these devices or a group of devices, allowing you to get a complete picture of activity on your network. For example, you can view the bandwidth savings for all MACH5 appliances or get a list of the top web applications seen on the networks your ProxySG appliances are connected to.

Device Reports

To view reports about the network traffic seen by a group of ProxySG devices, or by all ProxySG devices managed in Management Center:
1. (Optional) Create device groups for the ProxySG devices you want to report on. See "Add a Device Group" on page 56.

2. Decide which Devices report to view (such as Traffic Mix or Traffic Statistics). For descriptions of each report, see "Devices Reports" on page 502.

3. Select Reports > Statistics Monitoring and choose the report from the Devices panel. By default, the report displays data from all ProxySG devices managed in Management Center.

4. (Optional) To narrow down the consolidated report to a group of devices:
   a. Click Device Filter: All Devices or click the Options button. The Filters dialog displays.
   b. From the Filter drop-down, select Device Group.
   c. Click and select the device group.
   d. Click Save.

**WAN Optimization Reports**

To display consolidated reports for ProxySG appliances with Proxy or MACH5 Edition licenses:

1. (Optional) Create device groups for the ProxySG devices you want to report on. See "Add a Device Group" on page 56.

2. Decide which WAN Optimization report to view. For descriptions of each report, see "WAN Optimization Reports" on page 503.

3. Select Reports > Statistics Monitoring and choose the report from the WAN Optimization panel. By default, the report displays data from all ProxySG devices with a Proxy or MACH5 Edition license that are being managed in Management Center.

4. (Optional) To narrow down the consolidated report to a group of devices:
   a. Click Device Filter: All Devices or Options. The Filters dialog displays.
   b. From the Filter drop-down, select Device Group.
   c. Click and select the device group.
   d. Click Save.

**Reporter Reports**

If you have integrated Symantec Reporter into Management Center, the following additional categories of reports are available: Security, Web Applications, User Behavior, Log Detail, and Bandwidth Usage. The Reporter reports consolidate data from all ProxySG appliances in the selected Reporter database.

1. Make sure you have added Reporter as a managed device in Management Center. See "Integrate Reporter into Management Center" on the facing page.

2. Select Reports > Reporter > Database and select the database from which you want to produce a consolidated report.

3. Decide which Reporter report to view. For descriptions of each report, see "Reference: Report Descriptions" on page 465.

Integrate Reporter into Management Center

Reporter Enterprise Server 10.1.x is required to access and view Reporter Reports and Dashboards.

Prerequisites

- Obtain or verify administrator access to Reporter Enterprise Server 10.1.x or later.
- Verify that Reporter Enterprise Server is deployed inline with ProxySG appliances within your network.
- Ensure that you have access to a Reporter Enterprise Server (username and password).
- To be able to view Reporter reports on managed devices, you will need to add a Reporter Enterprise Server from the Network tab.

Procedure

To integrate Reporter so that you can view Reporter reports in the Management Center web console:

1. Verify prerequisites above.
2. Add Reporter as a managed device in Management Center.
Add a Device

Before you can manage and monitor your devices, you must add them to Management Center. Devices that can be added to and managed by Management Center include the following:

- Advanced Secure Gateway (credential authentication or public key)
- Content Analysis
- Malware Analysis
- PacketShaper
- ProxySG (credential authentication or public key)
- Reporter
- Security Analytics
- SSL Visibility
- Web Security Service

Configure how often devices are polled. See "Set the Device Polling Interval" on page 523.

About Public Key or Credential Authentication for ProxySG or Advanced Secure Gateway

When adding a device, you must specify how Management Center will connect to it. Management Center can connect to a device using the following methods:

- **Credential authentication**: Management Center uses the device’s credentials to connect. Credential authentication is considered less secure because the device’s credentials are stored in Management Center. Therefore, it is recommended that you use public key authentication.

  Management Center always uses credential authentication when importing devices from Director.

- **Public key authentication**: Management Center inserts a copy of its public key onto the device. The device then "trusts" Management Center connections. This authentication method is considered more secure because device credentials are not stored on Management Center.

  Management Center does not remove its public key from devices that are deleted and no longer managed.

  You can manually delete the key using the following CLI command on the ProxySG or Advanced Secure Gateway:

  ```
  # (config ssh-console) delete director-client-key key-id
  ```

About Host Key Validation

Host key validation is a feature of the SSH protocol. It is designed to prevent devices from impersonating legitimate servers in an attempt to steal credentials and data (man-in-the-middle attack). To prevent this, each device has a unique host key that can be used to establish a host’s identity. If a device supports it, Symantec recommends that you enable host key validation because the method can warn you of a man-in-the-middle attack. In that case, Management Center notes that host verification failed and prompts you to verify the SSH host fingerprint.

You can verify the host fingerprint using one of the following methods:
Enter the following command from a terminal that has a trusted network path to the device:

```
# ssh keygen -lf <(ssh-keyscan device_ip2>/dev/null)
```

The system displays the host key.

Do the following from the device's serial connection:

a. Enter the following command:

```
# (config ssh-console) view host-public-key sshv2
```

b. Copy the output to a file, for example, `/tmp/hostkey`.

c. Enter the following command from a system running OpenSSH 7.2:

```
# ssh-keygen -l -e sha256 -f /tmp/hostkey
```

The system displays the host key.

Add a ProxySG or Advanced Secure Gateway using Credential Authentication

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select the device type.
5. Specify the **Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
   - Specify whether to collect statistics for the device. See "View Statistics Monitoring Reports" on page 501.
6. In **Connection**, click **Credentials**. Set the following:
   - The IP address or hostname of the device.
   - The SSH port.
   - The username and password you use to authenticate to the device.
   - Your enable password for administrator actions.
   - Confirm whether to **Enable host key validation** (recommended).
7. Click **Connect**. Management Center attempts to connect to the device using the information you entered.
8. If you enabled host key validation, verify the SSH Host Fingerprint and click **Accept**.
9. Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

10. Verify or change the **Device Name**.
12. Click **Save**.
Management Center Configuration & Management

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

Add a ProxySG or Advanced Secure Gateway using Public Key Authentication

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select the device type.
5. Specify the **Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
   - Specify whether to collect statistics for the device. See "View Statistics Monitoring Reports" on page 501.
6. In **Connection**, click **Public Key**. Set the following:
   - The IP address or hostname of the device.
   - The SSH port.
   - Your enable password for administrator actions.
   - Confirm whether to **Enable host key validation** (recommended).
7. Click **Connect**. Management Center attempts to connect to the device using the information you entered.
8. If you enabled host key validation, verify the SSH Host Fingerprint and click **Accept**.
9. Enter the username and password you use to authenticate to the device. You must do this so that Management Center can install its public key onto the ProxySG appliance. The credentials are not saved.

Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

10. Verify or change the **Device Name**.
12. Click **Save**.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

Add a Reporter

Symantec recommends that you create a new non-administrator Reporter role before adding Reporter to Management Center. If you choose to add a Reporter using the default Admin role, you must specify the role as "_admin._"

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select the device type.
5. Specify the **Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
6. In **Connection**, specify the following:
   - The IP address or hostname of the device.
   - The protocol and port (HTTP or HTTPS).
   - The username and password you use to authenticate to the device.
   - The Reporter role. Specify the role assigned to this user in Reporter. If this is an admin account, input _admin_.
7. Click **Connect**. Management Center attempts to connect to the device using the information you entered.

Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

8. Verify or change the **Device Name**.
10. Click **Save**.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

**Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility**

If you upgrade an SSL Visibility appliance from 3.x to 4.x, you must delete the 3.x device from Management Center and then add it back as a 4.x device.

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select the device type.
5. For SSL Visibility only, select the version **3.8.3+ or 4+**.
6. Specify the **Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
7. In **Connection**, specify the following:
   - The IP address or hostname of the device.
   - The protocol and port (HTTP or HTTPS).
Management Center Configuration & Management

- The username and password you use to authenticate to the device.

8. Click Connect. Management Center attempts to connect to the device using the information you entered.

Management Center attempts to connect to the appliance. If the connection is established, the system displays Successful.

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

9. Verify or change the Device Name.
11. Click Save.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

Add a Security Analytics

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click Add Device. The system displays the Add Device wizard.
4. Select Security Analytics.
5. Specify the Device Management Modes:
   - Select Existing device if the device is already installed, or Unavailable (pre-deployment) if the device is not available yet. See "About Pre-Deployed and Deactivated Devices" on page 109 for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 125 for more information.
6. In Connection Details, specify the following:
   - The IP address or hostname of the device.
   - The port (the default is HTTPS 443).
   - The username you use to authenticate to the device.
   - In the Password field, enter the Security Analytics device API key.
7. Click Connect. Management Center attempts to connect to the device using the information you entered.

Management Center attempts to connect to the appliance. If the connection is established, the system displays Successful.

If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

8. Verify or change the Device Name.
10. Click Save.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

Add Web Security Service (WSS)
Note: As of November 2017, all connections from Management Center to WSS use the same username, *(mc-register)* and a unique token that identifies your WSS account as unique. This token associates your connection with the appropriate WSS account.

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select the device type.
5. Specify the **Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See “About Pre-Deployed and Deactivated Devices” on page 109 for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See “Put Device in Read-Only Mode” on page 125 for more information.
6. Open another browser, and log in to the WSS portal at [https://portal.threatpulse.com](https://portal.threatpulse.com).
   a. Click the **Solutions** menu and select **Service**.
   b. Click **Account Maintenance** and select **Integrations**.
   c. Click **New Integration**. The portal displays the **New Integration** wizard.
   d. Set the **Expiry Type** as appropriate for your purposes. If you select **Never**, the token can be used indefinitely.
   e. Copy the contents of the **Token** field and click **Save**.
7. Switch back to Management Center and do the following:
   a. Select the **Cloud Network** to connect to, Production or Pre-Production.
      
      If you are participating in a beta program, click **Analyze in Pre-Production**.
   b. Click **Connect**.
   c. Enter **mc-register** as the username and paste the integration token from the portal as the password.
   d. Click **Register**. After successfully connecting, the system populates the **Name** fields.

     After connecting to the WSS, Management Center deletes the credentials. They are not saved. For failover, this has special implications.

     If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

8. Verify or change the **Device Name**.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>&quot;Ensure Devices Belong to Device Groups&quot; on page 118</td>
</tr>
<tr>
<td>Check information specific to the selected device.</td>
<td>&quot;Monitor Device Health&quot; on page 58</td>
</tr>
<tr>
<td>Check device metrics.</td>
<td>&quot;View System Metrics&quot; on page 121</td>
</tr>
</tbody>
</table>
View a Reporter Report

Reporter reports can only be viewed if you have already added the Reporter Enterprise Server as a managed device. Reporter Enterprise Server 10.1.x is required to access and view Reporter Reports and Dashboards.

You can view one of the built-in reports as described below, or create your own custom reports and groups.

The procedure below documents an example of how to view a Reporter report. This example uses the Security report Trend of Blocked Requests.

1. Select Reports > Reporter.
2. Select a role and the Reporter database from the Database drop-down list at the top of Reports Home. The database you select determines the list of available reports.

If the database you want is not available, see "Determine Why A Reporter Database Does Not Display" on page 491.

Reporter has the following report categories:

- Security
- User Behavior
- Log Detail
- Bandwidth Usage
- Web Applications

3. In this example, select Trend of Blocked Requests in the Security list. A default line graph is displayed with Average Requests and a Normal Request Range. Line graphs show how data for the trend changes over time. Average Requests represent the average number of blocked requests specific to your organization. The Normal Request Range is a calculation that produces a "normal" range of blocked requests specific to your organization.

4. (Optional) Change the date filter to display a different time range on the report. The default time range for this report is 7d (7 days).
You can also use the arrows and to filter the date and time. When you change the date range, the dates are expanded or contracted along the bottom of the report.

5. (Optional) Most report data is generated in UTC time. To ensure the report you're viewing is relevant to the time zone where the users are located, you can set a time zone by clicking . The Profile dialog appears, with Reporter Time Zone selected. Select your preferred time zone from the drop-down menu and click Save.

6. (Optional) From the Quick Pick drop-down, select a type of relative date filter, for example, Before or Since.

7. (Optional) Change the graph type by selecting the button next to Actions

Graph types include:

- **Area** - An area graph displays graphically quantitative data. It is based on the line chart. The area between axis and line are commonly emphasized with colors and textures. Commonly used area graphs compare one area with two or more areas.

- **Bar** - A bar graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted horizontally and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped bar graphs display bars clustered in groups of more than one bar graph.

- **Column** - A column graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted vertically and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped column graphs display bars clustered in groups of more than one column graph.

- **Line** - Line graphs show how data for one data type changes over time.

- **Pie** - A pie graph is a circular statistical graphic, divided into slices to illustrate numerical proportion. In a pie graph, the arc length of each slice (and thus the central angle and area), is proportional to the quantity it represents. The pie chart displays the value name and metric when a user hovers the mouse over a section.

8. The default overlay for the Trend of Blocked Requests report is Requests. (Optional) To add or change overlays, select an overlay from the legend on the right of the report. Each overlay is represented by a different color and pattern. For example:
9. (Optional) Click each data type, (Requests, Page Views, Browse Time, etc.) to have them appear in the open report. To remove data types from the graph, click the appropriate entry again.

10. (Optional) Save the customized report you have open by clicking Actions > Save As. The Save As Dialog appears.
11. (Optional) Save the current report view in PDF, HTML, or CSV format for offline viewing. Click Actions > Download. The web console displays the Download dialog.

a. Select the format, PDF, HTML, or CSV.
b. For PDF, select the orientation, Portrait or Landscape. (This is not applicable to HTML or CSV.)
c. Select the number of rows you want included in the offline report. Leave the default value, Visible, if you
Management Center Configuration & Management

would like the report to contain only the data that appears on screen.

d. Click Download. Click Close to cancel.

12. (Optional) To view a report that is currently open, select that report from the menu on the left of the page. When multiple databases are available, open reports are separated by database.

13. (Optional) In addition to a graph, each report includes a table that displays the data used in the graph. You can drill down into this data to display additional reports. For example, if a Category report is displayed, you can click one of the categories in the data grid and drill down to find out what sites are being viewed and who is viewing them. There are two ways to drill down in a report:
   a. Click the text in the data field that you want to drill down into. The Overview report for that element, (URL, Category, User, etc.) displays.
   b. Right-click any field in the table at the bottom of a report to display a list of fields. The menu will display fields common to the type of report you are viewing. In the below example, a Category report offers Site as the most common option, to display the sites listed in the selected category. Select your preferred field from the More
Fields menu item to view drilled-down reports for other data fields.

14. (Optional) Generate an **Overview** report of items in the data grid. To see more information about an item in the report, click the hyperlink to launch an **Overview** report for that item. For example, if you click the hyperlink for CNN, the Overview report will show a daily trend of traffic to CNN, the top users and Client IPs accessing CNN, and a breakdown of the protocols used to access CNN.
15. (Optional) Filter or change the report criteria.

**Customize Reporter Report Options**

Starting with Management Center 1.6, you can now customize every Reporter report. In some cases, these reports can take significantly longer to run than the standard reports available on Management Center. You can create your own custom reports and save them by using the **Save As** button and providing the report with a name. See "Create a Custom Report" on page 475 for more information.

You can alter what is reported in the following ways:

- "Add Report Filters" below
- "Change the Report Grouping" on page 461

**Add Report Filters**

1. Select a Reporter database.

2. Select the desired report.

3. Optional—adjust the report settings (date range, format, and so on).

4. To customize the report, select the gear icon in the upper right corner.
5. Add a filter.
   a. In the **Filters** section, click **Add Filter**.

   ![Add Filter](image)

   b. Select a field.

   ![Select Field](image)

   c. Select the appropriate operator. The available operators change depending on the selected action.
Management Center Configuration & Management

6. Optional—Add another filter by repeating step 5. You can add any number of filters.

7. Click Run Report.

Filter Examples

Example 1: If the administrator selects the filter Site, the operator contains, and enters facebook for the value, the report returns only sites that contain the string “facebook.”

Example 2: If the administrator selects the filter Client IP, the operator matches, and enters the IP address range 10.1.1.0/22, the report includes all addresses in that network mask.

Example 3: If the administrator selects the filter Hours of Day, the operator in between, and selects the hours 9 a.m. and 5 p.m, the report includes data only for the time between 9 and 5.

Change the Report Grouping

This section describes how to change the way the information in a report is grouped.
Change the number of items displayed per page

1. In the **Group By** section, change the **Display** value.

2. Change other options as desired.

3. Click **Run Report**.

Change the grouping of the report (that is, change the focus of the report).

1. In the **Group By** section, choose the field you want to focus the report on from the **Group By** drop-down list. This field is the main metric that Management Center uses to present the data.
If a Reporter administrator had created custom log fields in Reporter 10.x, these fields will be displayed in the list along with the standard built-in fields.

2. Change other options as desired.

3. Click Run Report.

When you change the Group By field, a new report is generated and the name of the report is changed to match your selection. The previous report is still available in the left pane.

Create a two-level report

1. In the Group By section, click Two Level for the Summary Type.

2. Select the two values to report. In the following example, the report is grouped by Day and then by Verdict.
3. Change other options as desired.
4. Click **Run Report**.
Reference: Report Descriptions

The following report groups are available if you have integrated Reporter 10.1.x or later with Management Center:

- Security
- User Behavior
- Bandwidth Usage
- Web Applications
- Log Detail

From the Database drop-down list, select the Reporter database to use in your reports. The information displayed in the report group will differ according to the database selected. For example, WAF database reports contain an Actions report in the Security group. That report is not displayed for other databases.

The following tables briefly describe the default graph in each of the Reporter reports. In addition to a graph, each report has a data grid displaying the statistics used in the graph, you can drill-down into this data for more details. Note that you have many options for customizing reports: displaying just the graph, displaying just the data grid, changing the graph type, specifying a date filter, and selecting/unselecting overlays. See "View a Reporter Report" on page 453 for details.

- Reporter reports in Management Center are derived from Reporter database log files, and these reports may be different or enhanced from similar reports in Reporter Enterprise Server.

### Security

The Security reports reveal activity on the network that may pose security or liability concerns. The available reports may differ depending on the selected database type.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentially Infected Clients - Unified</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database.</td>
</tr>
<tr>
<td></td>
<td>Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing results from the Symantec Content Analysis (CA) appliances and Malware Analysis (MA) appliances that are deployed as part of your SGOS proxy security solution. These reports are called Unified reports.</td>
</tr>
<tr>
<td></td>
<td>Displays an area, bar, column, or pie chart of the client IP addresses that might be infected by malicious content, as found by sandboxing, file reputation, predictive analysis score, anti-virus, and WebPulse. By default, the report lists each IP address, sorted by the number of risky requests.</td>
</tr>
<tr>
<td>Potential Malware Infected Clients</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td></td>
<td>Displays a bar chart of the client IP addresses that might be infected by malicious content, as found by sandboxing, file Reputation, anti-virus, WebPulse. By default, the report lists each IP address, sorted by the number of risky requests.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malware Detected Names</td>
<td>Displays a bar chart of the names of the malware detected by Content Analysis/ Proxy AV. To view this report, you must add a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Blocked Users</td>
<td>For each user, this report shows a bar chart of the number of requests that were blocked due to the URL being from one or more of the following categories: Spyware, Suspicious, Phishing, or Malicious.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Blocked Request by User Agent</td>
<td>For each user agent (browser + version), the report shows a bar chart of the number of blocked web requests to URLs from one of the following categories: Spyware, Suspicious, Phishing, or Malicious.</td>
</tr>
<tr>
<td>Threat Sites Blocked</td>
<td>Displays a bar chart of the websites that had blocked web requests to URLs from any of the following categories: Spyware, Suspicious, Phishing, or Malicious. The sites with the most blocked web requests appear at the top of the report.</td>
</tr>
<tr>
<td>Trend of Risky Requests</td>
<td>Displays a line graph that shows the number of risky web requests (for example, requests to URLs of malware categories) over the specified time period. The graph contains a shaded area that represents the <em>normal requests range</em>, which is a range based on the organization’s web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of risky web requests during the last month.</td>
</tr>
<tr>
<td>Trend of Risky Users</td>
<td>Displays a line graph that shows the number of users making requests to URLs of risky categories (<em>Spyware, Suspicious, Phishing, or Malicious</em>) over the specified time period. The graph contains a shaded area that represents the <em>normal count range</em>, which is a range based on the organization’s web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of users making risky web requests during the last month.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> User drill-downs are blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Trend of Blocked Requests</td>
<td>Displays a line graph that shows the number of web requests that were blocked over the specified time period. The requests could be blocked for a variety of reasons, such as due to deny policies on the ProxySG. The graph contains a shaded area that represents the <em>normal requests range</em>, which is a range based on the organization’s web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of risky web requests blocked during the last month.</td>
</tr>
<tr>
<td>Trend of Blocked Users</td>
<td>Displays a line graph that shows the number of users who were blocked over the specified time period. The users could be blocked for a variety of reasons, such as due to deny policies on the ProxySG. The graph contains a shaded area that represents the &quot;normal count range,&quot; a range based on the organization’s web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of users blocked during the last month.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> User drill-downs are blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Trend of Risky Clients</td>
<td>Displays a line graph that shows the number of client IP addresses that accessed URLs in the following categories: Spyware, Suspicious, Phishing, or Malicious. The graph contains a shaded area that represents the &quot;normal count range,&quot; a range based on the organization’s web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of client IPs that were potentially infected during the last month.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Threats</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td></td>
<td>Displays a bar chart that provides details for the number of threats discovered by each detection method</td>
</tr>
<tr>
<td></td>
<td>(Sandboxing, File Reputation, Anti-virus, WebPulse).</td>
</tr>
<tr>
<td>Threats - Unified</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database.</td>
</tr>
<tr>
<td></td>
<td>Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing</td>
</tr>
<tr>
<td></td>
<td>results from the Symantec Content Analysis (CA) appliances and Malware Analysis (MA) appliances that are</td>
</tr>
<tr>
<td></td>
<td>deployed as part of your SGOS proxy security solution. These reports are called Unified reports.</td>
</tr>
<tr>
<td></td>
<td>Displays an area, bar, column, or pie chart that provides details for the number of threats discovered by each</td>
</tr>
<tr>
<td></td>
<td>detection method (sandboxing, file reputation, predictive analysis score, anti-virus, WebPulse).</td>
</tr>
<tr>
<td></td>
<td>If Malware Analysis processing results in a detonation, the Malware Analysis sends that result to the Content</td>
</tr>
<tr>
<td></td>
<td>Analysis, which notifies the SGOS proxy device. The SGOS proxy device caches the result and blocks subsequent</td>
</tr>
<tr>
<td></td>
<td>requests that match. However, the log entries for these cache block actions do not contain the sandboxing vendor</td>
</tr>
<tr>
<td></td>
<td>or score. Because of this, you might not see the Malware Analysis benefits reflected in the reports. For</td>
</tr>
<tr>
<td></td>
<td>example, the SGOS proxy device might block 20 requests that match a cached result; the Malware Analysis is</td>
</tr>
<tr>
<td></td>
<td>credited with only one result (the one that resulted in the cache entry). However, when the SGOS proxy device</td>
</tr>
<tr>
<td></td>
<td>receives a clear cache action (for example, when new AV patterns are loaded), the Malware Analysis action</td>
</tr>
<tr>
<td></td>
<td>re-occurs on the next request.</td>
</tr>
<tr>
<td>Trend of Threats</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td></td>
<td>Displays a column chart that shows the trend over time for each detection method (Sandboxing, File</td>
</tr>
<tr>
<td></td>
<td>Reputation, Anti-virus, Web Pulse).</td>
</tr>
<tr>
<td>Trend of Threats - Unified</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database.</td>
</tr>
<tr>
<td></td>
<td>Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing</td>
</tr>
<tr>
<td></td>
<td>results from the Symantec Content Analysis (CA) appliances and Malware Analysis (MA) appliances that are</td>
</tr>
<tr>
<td></td>
<td>deployed as part of your SGOS proxy security solution. These reports are called Unified reports.</td>
</tr>
<tr>
<td></td>
<td>Displays an area, bar, column, or pie chart that shows the trend over time for each detection method (sandboxing,</td>
</tr>
<tr>
<td></td>
<td>file reputation, predictive analysis score, anti-virus, WebPulse).</td>
</tr>
<tr>
<td>Threats - WAF</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td></td>
<td>Displays an area, bar, column, or pie chart that shows the number of threats by category (attack family or</td>
</tr>
<tr>
<td></td>
<td>anti-virus). Each colored section represents a threat type and corresponding number of incidents.</td>
</tr>
<tr>
<td>Trend of Threats - WAF</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td></td>
<td>Displays an area, bar, column, or pie chart that shows the trend over time for anti-virus and attack family</td>
</tr>
<tr>
<td></td>
<td>threats.</td>
</tr>
<tr>
<td>Actions</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td></td>
<td>Displays an area, bar, column, or pie chart that shows action-related data. This data includes requests,</td>
</tr>
<tr>
<td></td>
<td>page views, browse time, cost (time), cost (bytes), total bytes, bytes sent, bytes received, cache bytes,</td>
</tr>
<tr>
<td></td>
<td>server bytes, bytes saved.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Methods</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows data per HTTP method. These actions include requests, page views, browse time, cost (time), cost (bytes), total bytes, bytes sent, bytes received, cache bytes, server bytes, bytes saved.</td>
</tr>
<tr>
<td>Attack Families</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of requests per attack type (for example, SQL injection). The data corresponds to that recorded for the x-bluecoat-waf-attack-family log field. Each slice represents an attack type. The chart displays only the top ten attack types.</td>
</tr>
<tr>
<td>Attack Families Per Country</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the total number of attacks per country. The bar is segmented; each color represents a different attack type. The chart displays only the top ten countries. The data is based on geolocation data and is only shown when either x-bluecoat-waf-attack-family or x-virus-id does not include “-“ .</td>
</tr>
<tr>
<td>Sandboxing Risk Score</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</td>
</tr>
<tr>
<td>Trend of Sandboxing</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for each risk score.</td>
</tr>
<tr>
<td>Trend of Predictive Analysis</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for each predictive analysis score.</td>
</tr>
<tr>
<td>Trend of File Reputation</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for each file reputation score.</td>
</tr>
<tr>
<td>File Risk Score</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</td>
</tr>
<tr>
<td>File Risk Score</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</td>
</tr>
<tr>
<td>URL Threat</td>
<td>To view this report, you must add a Reporter appliance running 10.1.5.4 or later. Displays a pie chart that shows the risk threat level (a rating between 1 and 10) of URLs. Malicious sites rank higher (for example, a 9 or 10) while a site that may be questionable, yet not malicious, may rank lower (for example, a 4 or 5). You can use the report to filter out specific risk levels. You can also see the users who visit the higher risk sites more frequently.</td>
</tr>
</tbody>
</table>
### Description of Default Graph

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risky Sites per Country</td>
<td>To view this report, you must add a Reporter appliance running 10.1.5.4 or later. Displays which sites in countries are getting the most risky traffic (a web threat level of 7 or greater). This provides the ability to drill down to more specific information, such as which sites are being viewed by country.</td>
</tr>
<tr>
<td>Risky Clients per Country</td>
<td>To view this report, you must add a Reporter appliance running 10.1.5.4 or later. Displays which clients are visiting the riskiest sites (a web threat level of 7 or greater). The report gives the ability to view specific client risk information, such as which clients are requesting the riskiest sites, and even the clients they are speaking to.</td>
</tr>
</tbody>
</table>

### User Behavior

The User Behavior reports give you insight into the websites and categories of web traffic users are viewing or are blocked from viewing, and the amount of web traffic for different time periods.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked Requests by Site</td>
<td>Displays a bar graph that shows the number of web requests that were blocked on each website. The sites with the most blocked requests appear at the top of the report.</td>
</tr>
<tr>
<td>Blocked Requests by Category</td>
<td>Displays a bar graph that shows the number of web requests that were blocked in each URL category. The categories with the most blocked requests appear at the top of the report.</td>
</tr>
</tbody>
</table>
| Blocked Requests by User      | Displays a bar graph that shows the number of web requests that were blocked for each user. The users with the most blocked requests appear at the top of the report.  
**Note:** This report will be blank if user name data isn’t available in the Reporter log file. |
| Filtering Verdict Trend by Day| Displays a stacked column graph that shows the number of web requests that triggered specific policy verdicts. By default, all verdicts are selected; you will want to select just the policy verdicts you are interested in (such as connect_method_denied and policy_denied). |
| Sites                         | Displays a bar graph that lists the websites with the most page views. For each website, the graph illustrates the number of page views during the specified time period. The site with the most page views appears at the top of the report. |
| Categories                    | Displays a pie chart that shows the categories with the most page views; all other categories are combined into an Other slice. |
| Categories per User           | Displays a bar graph that lists the names of the most active users and indicates the most accessed URL categories for the pages they viewed. The graph shows the number of pages viewed in each category for each user.  
**Note:** This report will be blank if user name data isn’t available in the Reporter log file. |
| Users                         | A bar graph that shows the users with the most page views during the specified time period. The user with the most page views appears at the top of the report.  
**Note:** This report will be blank if user name data isn’t available in the Reporter log file. |
<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IPs</td>
<td>Displays a bar graph that shows the client IP addresses with the most page views during the specified time period. The client IP with the most page views appears at the top of the report.</td>
</tr>
<tr>
<td>User Agent Families</td>
<td>In releases prior to 1.11.1.5, you must add a WAF database from a Reporter appliance running 10.1.3.x or later to view this report. In 1.11.1.5 and later, this report is available for Main and Unified databases if you are using a Reporter 10.1.5.x database. Displays an area, bar, column, or pie chart that shows the top 10 client user agent families (not user agent strings). For example, Firefox.</td>
</tr>
<tr>
<td>Countries</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the top ten countries per number of requests (based on geolocation data).</td>
</tr>
<tr>
<td>Protocols</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of number or requests per protocol. The chart shows only the top 10 protocols.</td>
</tr>
<tr>
<td>Days</td>
<td>Displays an area graph that shows the number of web requests for each day in the selected time period.</td>
</tr>
<tr>
<td>Days of Week</td>
<td>Displays a column graph that shows the number of web requests for each day of the week in the selected time period. For example, the Monday column reflects the total of all requests that were made on Mondays during the time period. This report allows you to see how the trends in web browsing differ by day of the week.</td>
</tr>
<tr>
<td>Hours of Day</td>
<td>This column graph totals web requests for each hour of the day. For example, every Web page request that occurred at 9am, 10am, and so on. This allows you to analyze which hours are consistently the heaviest with Web requests. Network administrators might use this data to adjust bandwidth policy.</td>
</tr>
<tr>
<td>Months</td>
<td>This report totals web requests for each month. For example, every web page request that occurred in January, February, and so on. This allows you to drill down each month and analyze trends.</td>
</tr>
<tr>
<td>Trend of Discovered Users</td>
<td>Displays the number of unique users per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
</tbody>
</table>

**Bandwidth Usage**

Use the **Bandwidth Usage** reports to analyze hourly, daily, and monthly bandwidth usage on the network, and to estimate the time and data cost of that usage.

The cost-related reports calculate bandwidth cost based on the **Cost per MB** and **Cost per Hour** settings in Reporter. For example, if **Cost per Hour** is set to $10, the Cost (Time) value is calculated by multiplying the time spent web browsing by $10. Or if Cost per MB is set to $4, the Cost (Bytes) value is calculated by multiplying the number of megabytes of traffic by $4.
<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
</table>
| Cost per User| The data in this bar graph approximates the cost accrued per user based on total bytes of throughput and time spent web browsing. Reporter lists each user, sorted by the total cost of bandwidth. 
**Note:** This report are blank if user name data isn’t available in the Reporter log file. |
| Cost per User and Site | Displays a bar graph that shows the total bandwidth cost for the websites each user visited during the selected time period. The users with the highest bandwidth cost appear at the top of the graph. 
**Note:** This report are blank if user name data isn’t available in the Reporter log file. |
| Cost per Hour of Day | Displays a column chart that shows the total cost of time and bandwidth for each hour of the day. For example, total cost at 9am, 10am, and so on. This allows you to analyze which hours have the most traffic and are therefore most expensive. Network administrators might use this data to adjust bandwidth policy. |
| Cost per Day | Displays an area chart that shows the cost of time and bandwidth each day in the specified time period. |
| Cost per Day of Week | Displays a column graph that shows the total cost of time and bandwidth each day of the week in the selected time period. For example, the Monday column reflects the total cost on Mondays during the time period. This report allows you to see how the cost of web usage differs by day of the week. |
| Cost per Month | This area graph totals time and bandwidth costs for each month. For example, total costs in January, February, and so on. This allows you to drill down each month and analyze trends. |
| Bandwidth per Hour of Day | This column chart shows the total bytes sent and received for each hour of the day. For example, total bandwidth usage at 9am, 10am, and so on. This allows you to analyze which hours have the most traffic. Network administrators might use this data to adjust bandwidth policy. |
| Bandwidth per Day | This area chart shows the total bytes sent and received each day in the specified time period, allowing you to see a trend of bandwidth usage over time. |
| Bandwidth per Day of Week | This column graph shows the total bytes sent and received each day of the week in the selected time period. For example, the Monday column reflects the amount of bandwidth used on Mondays during the time period. This report allows you to see how the trends in web usage differ by day of the week. |
| Bandwidth per Month | This area chart shows total bandwidth used each month. For example, total bytes in January, February, and so on. This allows you to drill down each month and analyze trends. |
| Server IPs | To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of requests per server IP address. You can also select other data, including requests, page views, browse time, cost (time), cost (bytes), total bytes, bytes sent, bytes received, cache bytes, server bytes, and bytes saved. |

**Log Detail**

The Log Detail reports provide information about the bcreporterwarp_v1 access log fields.
### Web Applications

The **Web Application** reports provide insight into the web applications being accessed on your network, as well as the riskiness of these applications.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Log Details</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a grid report of the access log fields associated with the selected database. For example, if a WAF database is selected, this report shows data for the bcreporterwarp_v1 access log.</td>
</tr>
<tr>
<td>Blocked Log Details</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a grid report of the access log fields for blocked requests associated with the selected database. For example, if a WAF database is selected, this report shows data for the bcreporterwarp_v1 access log.</td>
</tr>
<tr>
<td>Web Applications</td>
<td>A bar graph that shows the number of requests for each web application during the specified time period. The web applications having the most web requests appear at the top of the report. Use this report to see what types of web application traffic are running on your network.</td>
</tr>
<tr>
<td>Web Applications by Users</td>
<td>Displays a pie chart of the top web applications as calculated by the number of users accessing the content over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Web Applications by Client IPs</td>
<td>Displays a pie chart of the top web applications as calculated by the number of unique IP addresses accessing the content over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Blocked Web Applications</td>
<td>Displays a bar graph that shows the number of web requests denied by a policy verdict (that is, blocked) for each web application during the specified time period. The web applications with the most blocked requests appear at the top of the report. Use this report to confirm that policies are being enforced properly.</td>
</tr>
<tr>
<td>Trend of Active Web Applications</td>
<td>Displays the number of unique web applications per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Trend of Web Application Traffic</td>
<td>Displays total bytes sent, bytes received, and the number of requests per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Web Application Operations</td>
<td>Displays a bar graph that shows the number of requests for different web application operations (such as Play Video, Download Files, Upload Media) during the specified time period.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Users of Risky Applications</td>
<td>Risky applications are those with risk scores greater than 70. (You can change the filter to make the number higher or lower.) Ranked by total bytes received, this report lists users who have accessed web applications that are widely deemed as risky for business network use.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Web Applications per Risk</td>
<td>Displays a pie chart that shows the number of requests for web applications at each risk score (1 to 10). For example, the report shows a bar for each risk score with different color segments representing different web applications. The length of each segment corresponds to the number of requests for that application.</td>
</tr>
<tr>
<td></td>
<td><strong>Tips:</strong></td>
</tr>
<tr>
<td></td>
<td>• Sort the values in the Web Application column to alter the pie chart to show the corresponding data.</td>
</tr>
<tr>
<td></td>
<td>• You may want to turn off the Other overlay, if this segment has a significant number of requests.</td>
</tr>
<tr>
<td>Users Per Risk Score</td>
<td>Shows the number of users per risk score (1 to 10) over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Risk Distribution Per User</td>
<td>Displays a pie chart that shows the percentage of requests at each risk level. Each slice represents a risk level.</td>
</tr>
<tr>
<td>Risk Distribution Per User</td>
<td>Displays a color-coded bar chart that shows the amount of traffic (hits and bytes) for each risk score (1 to 10) per user over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Trend of Risk Distribution</td>
<td>Displays a color-coded bar chart representing the amount of traffic (hits and bytes) for each risk score (1 to 10) per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Social Media Activity</td>
<td>Displays a bar graph that shows the number of requests for each operation (such as Post Messages and Upload Media) used in social networking web applications. The operations that have the most activity appear at the top of the report.</td>
</tr>
<tr>
<td>Social Media Applications</td>
<td>Displays a bar graph that shows the number of requests for each social networking application (Facebook, Twitter, Pinterest, and so on). The social networking applications with the most requests appear at the top of the report. With this report, you can see how much social media traffic your network has and which applications are most popular. Depending on company policy, you may decide to put controls on social networking after viewing this report.</td>
</tr>
<tr>
<td>Facebook Users</td>
<td>Displays a bar graph that shows the number of Facebook requests by each user. The names of the users with the most Facebook requests appear at the top of the report. This report allows you to see who the most active Facebook users are.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Facebook Categories</td>
<td>Displays a bar chart that shows the amount of traffic attributed to different categories of Facebook traffic (other than social networking). For example, you can see the number of Facebook requests that are for games or messaging.</td>
</tr>
<tr>
<td>Mail Activity</td>
<td>Displays a bar graph that shows the number of requests for various email operations. For example, you can see the number of requests for Send Email, Download Attachment, and Upload Attachment operations for email web applications.</td>
</tr>
</tbody>
</table>
### Report | Description of Default Graph
---|---
Mail Applications | Displays a bar graph that shows the number of requests for web mail applications (Gmail, Yahoo Mail, Hotmail, and so on). The email applications with the most requests appear at the top of the report. This report allows you to determine the most popular web mail applications on your network.
Top Mail Senders | Displays a bar graph that shows, for each user, the number of requests for Send Email or Send Attachment operations. This report allows you to see which users are the biggest web mail consumers. The IP addresses of the users with the most web mail traffic appear at the top of the report.
Search Terms | Displays a bar graph that displays top search terms that users enter in browser search engines (Google, Yahoo, Bing, and so forth). You can drill down to find the user(s) who searched for the term and which search engine was used.
Search Applications | Displays a bar graph that displays the number of requests for each search engine (Search Engines/Portals category).

### Create Custom Report Groups
Reporter-based reports are grouped into five groups: Security, Bandwidth Usage, User Behavior, Log Detail, and Web Applications. These groups are static and cannot be modified. However, you can create your own report groups and save custom reports you create into these new groups.

1. Select **Reports > Reporter**.
3. Enter a **Name** for the report group.
4. (Optional) Enter a **Description** up to 1024 characters.
5. Click **Save**. The container for the new group displays at the bottom of the Reporter page, underneath the built-in groups. You can now create and save custom reports to this group.

### Additional Information

- To modify the name or description of a custom report group, click the gear icon in the group's title bar.
- To delete a custom report group, click the delete (X) icon in the group's title bar. Note that you cannot delete a group that contains custom reports; you must delete the reports before you can delete the group.
- To move a custom report from one group to another, select the check box next to the report name and issue the **Operations > Move** command.

### Create a Custom Report

If you can't find a standard Reporter report that suits your needs, you can design and save a custom report using Management Center’s flexible and powerful report designer. When designing your report, you choose one or two metrics to report on, select the type of chart (such as pie or bar), define the report time frame (such as one day or one year), select the columns of data (for example, Page Views and Bytes Sent), and configure one or more filters (such as a particular URL category or a range of risk scores). As you design your report, it dynamically displays in the preview window with sample data so that you can get a good picture of what it will look like.

Once you have finished designing the report, you can save it for future use and run it at any time.

### Step 1: Create the Report

1. Select **Reports > Reporter**.
2. Select a Reporter database.
4. (Optional) To enlarge the Preview window, hover on the divider line between panes and drag to the left.
5. From the **Group By** drop-down list, select the main metric that Management Center will use to present the data.
If a Reporter administrator had created custom log fields in Reporter 10.x, these fields will be displayed in the list along with the standard built-in fields.

6. In the **Display** field, specify the number of items to display in the chart.
7. If you want to report on two metrics:
   a. Select Two Level for the Group Type. An additional row displays so that you can choose a second metric.
   ![Group By window](image)
   b. In the Then By drop-down, select the secondary metric to report on.
   c. Select the number of items to Display.

8. As you set options, watch the report build in the Preview window pane.

**Step 2: Select the Chart Type**

Horizontal bar is the default chart type. The following chart types are available:

- **Area** - An area graph displays graphically quantitative data. It is based on the line chart. The area between axis and line are commonly emphasized with colors and textures. Commonly used area graphs compare one area with two or more areas.

- **Bar** - A bar graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted horizontally and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped bar graphs display bars clustered in groups of more than one bar graph.

- **Column** - A column graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted vertically and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped column graphs display bars clustered in groups of more than one column graph.

- **Line** - Line graphs show how data for one data type changes over time.
Management Center Configuration & Management

- **Pie** - A pie graph is a circular statistical graphic, divided into slices to illustrate numerical proportion. In a pie graph, the arc length of each slice (and thus the central angle and area), is proportional to the quantity it represents. The pie chart displays the value name and metric when a user hovers the mouse over a section.

After you click a chart type, the Preview window pane displays the report with the selected type of chart.

If you selected a two-level report in Step 1, be sure to choose bar or column for the chart type. These are the only chart types that represent both levels of data in two-level reports. When a two-level report is selected, the column and bar charts display as stacked columns and stacked bars.

### Step 3: Define the Time Frame

Define the reporting period for the report using any of the methods below:

- Choose one of the standard time periods, such as 30d or 1y. The default time period is 24h.
- Use the arrows and  to select the date or date range.
- From the Quick Pick drop-down, select a type of relative date filter, for example, Before or Since.
- To specify a custom range of dates, choose Custom from the Quick Pick drop-down, enter the beginning and ending date, and click Apply.

### Step 4: Choose Report Columns

A statistical table appears below the chart in the custom report. For example, if User is the metric selected in the Group By field, the table includes statistics for each user.
The default statistics are Requests and Total Bytes. Note that the Preview window only shows two statistical columns, but the full report when generated will show all selected columns.

Step 5: Add Filters

You can narrow down what is displayed in the report by setting up filters. Here are several examples of filters you can
Example 1: If the administrator selects the filter **Site**, the operator **contains**, and enters **facebook** for the value, the report returns only sites that contain the string “facebook.”

Example 2: If the administrator selects the filter **Client IP**, the operator **matches**, and enters the IP address range **10.1.1.0/22**, the report includes all addresses in that network mask.

Example 3: If the administrator selects the filter **Hours of Day**, the operator **in between**, and selects the hours **9 a.m.** and **5 p.m.**, the report includes data only for the time between 9 and 5.

For each filter you want to add to the report, follow the steps below.

1. In the **Filters** section, click **Add Filter**.

2. Select a field.

3. Select the appropriate operator. The available operators change depending on the selected field.
4. Select or enter a value.

Step 6: Save the Custom Report

So that you can run the report in the future, without having to recreate it, you should save it into a report group.
1. In the **Save Report** section, select **Save report for running later**.

2. Enter a **Name** for the report.

3. (Optional) Enter a **Description** up to 1024 characters. In the description mention the report settings such as the type of chart, the time period, filters used, and so forth.

4. Select the **Group** to save the report in. If you haven't created the group yet, you can select the **New Group** option from the **Group** drop-down and define the group name at that time.

5. Click **Save and Run** to save the settings and view the full report.

### Edit Custom Reports

After designing and saving a custom report, you may want to tweak some of the settings.

- For more information about any of these settings, see "Create a Custom Report" on page 475.

### Modify Report Settings

1. Select **Reports > Reporter**.

2. Click the name of the custom report you want to modify; this runs the report.

3. To modify the **Group By** fields and/or **Filters**, click the gear settings icon.
4. To modify the chart type, click the chart icon and select the desired type.

5. The Time Frame can be changed using the time tool bar at the top of the report.

6. To modify the columns:
   a. In the report table below the chart, hover the mouse on the right side of a column heading until you see the triangle, then click.

   b. Select Columns.
   c. Select the columns you want to include in the report.

7. To save the custom report modifications, select Actions > Save.
Delete a Custom Report

1. Select **Reports > Reporter**.
2. Select the check box by each report name you want to delete.

![Custom Reports]

3. Select **Operations > Delete**.

![Operations]

4. Click **Delete** to confirm.

Additional Information

- To rename a custom report, select the check box next to the report name and issue the **Operations > Rename** command.
- To copy a built-in or custom report, run the report and issue the **Actions > Save As** command.

Search for Specific Report Data (Search and Forensic Report)

Management Center enables you to search for specific report data using a simple search or by executing a forensic report.

Use Simple Search

The **Reports > Reporter** page includes a simple search field in the top right-hand corner, as shown below.
1. By default, a search term entered here searches all criteria. If you want to run a search on a specific database, select the menu icon on the search box [ ] . This brings up a more detailed search page that has other search options in a drop-down menu.

2. Select a search type from the menu. The available criteria differs, depending on the selected database.

3. Enter a search term and click the magnifying glass (or press Enter).

4. The search results display in a new tab on the left.

5. Click the search result to view detailed data about that item.
Run Forensic Report

Use the Forensic Report feature to drill down into the database to find specific information based on the source, destination, and verdict properties of one or more requests. The Forensic Report option is located directly beneath the Management Center banner in the New Report menu.

1. Select **Forensic Report** from the **New Report** menu. The system opens the Run Forensic Report window.

![Run Forensic Report Window]

---

2. Select (or enter) the search criteria from the available data or enter a transaction ID.
3. Select a time duration.
4. Click **Run Report**. The system displays the search results in the **Full Log Details** report.

5. Click links in the search result to view detailed data about that item.
Reporter Graph Types and Views

Reporter Enterprise Server 10.1.x is required to access and view Reporter Reports and Dashboards.

Reporter graph types depend on the type of data represented in the report. The available graph types are:

- **Area** - An area graph displays graphically quantitative data. It is based on the line chart. The area between axis and line are commonly emphasized with colors and textures. Commonly used area graphs compare one area with two or more areas.

- **Bar** - A bar graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted horizontally and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped bar graphs display bars clustered in groups of more than one bar graph.

- **Column** - A column graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted vertically and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped column graphs display bars clustered in groups of more than one column graph.

- **Line** - Line graphs show how data for one data type changes over time.

- **Pie** - A pie graph is a circular statistical graphic, divided into slices to illustrate numerical proportion. In a pie graph, the arc length of each slice (and thus the central angle and area), is proportional to the quantity it represents. The pie chart displays the value name and metric when a user hovers the mouse over a section.

Drill down on specific data within a report by selecting a line the column portion in the report, right-click, and selecting from the available options. Drilling down is most helpful when you know what you are looking for. For example, if you are viewing a **Trend of Risky Users** report, you can drill down on the username or risk categories to find the sites that the user is visiting the most. The following is an example of data that can is available when you are drilling down in a report:
Set Time Zone for Reporter Reports

Associate a custom time zone with your user profile. That time zone is then used for all Reporter reports. Each user can set a different time zone without affecting other user’s views.

1. In the web console banner, click and select your username.

2. Select the **Reporter Time Zone** tab.

   - Time Zone: (UTC-07:00) America/Denver

   This time zone setting will affect all Reporter Reports, and Reporter based dashboard widgets on Reporter and Mixed dashboards
3. Select the new time zone.
4. Click **Save**.
5. When you open a Reporter report, verify your settings by opening a Reporter report and hovering over the time zone icon.

![Time Zone Icon](image)

6. (Optional) Once set, you can change the time zone by clicking the time zone icon.

### Determine Why A Reporter Database Does Not Display

If you try to run reports and the database you want is not available in the **Database** drop-down menu (**Reports > Reporter**), click **Status** to display that database’s current status.

![Status Button](image)

1. Click **Reports > Reporter**.
2. Click the **Database**: drop-down. The system displays the available databases.

![Database List](image)

3. If the database you want is not in the menu or you want to see the current status of the Reporter servers and all associated databases, click **Status**.

![Reporter Status](image)

4. If a Reporter server is available (and you have permissions to view it), you can click the plus symbol to display the
associated database(s).

Use the status information to help you determine why the database is not available.

**View Statistics Monitoring Reports**

An organization without an effective monitoring system is susceptible to issues such as unplanned downtime and performance degradation; thus, the ability to monitor network activity is crucial for capacity planning and quick responses to potential problems. By analyzing report data, organizations can plan for scalability and anticipate future requirements.

Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. See Statistics Monitoring Over HTTPS for more information.

Management Center keeps up to 12 months of per hour data and 7 days of per minute data for all devices that have statistics monitoring enabled. To purge this data from Management Center, see Purge Statistics.

As an administrator, it is critical that you be aware of issues, changes, and trends that could arise in your network. In Management Center, you can report on key metrics such as CPU usage, connection counts, bandwidth gains and losses, and other statistics of managed appliances. Statistics Monitoring reports provide you with visibility into network performance. With reports, you can identify trends such as:

- Usage patterns
- Bandwidth savings
- Peak numbers of concurrent users
- Statistics averaged over weeks and months

To ensure that your data analysis is accurate and timely, identify the metrics that are most important to you and run reports regularly.

You can monitor the health of your devices without generating a report. See "Monitor Device Health " on page 58.

**Prerequisites**

You can reports on ProxySG appliances that:

- Run SGOS 6.3.x and later
- Have a Proxy or MACH5 Edition license (Note: this is a requirement for WAN Optimization reports, not Device reports)
- Have the latest trust package installed
- Have statistics collection enabled in device properties (see "Add a Device" on page 447)

You can still manage ProxySG appliances that do not meet these requirements, but their statistics will be unavailable from **Statistics Monitoring**.

**Procedure**

To view Statistics Monitoring reports:
1. Select **Reports > Statistics Monitoring**.
2. Select a report from **Devices** or **WAN Optimization**. See "Reference: Statistics Monitoring Reports in Management Center" on page 502 for descriptions.
3. From a dashboard widget, you can also "Display a Full Report" on page 508.
4. Refine reports to make them more useful:
   - Display data for a specific time period. See “Change the Scope of a Statistics Monitoring Report” on page 507.
   - Add metrics to focus on specific data. See "Modify Options for Statistics Monitoring Reports" on page 505.

**Reference: Statistics Monitoring Reports in Management Center**

The following **Statistics Monitoring** reports are available in Management Center.

### Devices Reports

Device reports show statistics on network traffic seen by a single ProxySG device, ProxySG appliances in a device group, or all ProxySG devices.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Report Format</th>
<th>Field</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Displays the percentage of CPU being used. By default, data shown in this report is an average of CPU usage across all devices.</td>
<td>Line graph</td>
<td>Memory, Users</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>Displays the percentage of memory being used. By default, data shown in this report is an average of memory usage across all devices.</td>
<td>Line graph</td>
<td>CPU, Users</td>
<td></td>
</tr>
<tr>
<td>Current Users</td>
<td>Displays the total number of users that currently have traffic going through the ProxySG appliance. By default, data shown in this report is the number of current users across all devices.</td>
<td>Line graph</td>
<td>CPU, Memory</td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td>Displays the total number of bytes or packets sent or received through ProxySG appliance network ports. Select the device for which you want to view interface information; the data renders as a pie chart, where each segment represents one interface.</td>
<td>Circle graph</td>
<td>Bytes Received, Bytes Sent, Packets Received, Packets Sent</td>
<td></td>
</tr>
<tr>
<td>Interfaces Detail</td>
<td>Displays the bytes sent and received and packets sent and received through ProxySG appliance network ports. The information is presented in a grid; you can sort data by column headers or hide some columns to limit the information displayed.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Trend of Interfaces
Displays the trend of bytes or packets sent or received through ProxySG appliance network ports over the specified period of time.

**Report Format:** Stack graph
- **Field:** Bytes Received, Bytes Sent, Packets Received, Packets Sent

### Devices
Displays a comparison of the traffic through specified ProxySG appliances measured in bytes.

**Report Format:** Circle graph
- **Field:** Bypassed Bytes, Server Bytes, Client Bytes

### Devices Detail
Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain for traffic through ProxySG appliances.

**Report Format:** Table chart

### Intercepted Traffic Savings
Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain for intercepted traffic through different ProxySG appliances.

**Report Format:** Table chart

### Traffic Mix
Displays the distribution of traffic and bandwidth statistics.

**Report Format:** Line graph, circle graph, and table chart

### Traffic Statistics
Displays the effective bandwidth, actual bandwidth, and bandwidth savings for different services.

**Report Format:** Line graph and table chart

---

### WAN Optimization Reports

The **WAN Optimization** reports display statistics for ProxySG appliances with a Proxy or MACH5 Edition license.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Report Format</th>
<th>Field</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Savings (bytes)</td>
<td>Displays bandwidth savings in bytes received from monitored devices.</td>
<td>Line graph</td>
<td></td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Bandwidth Savings (cost)</td>
<td>Displays bandwidth savings expressed in terms of cost.</td>
<td>Line graph</td>
<td></td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Report Format</td>
<td>Field</td>
<td>Overlays</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Bandwidth Savings</td>
<td>Displays bandwidth savings expressed as a percentage.</td>
<td>Line graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage,</td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>(percent)</td>
<td></td>
<td></td>
<td>Bandwidth Gain</td>
<td></td>
</tr>
<tr>
<td>Bandwidth Gain</td>
<td>Displays bandwidth gains (including negative gains) for a specified interval.</td>
<td>Line graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage,</td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Effective Bandwidth</td>
<td>Compares effective and actual bandwidth, measured in bytes.</td>
<td>Line graph</td>
<td>Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes,</td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Services</td>
<td>Compares specified services.</td>
<td>Circle graph</td>
<td>New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>Services Detail</td>
<td>Displays bandwidth savings for different services in bytes, actual bandwidth,</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>effective bandwidth, and the bandwidth gain.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trend of Services</td>
<td>Displays the trend of the specified service over a period of time.</td>
<td>Stack graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>Proxies</td>
<td>Breaks down the total number of server bytes through different proxies.</td>
<td>Circle graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Intercepted Connections, Peak Intercepted Connection</td>
<td></td>
</tr>
<tr>
<td>Proxies Detail</td>
<td>Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth,</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and the bandwidth gain.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Report Format</td>
<td>Field</td>
<td>Overlays</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Trend of Proxies</td>
<td>Displays the trend of proxies versus the Server Bytes by default aggregated across all devices.</td>
<td>Stack graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>ADN History</td>
<td>Displays the number of optimized and unoptimized bytes for different peer IP addresses.</td>
<td>Line graph and table chart</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Modify Options for Statistics Monitoring Reports**

By default, a **Statistics Monitoring** report displays data for the last seven days for all ProxySG devices but you can customize the report by changing the start date and interval, choosing which devices or device group to report on, and adding overlays of additional statistics.

To have the reports on the **Statistics Monitoring** dashboard to automatically refresh the displayed reports, select **Options** and click the **Auto-refresh** box to select it. The default is set to 5 minutes, though you can set it to any desired interval of minutes (up to 59) or hours (up to 24).

To customize the reports:

1. Select **Reports > Statistics Monitoring**.
2. Select a report from **Devices** or **WAN Optimization**. See "Reference: Statistics Monitoring Reports in Management Center" on page 502 for descriptions.
3. After you select the report, the report opens in a new tab.
4. To open the Filters dialog, click the gear settings icon within the report.
5. Filter the report data using the options described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>The date and time from which report data begins. The interval you select is based on the start date. For example, if you specify the 13th of the month for the start date and an interval of 7 days, the report shows data from the 13th through the 19th. Specify the date in MM/DD/YY format, or click the calendar 📗 to pick a date.</td>
</tr>
<tr>
<td>Interval</td>
<td>The number of hours or days after the start date for which the report shows data. <strong>Note</strong>: The start date and interval in conjunction might result in future days on the report. For example, if you want data from only the last four days, selecting a start date from four days ago results in three future days on the report. To avoid confusion, you can select a start date that is earlier than required so that future days do not display. Select the interval from the drop-down list. Intervals can include 60 minutes, 24 hours, 7 days or 31 days. If you select 60 minutes, the time field is available. Select a time from the drop-down list. Times are available in one-hour increments.</td>
</tr>
<tr>
<td>Filter</td>
<td>Select a filter from the drop-down list. If you select <strong>Device</strong> or <strong>Device Groups</strong>, use the ✏️ to select multiple ProxySG devices or a single device group.</td>
</tr>
<tr>
<td>Graph</td>
<td>Changes how the data is displayed. You can graph the data as the mean average for all devices (single data line) or as individual metrics for each device (one line per device). Hover the mouse cursor over a graph line to get additional information.</td>
</tr>
</tbody>
</table>

(This option is not available for all reports)
6. Click **Save**.

The web console displays the Statistics Monitoring report with the options you selected. The name and number of devices will display next to **Device Filter** at the top of the report. If a filter isn't defined, the **Device Filter** will say **All Devices**.

**Change the Scope of a Statistics Monitoring Report**

By default, **Statistics Monitoring** reports and report widgets display data for the last seven days. For example, if you select a report on April 14th, the report opens with **Last 7 Days** selected for the date range at the bottom left corner. The start date or time of the selected rate range is displayed between **<>**. The bottom right of the reports indicates the specific date range of the data shown in the report, such as **Displaying days for 04/14/15 - 4/21/15**.

To view data from a broader or narrower time frame, select an interval from the **Date Range** drop-down list. The report data updates immediately to reflect your selection.

Refer to the following table to understand how the date range affects the report data; assume that the current date and time is Tuesday, October 15th at 09:05.

<table>
<thead>
<tr>
<th>Selected Date Range</th>
<th>Description</th>
<th>Report shows data for this period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Hour</td>
<td>The current hour.</td>
<td>09:00 - 10:00</td>
</tr>
<tr>
<td>Today</td>
<td>The current day.</td>
<td>October 15th</td>
</tr>
<tr>
<td>Current Week</td>
<td>The current calendar week, starting on Monday.</td>
<td>October 14th - October 20th</td>
</tr>
<tr>
<td>Current Month</td>
<td>The current calendar month, starting on the 1st.</td>
<td>October 1st - 31st</td>
</tr>
<tr>
<td>Yesterday</td>
<td>The previous day.</td>
<td>October 14th</td>
</tr>
<tr>
<td>Previous Week</td>
<td>The previous calendar week, starting on Monday.</td>
<td>October 7th - 13th</td>
</tr>
<tr>
<td>Previous Month</td>
<td>The previous calendar month, starting on the 1st.</td>
<td>September 1st - 30th</td>
</tr>
</tbody>
</table>
To view data from different points in time, use the date range and < > in conjunction. Using < > causes the report to go back and forward, respectively, at the interval specified in Date Range. For example, if the date range is Last 7 Days and the report shows data from October 8th to October 15th, clicking < causes the report to display data from October 1st to October 8th. If you change the date range to Today and click <, the report displays data from the previous day. You can use > to return to more recent dates and times.

For more information about report dates, see Date Filters.

It is possible to display future days in reports if you use >. If a report abruptly shows no data while you are changing the dates or times, check the dates/times that have no data and exclude them from your analysis (or change the date range again).

**Filter on Devices or Device Groups**

To view a report of data from multiple devices or from a particular device group:

1. Display the desired Statistics Monitoring report.
2. Click the Options button.
3. Change the Start Date and Interval, if desired.
4. Use the Filter drop-down list to select individual devices or specify a device group.
5. To choose from the available devices or device groups, click .
   - Device: Select one or more devices and click OK.
   - Device Group: Select one group and click OK.
6. Click Save.

After you save your changes, the report data updates immediately. The Device Filter displays the names (or IP addresses) of the devices filtered in the reports. See "Modify Options for Statistics Monitoring Reports" on page 505.

**Zoom In and Out on Reports**

In reports that display changes over time, it is useful to see more detail on a specific data point. For example, if you are looking at a report with Current Week as the date range, zooming in on a specific day displays the report for the day at hourly intervals. Zooming in on a specific hour displays the report for the hour at five-minute intervals.

1. In the report, hover over the data point you want to see in greater detail. The data point expands slightly.
2. Click the data point and select Zoom In. The report displays the data at the new level.
3. To return to the previous level, click any data point and select Zoom Out.

**Statistics Monitoring Graph Types**

Statistics Monitoring graph types depend on the type of data represented in the report. Some reports consist of a combination of these formats.
- **Line graphs** show how data for one data type changes over time. You can hover over the line graphs for extra tool tips that can include data such as the date, percentage, total number, etc.

- **Stack graphs** show changes in a set of data, for both for the individual data types and the total of the individual items. Each color in a stack graph represents one type of data changing over time.

- **Circle graphs** show the proportions of specific data with a set of data.

  **Example:** The Effective Bandwidth graph in the Traffic Mix report shows the proportion (in percentage) of effective bandwidth for different traffic types. Hover over a segment in the graph to display the number of bytes for each traffic type.

- **Table charts** arrange data in rows to compare data from multiple sources.

  **Example:** The Devices Detail report widget shows the actual bandwidth versus effective bandwidth for all devices in the system.

### Display a Full Report

Display a full report from a statistics monitoring widget.

2. Do one of the following:
   - If the report you want has a widget on the dashboard, expand the widget if necessary and then click **View Full Report** at the bottom of it.
   - If the report does not have a widget on the dashboard, click **Report > Statistics Monitoring**. Available reports are displayed in two lists: **Devices** and **WAN Optimization**.
3. Select the report you want to view. The report opens in a new tab.

   **Tip:** If you leave a report open for an extended period of time, you can refresh it to ensure that no stale data is displayed.

   To refresh a report, click 🔄 at the bottom of the report.

### Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about different graph types.</td>
<td>&quot;Statistics Monitoring Graph Types&quot; on page 509</td>
</tr>
<tr>
<td>See the report for different dates or times.</td>
<td>&quot;Change the Scope of a Statistics Monitoring Report&quot; on page 507</td>
</tr>
</tbody>
</table>
What do you want to accomplish? | Refer to this topic
---|---
Change the metrics and other data that display on the report. | "Modify Options for Statistics Monitoring Reports" on page 505
View descriptions of the Statistics Monitoring reports. | "Reference: Statistics Monitoring Reports in Management Center" on the facing page

View Statistics Monitoring Reports

An organization without an effective monitoring system is susceptible to issues such as unplanned downtime and performance degradation; thus, the ability to monitor network activity is crucial for capacity planning and quick responses to potential problems. By analyzing report data, organizations can plan for scalability and anticipate future requirements.

Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. See Statistics Monitoring Over HTTPS for more information.

Management Center keeps up to 12 months of per hour data and 7 days of per minute data for all devices that have statistics monitoring enabled. To purge this data from Management Center, see Purge Statistics.

As an administrator, it is critical that you be aware of issues, changes, and trends that could arise in your network. In Management Center, you can report on key metrics such as CPU usage, connection counts, bandwidth gains and losses, and other statistics of managed appliances. Statistics Monitoring reports provide you with visibility into network performance. With reports, you can identify trends such as:

- Usage patterns
- Bandwidth savings
- Peak numbers of concurrent users
- Statistics averaged over weeks and months

To ensure that your data analysis is accurate and timely, identify the metrics that are most important to you and run reports regularly.

You can monitor the health of your devices without generating a report. See "Monitor Device Health" on page 58.

Prerequisites

You can reports on ProxySG appliances that:

- Run SGOS 6.3.x and later
- Have a Proxy or MACH5 Edition license (Note: this is a requirement for WAN Optimization reports, not Device reports)
- Have the latest trust package installed
- Have statistics collection enabled in device properties (see "Add a Device" on page 447)

You can still manage ProxySG appliances that do not meet these requirements, but their statistics will be unavailable from Statistics Monitoring.

Procedure

To view Statistics Monitoring reports:
1. Select **Reports > Statistics Monitoring**.
2. Select a report from **Devices** or **WAN Optimization**. See "Reference: Statistics Monitoring Reports in Management Center" below for descriptions.
3. From a dashboard widget, you can also "Display a Full Report" on page 508.
4. Refine reports to make them more useful:
   - Add metrics to focus on specific data. See "Modify Options for Statistics Monitoring Reports" on page 505.

**Reference: Statistics Monitoring Reports in Management Center**

The following **Statistics Monitoring** reports are available in Management Center.

### Devices Reports

Device reports show statistics on network traffic seen by a single ProxySG device, ProxySG appliances in a device group, or all ProxySG devices.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Report Format</th>
<th>Field</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Displays the percentage of CPU being used. By default, data shown in this report is an average of CPU usage across all devices.</td>
<td>Line graph</td>
<td>Memory, Users</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>Displays the percentage of memory being used. By default, data shown in this report is an average of memory usage across all devices.</td>
<td>Line graph</td>
<td>CPU, Users</td>
<td></td>
</tr>
<tr>
<td>Current Users</td>
<td>Displays the total number of users that currently have traffic going through the ProxySG appliance. By default, data shown in this report is the number of current users across all devices.</td>
<td>Line graph</td>
<td>CPU, Memory</td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td>Displays the total number of bytes or packets sent or received through ProxySG appliance network ports. Select the device for which you want to view interface information; the data renders as a pie chart, where each segment represents one interface.</td>
<td>Circle graph</td>
<td>Bytes Received, Bytes Sent, Packets Received, Packets Sent</td>
<td></td>
</tr>
<tr>
<td>Interfaces Detail</td>
<td>Displays the bytes sent and received and packets sent and received through ProxySG appliance network ports. The information is presented in a grid; you can sort data by column headers or hide some columns to limit the information displayed.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Report Format</td>
<td>Field.</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Trend of Interfaces</td>
<td>Displays the trend of bytes or packets sent or received through ProxySG appliance network ports over the specified period of time.</td>
<td>Stack graph</td>
<td>BytesReceived, BytesSent, PacketsReceived, PacketsSent</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>Displays a comparison of the traffic through specified ProxySG appliances measured in bytes.</td>
<td>Circle graph</td>
<td>BypassedBytes, ServerBytes, ClientBytes</td>
<td></td>
</tr>
<tr>
<td>Devices Detail</td>
<td>Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain for traffic through ProxySG appliances.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intercepted Traffic Savings</td>
<td>Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain for intercepted traffic through different ProxySG appliances.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Mix</td>
<td>Displays the distribution of traffic and bandwidth statistics.</td>
<td>Line graph, circle graph, and table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Statistics</td>
<td>Displays the effective bandwidth, actual bandwidth, and bandwidth savings for different services.</td>
<td>Line graph and table chart</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**WAN Optimization Reports**

The **WAN Optimization** reports display statistics for ProxySG appliances with a Proxy or MACH5 Edition license.
<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Report Format</th>
<th>Field</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Savings (bytes)</td>
<td>Displays bandwidth savings in bytes received from monitored devices.</td>
<td>Line graph</td>
<td></td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Bandwidth Savings (cost)</td>
<td>Displays bandwidth savings expressed in terms of cost.</td>
<td>Line graph</td>
<td></td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Bandwidth Savings (percent)</td>
<td>Displays bandwidth savings expressed as a percentage.</td>
<td>Line graph</td>
<td></td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Bandwidth Gain</td>
<td>Displays bandwidth gains (including negative gains) for a specified interval.</td>
<td>Line graph</td>
<td></td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Effective Bandwidth</td>
<td>Compares effective and actual bandwidth, measured in bytes.</td>
<td>Line graph</td>
<td></td>
<td>CPU, Memory, Users</td>
</tr>
<tr>
<td>Services</td>
<td>Compares specified services.</td>
<td>Circle graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>Services Detail</td>
<td>Displays bandwidth savings for different services in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trend of Services</td>
<td>Displays the trend of the specified service over a period of time.</td>
<td>Stack graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>Proxies</td>
<td>Breaks down the total number of server bytes through different proxies.</td>
<td>Circle graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connection</td>
<td></td>
</tr>
<tr>
<td>Proxies Detail</td>
<td>Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Report Center Configuration & Management

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Report Format</th>
<th>Field</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend of Proxies</td>
<td>Displays the trend of proxies versus the Server Bytes by default aggregated across all devices.</td>
<td>Stack graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>ADN History</td>
<td>Displays the number of optimized and unoptimized bytes for different peer IP addresses.</td>
<td>Line graph and table chart</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Modify Options for Statistics Monitoring Reports

By default, a Statistics Monitoring report displays data for the last seven days for all ProxySG devices but you can customize the report by changing the start date and interval, choosing which devices or device group to report on, and adding overlays of additional statistics.

To have the reports on the Statistics Monitoring dashboard to automatically refresh the displayed reports, select **Options** and click the **Auto-refresh** box to select it. The default is set to 5 minutes, though you can set it to any desired interval of minutes (up to 59) or hours (up to 24).

To customize the reports:

1. Select **Reports > Statistics Monitoring**.
2. Select a report from **Devices** or **WAN Optimization**. See "Reference: Statistics Monitoring Reports in Management Center" on page 502 for descriptions.
3. After you select the report, the report opens in a new tab.
4. To open the Filters dialog, click the gear settings icon within the report.
5. Filter the report data using the options described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>The date and time from which report data begins. The interval you select is based on the start date. For example, if you specify the 13th of the month for the start date and an interval of 7 days, the report shows data from the 13th through the 19th. Specify the date in MM/DD/YY format, or click the calendar 📅 to pick a date.</td>
</tr>
<tr>
<td>Interval</td>
<td>The number of hours or days after the start date for which the report shows data. <strong>Note:</strong> The start date and interval in conjunction might result in future days on the report. For example, if you want data from only the last four days, selecting a start date from four days ago results in three future days on the report. To avoid confusion, you can select a start date that is earlier than required so that future days do not display. Select the interval from the drop-down list. Intervals can include 60 minutes, 24 hours, 7 days or 31 days. If you select 60 minutes, the time field is available. Select a time from the drop-down list. Times are available in one-hour increments.</td>
</tr>
<tr>
<td>Filter</td>
<td>Select a filter from the drop-down list. If you select <strong>Device</strong> or <strong>Device Groups</strong>, use the 🔄 to select multiple ProxySG devices or a single device group.</td>
</tr>
<tr>
<td>Graph (This option is not available for all reports)</td>
<td>Changes how the data is displayed. You can graph the data as the mean average for all devices (single data line) or as individual metrics for each device (one line per device). Hover the mouse cursor over a graph line to get additional information.</td>
</tr>
</tbody>
</table>
6. Click **Save**.

The web console displays the Statistics Monitoring report with the options you selected. The name and number of devices will display next to **Device Filter** at the top of the report. If a filter isn’t defined, the **Device Filter** will say **All Devices**.

**Change the Scope of a Statistics Monitoring Report**

By default, **Statistics Monitoring** reports and report widgets display data for the last seven days. For example, if you select a report on April 14th, the report opens with **Last 7 Days** selected for the date range at the bottom left corner. The start date or time of the selected rate range is displayed between <>. The bottom right of the reports indicates the specific date range of the data shown in the report, such as **Displaying days for 04/14/15 - 4/21/15**.

To view data from a broader or narrower time frame, select an interval from the **Date Range** drop-down list. The report data updates immediately to reflect your selection.

Refer to the following table to understand how the date range affects the report data; assume that the current date and time is Tuesday, October 15th at 09:05.

<table>
<thead>
<tr>
<th>Selected Date Range</th>
<th>Description</th>
<th>Report shows data for this period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Hour</td>
<td>The current hour.</td>
<td>09:00 - 10:00</td>
</tr>
<tr>
<td>Today</td>
<td>The current day.</td>
<td>October 15th</td>
</tr>
<tr>
<td>Current Week</td>
<td>The current calendar week, starting on Monday.</td>
<td>October 14th - October 20th</td>
</tr>
<tr>
<td>Current Month</td>
<td>The current calendar month, starting on the 1st.</td>
<td>October 1st - 31st</td>
</tr>
<tr>
<td>Yesterday</td>
<td>The previous day.</td>
<td>October 14th</td>
</tr>
<tr>
<td>Previous Week</td>
<td>The previous calendar week, starting on Monday.</td>
<td>October 7th - 13th</td>
</tr>
<tr>
<td>Previous Month</td>
<td>The previous calendar month, starting on the 1st.</td>
<td>September 1st - 30th</td>
</tr>
</tbody>
</table>
To view data from different points in time, use the date range and < > in conjunction. Using < > causes the report to go back and forward, respectively, at the interval specified in Date Range. For example, if the date range is Last 7 Days and the report shows data from October 8th to October 15th, clicking < causes the report to display data from October 1st to October 8th. If you change the date range to Today and click <, the report displays data from the previous day. You can use > to return to more recent dates and times.

For more information about report dates, see Date Filters.

It is possible to display future days in reports if you use >. If a report abruptly shows no data while you are changing the dates or times, check the dates/times that have no data and exclude them from your analysis (or change the date range again).

Filter on Devices or Device Groups

To view a report of data from multiple devices or from a particular device group:

1. Display the desired Statistics Monitoring report.
2. Click the Options button.
3. Change the Start Date and Interval, if desired.
4. Use the Filter drop-down list to select individual devices or specify a device group.
5. To choose from the available devices or device groups, click .
   - Device: Select one or more devices and click OK.
   - Device Group: Select one group and click OK.
6. Click Save.

After you save your changes, the report data updates immediately. The Device Filter displays the names (or IP addresses) of the devices filtered in the reports. See "Modify Options for Statistics Monitoring Reports" on page 505.

Zoom In and Out on Reports

In reports that display changes over time, it is useful to see more detail on a specific data point. For example, if you are looking at a report with Current Week as the date range, zooming in on a specific day displays the report for the day at hourly intervals. Zooming in on a specific hour displays the report for the hour at five-minute intervals.

1. In the report, hover over the data point you want to see in greater detail. The data point expands slightly.
2. Click the data point and select Zoom In. The report displays the data at the new level.
3. To return to the previous level, click any data point and select Zoom Out.

Display a Full Report

Display a full report from a statistics monitoring widget.

2. Do one of the following:
   - If the report you want has a widget on the dashboard, expand the widget if necessary and then click **View Full Report** at the bottom of it.
   - If the report does not have a widget on the dashboard, click **Report > Statistics Monitoring**. Available reports are displayed in two lists: **Devices** and **WAN Optimization**.

3. Select the report you want to view. The report opens in a new tab.

---

If you leave a report open for an extended period of time, you can refresh it to ensure that no stale data is displayed.

To refresh a report, click ⌁ at the bottom of the report.

---

### Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about different graph types.</td>
<td>&quot;Statistics Monitoring Graph Types&quot; below</td>
</tr>
<tr>
<td>See the report for different dates or times.</td>
<td>&quot;Change the Scope of a Statistics Monitoring Report&quot; on page 507</td>
</tr>
<tr>
<td>Change the metrics and other data that display on the report.</td>
<td>&quot;Modify Options for Statistics Monitoring Reports&quot; on page 505</td>
</tr>
</tbody>
</table>

---

### Statistics Monitoring Graph Types

Statistics Monitoring graph types depend on the type of data represented in the report. Some reports consist of a combination of these formats.

- **Line graphs** show how data for one data type changes over time. You can hover over the line graphs for extra tool tips that can include data such as the date, percentage, total number, etc.

- **Stack graphs** show changes in a set of data, for both for the individual data types and the total of the individual items. Each color in a stack graph represents one type of data changing over time.

- **Circle graphs** show the proportions of specific data with a set of data.

**Example:** The Effective Bandwidth graph in the Traffic Mix report shows the proportion (in percentage) of effective bandwidth for different traffic types. Hover over a segment in the graph to display the number of bytes for each traffic type.
Table charts arrange data in rows to compare data from multiple sources.

Example: The Devices Detail report widget shows the actual bandwidth versus effective bandwidth for all devices in the system.

Work with Reports

Reporter

Reporter Enterprise Server 10.1.x is required to access and view Reporter Reports and Dashboards.

See the following for information about working with Reporter reports:

- "View a Reporter Report" on page 453
- "Customize Reporter Report Options" on page 459
- "Reporter Graph Types and Views" on page 489
- Date Filters
- "Search for Specific Report Data (Search and Forensic Report)" on page 485
- "Set Time Zone for Reporter Reports" on page 490

Statistics Monitoring

See the following for information about working with Statistics Monitoring reports:

- "View Statistics Monitoring Reports" on page 501
- "Change the Scope of a Statistics Monitoring Report" on page 507
- "Statistics Monitoring Graph Types" on the previous page
- "Modify Options for Statistics Monitoring Reports" on page 505
- Date Filters
**Customize Report Widgets**

Widgets on the Dashboard and Reports tabs can be customized based on the type of data that you want to view.

**Collapse Report Widgets**

You can collapse report widgets if you have limited room on the dashboard, or if you prefer not to see all of the widgets expanded at once.

- To expand a report widget, click the down arrow in the widget title bar.
- To collapse a collapsed widget, click the up arrow in the widget title bar.

**Move Report Widgets**

You can move report widgets. Because widgets align themselves automatically when you move them, you can put them in groups.

1. Hover over a widget title bar. The pointer changes to a multi-directional arrow.
2. Drag the widget to its new location.

**Remove Report Widgets**

To remove a report widget, click the X on the top right corner of the widget.

To add the widget to the dashboard again, click **Add Report** and select the widget from the list.

**Add Reports**

The amount of report widgets that you can add and customize is wholly dependent upon whether you have integrated Reporter 10.x into your network.

Reporter Enterprise Server 10.1.x is required to access and view Reporter Reports and Dashboards.

**Close a Report**

When you no longer need to view a report, close it using one of the following methods.

**Close the Active Report**

Click **Close** to close the report.

Alternatively, close the report by clicking the X on the tab at the bottom of the screen.

**Close a Report on Another Widget**

If you have multiple reports open, you can close a report other than the active one by clicking the X on the appropriate tab at the bottom of the screen.

**Modify Display of Table Data**

You can modify the view of table data as described below. Each table supports specific actions; all actions may not be available.
Show Available Actions

Click the arrow to the right of the column headings to show the available actions.

Change Columns

Hover over Columns to change the displayed columns.

Group Table Data

Select Group by this field to group the table data in accordance with that column heading.
The data is then grouped. In the example below, the Type column was grouped.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Version</th>
<th>Last Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type: WAF Application</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Security</td>
<td>WAF Application</td>
<td>1.0</td>
<td>7/14/16 9:</td>
<td></td>
</tr>
<tr>
<td>WAF App</td>
<td>WAF Application</td>
<td>1.1</td>
<td>12/7/16 9:</td>
<td></td>
</tr>
<tr>
<td><strong>Type: Universal VPM Policy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UP_Test</td>
<td>Universal VPM Policy</td>
<td>1.1</td>
<td>10/19/16 5</td>
<td></td>
</tr>
<tr>
<td>UP Test2</td>
<td>Universal VPM Policy</td>
<td>1.0</td>
<td>11/2/16 9:</td>
<td></td>
</tr>
<tr>
<td><strong>Type: VPM</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test:VPM</td>
<td>VPM</td>
<td>1.1</td>
<td>8/18/16 4:</td>
<td></td>
</tr>
<tr>
<td>VPM1</td>
<td>VPM</td>
<td>1.5</td>
<td>12/5/16 7:</td>
<td></td>
</tr>
<tr>
<td><strong>Type: Tenant Determination File</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Landlord Policy</td>
<td>Tenant Determin...</td>
<td>1.0</td>
<td>7/5/16 7:2</td>
<td></td>
</tr>
<tr>
<td><strong>Type: SSLV Lists</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSLV Policy</td>
<td>SSLV Lists</td>
<td>policy for SSLV lists</td>
<td>1.0</td>
<td>12/9/16 7:</td>
</tr>
<tr>
<td>KeSSL Policy</td>
<td>SSLV Lists</td>
<td></td>
<td>1.1</td>
<td>12/7/16 11</td>
</tr>
</tbody>
</table>

Deselect *Show in groups* on the dropdown menu to put data back into a plain list.
View Raw Report Data

The Source Data Viewer displays a report in raw data format, which breaks down specific data types that Management Center collects from devices. If the interaction of data in a standard report seems wrong or misleading, you can view the data in isolation from other metrics.

2. Click Source Data Viewer. The Source Data Viewer opens on a new tab.
3. In the tree on the left, browse to the data you want to display and select it. The report opens on a new tab on the right.

Reports: Save as PDF

Most Management Center reports can now be saved and downloaded to your local client as a PDF file.

1. To download the current report as a PDF, click Download PDF. The web console displays the Download dialog.

![Download Dialog]

2. Select the orientation, Portrait or Landscape.
3. Optional—Change the report title or file name. Click Download. Click Close to cancel.

Some reports do not have the PDF option. These include detail reports or reports that include source data. For example:

- Interfaces Detail
- Devices Detail
- Intercepted Traffic Savings
- Traffic Mix
- Traffic Statistics
- Services Detail
- Proxies Detail
- ADN History
Manage Dashboards

Dashboards allow you to quickly view important device data. This data is represented by widgets. Widgets represent data from managed devices. Dashboards are highly customizable and can help you quickly view the information you deem important.

To monitor devices from a single screen, add dashboards and add widgets to those dashboards using the options on the **Dashboards > Manage Dashboards** page.

<table>
<thead>
<tr>
<th>Order ↑</th>
<th>Name</th>
<th>Type</th>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3, etc.</td>
<td>The name of the dashboard as it appears on the Dashboard tab.</td>
<td>Reporter - displays only Reporter widgets on the dashboard.</td>
<td>Each dashboard can display multiple widgets.</td>
<td>The description helps to differentiate the dashboard type, and the widgets within the dashboard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WAF Reporter - displays only WAF widgets on the dashboard</td>
<td>For a quick reference of what is displayed on each dashboard, view the widget count for each dashboard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mixed - Can display data from all widgets on the dashboard.</td>
<td>Statistics Monitoring - displays only Statistics Monitoring widgets on the dashboard.</td>
<td></td>
</tr>
</tbody>
</table>

Notes

- Reporter Enterprise Server 10.1.x is required to access and view Reporter Reports and Dashboards.
- Dashboards are dependent on the reports that you can generate for each managed device. To generate advanced reports and view advanced real-time data within dashboards, see Add Reporter as a Managed Device.

Add a Dashboard

To accommodate your screen size or personal preference, you can change the number of dashboards that display, as well as define the layout of the dashboards. You must also define the dashboard type. Layouts arrange widgets in one to four columns of equal width, with the columns expanding to fit the width of the screen. When you select a layout, your change persists (beyond the current session) until you change the layout again.

Although you can add multiple dashboards, remember that dashboards display data from databases that may not be the only database available. For example, a Reporter Enterprise Server can provide data from multiple databases. When adding Reporter widgets to dashboards, you can choose from the available databases.
1. From **Dashboards > Manage Dashboards**, click **Add Dashboard**. An asterisk denotes fields that are mandatory.

2. Enter a descriptive **Dashboard Name** and **Description**.

3. Choose a **Type**:
   - Mixed - A dashboard that displays both ProxySG appliance and Reporter widgets
   - Reporter - A dashboard that displays Reporter widgets
     If you select Reporter as the dashboard Type, from the **Template** drop-down list, select from the following templates to pre-populate widgets:
     - Web Application Usage
     - Threat Detection
     - Content Filtering
   - WAF Reporter - A dashboard that displays Reporter Web Application Firewall (WAF) widgets.
     If you select **Reporter WAF** as the dashboard Type, select **Web Application Firewall** from the **Template** drop-down list.
   - Statistics Monitoring - A dashboard that displays ProxySG appliance widgets.

4. Select the auto-refresh rate. Specifies the amount of elapsed time before widget data is refreshed. The default refresh rate is 5 minutes. This time is customizable from 1 to 59 minutes or 1 to 24 hours.

Select the Layout for the dashboard.

5. Click **Save**. The saved dashboard is displayed in the **Dashboard** drop-down with the name that you gave it.

   **After you have created a dashboard, you cannot edit the type.**

---

**Reorder Dashboard List**

When you add a new dashboard, the most recently added dashboard is appended to the end of the list. For example if you have three dashboards and add one, the new dashboard becomes the fourth dashboard on the list and will appear to the right of the previously added dashboards. To change the order dashboards are displayed:

1. From **Dashboards > Manage Dashboards**, select the dashboard you want to move.
2. Click **Move Up** or **Move Down** to change the order.

**Duplicate a Dashboard**

To use a dashboard as a template for a dashboard that you may want to clone (and perhaps edit later), you can duplicate a dashboard that already exists. You are unable to change the type of dashboard when you duplicate.

1. From **Dashboards > Manage Dashboards**, click **Duplicate**.
2. From the Duplicate Dashboard dialog, give the dashboard a unique name.
3. Click **Duplicate**. The duplicated dashboard is displayed under **Manage Dashboards**.
Dashboards and Widgets

A dashboard provides a simplified view of data in widgets. A widget is a graphical representation of information, designed to provide a quick overview of statistics or other important information. The variety of widgets available to add to dashboards is dependent upon dashboard Type. See "Manage Dashboards" on page 515.

The web console displays the Home dashboard after users log into the web console. The dashboard displays Device Health and Top Problem Devices widgets by default, but you can add and remove widgets to any dashboard.

When you open or view the Statistics Monitoring dashboard it does not display filtered data from the last session. Each new session opens with no filters applied.

Add a Widget to the Current Dashboard

1. Select the Dashboards tab.
2. Click Add Widgets.

The available widgets are controlled by the report permissions associated with a user's role. Users cannot add widgets for restricted fields.

3. (Optional) From the report groups in the left pane, select the group that contains the report widget you want to add: Bandwidth Usage, Devices, Health, Security, User Behavior, WAN Optimization, Web Applications. The right pane updates with the list of report widgets for the selected report type.
4. Select the report widget you want to add.
5. For Reporter widgets, select the Role, Database, and the Layout.
6. Click Add Widget Now.
7. Repeat steps 3 to 6 to add more widgets, and then click Close.
Add the Bookmarked Devices Widget

The Home dashboard displays the Device Health and the Top Problem Devices widgets by default after you log in. To add a widget specifically to view real-time data for favorite devices, add the **Bookmarked Devices** widget to a dashboard.

1. From the Home dashboard, select **Add Widgets**. The web console displays the Add Widgets wizard.
2. Scroll to **Health** and select **Bookmarked Devices**.

3. Select **Add Widget Now**. Click **Close**. The dashboard displays an empty widget.
4. Select **Add Devices**. Give the widget a name and select the devices that you want to monitor in the dashboard.

5. Select the devices that you want to “bookmark” as your favorite devices and click **OK**. The new widget displays the
selected devices.

![Bookmarked Devices](image)

**Edit or Duplicate Dashboards**

Management Center displays the following default dashboards after users "Log into the Web Console" on page 36.

**Home**

The home dashboard displays when you log into the web console by default. Default widgets displayed are the Device Health and Top Problem Devices widgets.

The home dashboard displays Device Health and Top Problem Devices widgets by default, but you can add and remove widgets based on:

- The type of data that you want to monitor (such as statistics)
- Reporter server integration

1. Select the **Dashboards** tab.
2. Click **Add Widgets**.

**Statistics Monitoring Dashboard**

The web console displays the Statistics Dashboard when you select **Dashboards > Statistics Monitoring**. It displays widgets that provide a simplified view of the statistics monitoring data in a full report.

To customize the layout and widgets of your Statistics Dashboard, see "Change the Dashboard Layout or Refresh Rate" below.

**Change the Dashboard Layout or Refresh Rate**

To accommodate your screen size or personal preference, you can change the layout of the main **Dashboard** tab and define the dashboard type and refresh rate. Layouts arrange widgets in one to four columns of equal width, with the columns expanding to fit the width of the screen.

Reporter Enterprise Server 10.1.x is required to access and view Reporter Reports and Dashboards.

When you select a layout, your change is saved beyond the current session until you change the layout again.

1. Select the **Dashboard** tab. To customize the layout and type, click **Options**. The web console displays the Layout Options dialog. You can change the following:
Management Center Configuration & Management

- Dashboard name
- Description
- Dashboard Type
  - Mixed - A dashboard that displays both ProxySG appliance and Reporter widgets
  - Reporter - A dashboard that displays Reporter widgets
  - Statistics Monitoring - A dashboard that displays ProxySG appliance widgets
- Auto-refresh rate. Specifies the amount of elapsed time before widget data is refreshed. The default refresh rate is 5 minutes. This time is customizable from 1 to 59 minutes or 1 to 24 hours.
- Layout

2. Click **Save**.

After you add a dashboard, you cannot change the dashboard type.
Administrate Management Center

- "Configure General System Settings" below
- "Upgrade/Downgrade System Images" on page 544
- "Back Up the Management Center Configuration" on page 546
- "Encrypt Sensitive System Data" on page 548
- "Restore a Management Center Backup Configuration" on page 549
- "Configure Management Center Failover" on page 550

Configure General System Settings

Configure Management Center general settings about bandwidth cost, the number of backup slots for Management Center backups and the maximum number of policy and script revisions to store. You can also create a password reset email and configure settings to apply to Management Center users.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

1. Select Administration > Settings. An asterisk denotes fields that are mandatory.
2. From System Settings, select General on the left.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Cost per GB*</td>
<td></td>
</tr>
<tr>
<td>See &quot;Set Bandwidth Cost for Reports&quot; on page 523</td>
<td></td>
</tr>
<tr>
<td>Device Polling Interval*</td>
<td></td>
</tr>
<tr>
<td>See &quot;Set the Device Polling Interval&quot; on page 523</td>
<td></td>
</tr>
<tr>
<td>Number of backup slots*</td>
<td></td>
</tr>
<tr>
<td>&quot;Set the Number of Backup Slots&quot; on page 523</td>
<td></td>
</tr>
<tr>
<td>Maximum number of policy revisions to store*</td>
<td></td>
</tr>
<tr>
<td>&quot;Set the Maximum Number of Policy Versions to Store in Management Center&quot; on page 321</td>
<td></td>
</tr>
<tr>
<td>Inactivity timeout (minutes)*</td>
<td></td>
</tr>
<tr>
<td>Specifies the number of minutes before an inactive user is logged out. Users are warned 30 seconds before they are logged out.</td>
<td></td>
</tr>
</tbody>
</table>
### Setting Summary

<table>
<thead>
<tr>
<th>Setting</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inactivity timeout exclusions</strong></td>
<td>The list of usernames that should be excluded from the Inactivity timeout setting.</td>
</tr>
<tr>
<td><strong>Maximum number of script revisions to store</strong></td>
<td>“Set the Maximum Number of Script Revisions to Store in Management Center” on page 174</td>
</tr>
<tr>
<td><strong>Is Reset Password enabled?</strong></td>
<td>false</td>
</tr>
<tr>
<td><strong>Reset Password Email Subject</strong></td>
<td>text: Management Center Reset Password</td>
</tr>
<tr>
<td><strong>Reset Password Email Message</strong></td>
<td>text: Enter the body text of the email that will be sent upon a user’s request of a password reset. Click OK.</td>
</tr>
</tbody>
</table>

4. Do one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server. If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

5. Instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.
Set Bandwidth Cost for Reports

Statistics Monitoring reports require that you specify a bandwidth cost to display data. The bandwidth cost is a multiplier and is thus not expressed in a specific currency unit. For example, you can enter a value to represent on average how you pay per gigabit for data usage on your network.

2. Enter a decimal value.
3. Do one of the following:
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server.
   - If you are unable to save your changes, make sure that all required settings are specified.
   - Click Activate to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

Set the Device Polling Interval

You can specify the frequency with which Management Center looks for updates on managed devices. Specify an appropriate interval to ensure that device health statuses display accurately. The default interval is 10 seconds.

1. In the web console banner, select the Administration tab and select Settings.
2. Select General on the left. General fields display on the right.
3. Select Device Polling Interval (sec).
4. Enter a value in seconds.
5. Do one of the following:
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server.
   - Click Activate to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

Set the Number of Backup Slots

By default, Management Center stores up to five backups per device, with each backup placed in a slot. After five backups, Management Center prunes (deletes) an unpinned backup to make room for the new backup. (Backups that are pinned are preserved and cannot be manually deleted or automatically pruned.) If you want Management Center to store more or fewer backups per device, you can adjust the number of backup slots.

1. Click the Administration tab and select Settings.
2. Select General on the left.
3. In the Number of backup slots enter a new value.
4. Click Save.

You can override the default number of backups that are retained for a device by entering a Retention Count when exporting backups. See "Export Device Backups" on page 98.
Management Center Configuration & Management

**View Audit Log**

You can view the history of all transactions in Management Center in the Audit Log (Administration > Auditing). The log is a chronological record of changes made by users of the system.

Audit Log records are:

- Comprehensive. Records are created automatically and cannot be deleted.
- Centralized. Multiple levels of transactions are logged and displayed on one screen.
- Security-oriented. The operating user for each transaction is logged.

Audit Log records can give you insight into daily activities at a high level as well as help you diagnose and troubleshoot issues. For example, if a number of devices experience policy-related issues, you could check the log for policy-related transactions within a selected date range. You can also examine records in the Audit Log to ensure process integrity.

The audit log displays system, web-access and web logs, if configured. To access remote system logs, from the CLI enter "# rsyslog-output" on page 616.

Audit Log records can be printed in a user-friendly format. Before printing, check the bottom of the page of the Audit Log Viewer to see how many pages of records will print.

1. Learn about the types of transactions recorded in the Audit Log. See "Understanding Transaction Types" below.
2. Inspect the data recorded for transactions. See "Audit Transactions" on page 559.
3. (Optional) "Customize the Audit Log" on page 562 to focus on specific transaction data.

You can export the information in the audit log. From the Network > Export Data. You will be prompted to name the .csv file that you are exporting. Click OK.

**Understanding Transaction Types**

The Audit Log records two levels of transactions:

- EVENT: High-level transactions that occur as a result of a user action, such as adding or deleting a device
- AUDIT: Low-level internal system actions, such as deleting connection information

Each record contains the target of the operation, the operation detected, the user who executed the operation, and additional data depending on transaction type.
In the previous example, the Object Type is Role and the AUDIT transactions are changes at the system and admin levels. Filters were applied to the record type. You might find that in most cases, EVENT records provide enough detail about transactions and their effects on the system.

**Specify Explicit Proxy Settings**

If you have configured an explicit proxy server in your environment, you can specify the settings in Management Center. These settings are used for all outgoing HTTP requests and other functions such as licensing, heartbeats, and support case reports.

1. Select **Administration > Settings > HTTP Proxy**. Fields marked with a red asterisk (*) are required settings.
2. Specify explicit proxy settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable*</td>
<td>Specify whether an explicit proxy is configured.</td>
<td>false</td>
</tr>
<tr>
<td>HTTP Proxy IP or hostname</td>
<td>Specify the IP address or hostname of proxy server.</td>
<td>Example: https://&lt;IP_address&gt;</td>
</tr>
<tr>
<td>HTTP Proxy Port</td>
<td>Specify the port for the proxy server.</td>
<td>Example: 8082</td>
</tr>
</tbody>
</table>
Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>If necessary, enter the username to authenticate to the proxy.</td>
<td>Example: admin</td>
</tr>
<tr>
<td>Password</td>
<td>If necessary, enter the password to authenticate to the proxy.</td>
<td>Example: admin123</td>
</tr>
</tbody>
</table>

3. Do one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server.
     If you are unable to save your changes, make sure that all required settings are specified.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

**Configure Diagnostics Logging**

Use this page to set the logging levels. The Master Log includes all of the General and Device Plugin data. To reduce the size of the Master Log or to produce a targeted log, configure the levels accordingly. The level you choose determines the amount of information provided in each log. For example, debug logs can later be used to send diagnostic information to Support. The logging levels are described in the following table.

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEBUG</td>
<td>Logs detailed informational events and is most useful when you are attempting to diagnose problems.</td>
</tr>
<tr>
<td>INFO</td>
<td>Logs high-level informational messages only.</td>
</tr>
<tr>
<td>WARN</td>
<td>Logs potentially harmful events.</td>
</tr>
<tr>
<td>ERROR</td>
<td>Logs all errors that do not cause the system to restart.</td>
</tr>
<tr>
<td>OFF</td>
<td>Disables logging. The Master Log cannot be disabled.</td>
</tr>
<tr>
<td>ALL</td>
<td>Logs everything. Applicable only to the Master Log.</td>
</tr>
</tbody>
</table>

When you enable a log, data is written to a specific log file. For example, if the Master log is set to INFO or above, messages are written to `log.log`. If the Master Log is set to DEBUG, all messages are written to `debug.log` and also to `log.log` (messages for INFO and above). All other logs send data to a log of the same name, for example, `security.log` and `network.log`.

**Configure Diagnostic Logging**

1. Select **Administration > Settings > Diagnostics**.
   
The system displays the Diagnostics window. An asterisk denotes fields that are mandatory.
2. Specify the **Master Logging Level**, **General**, and **Device Plugin** settings.

3. Do one of the following:
   - Click **Save** to store the settings on the server.
     If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

### Configure Housekeeping Settings

Configure general housekeeping settings. When these settings are activated, they affect what is displayed in the Audit Log Viewer and how big audit logs can grow.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

1. Select **Administration > Settings**.
2. Click **Housekeeping** on the left.
3. Select the default housekeeping settings. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run every n hours. * Default is 12.</td>
<td>The value represents (in hours) how often to run a full audit.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Number of days of audit records to keep. * Default is 120.</td>
<td>The value represents the number of days that audit records are kept.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Number of days of job execution records to keep. * Default is 120.</td>
<td>The value represents the number of days that job executions records are kept.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Number of days of closed alert records to keep. * Default is 120.</td>
<td>The value represents the number of days that alerts are kept after being closed.</td>
<td>numeric using up and down arrows</td>
</tr>
</tbody>
</table>

4. Perform one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server.
     - If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

### Configure Mail Settings

In order to receive notifications via email, you must configure SMTP alerts. Management Center stores the settings so that SMTP alerts (emails) can be transmitted and received correctly. See “Configure SMTP Alerts” on page 424.

1. Select **Administration > Settings**.
2. Select **Mail Settings**. Mail settings display on the right. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server*</td>
<td>The SMTP mail server to use for outgoing mail.</td>
<td>Example: smtp.organization.com</td>
</tr>
<tr>
<td>Mail Server Port*</td>
<td>The Port that the SMTP mail server uses.</td>
<td>Example: 25</td>
</tr>
<tr>
<td>From address*</td>
<td>The e-mail address from which e-mails are sent.</td>
<td>Example: <a href="mailto:bccm@organization.com">bccm@organization.com</a></td>
</tr>
<tr>
<td>Username</td>
<td>The User name used to access the SMTP mail server.</td>
<td>Example: joe.admin</td>
</tr>
<tr>
<td>Passphrase</td>
<td>The password required to access the SMTP mail server</td>
<td>Example: admin123</td>
</tr>
</tbody>
</table>

4. Do one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server.
If you are unable to save your changes, make sure that all required settings are specified.

- Click **Activate** to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

**Configure the SNMP Agent Password**

The Simple Network Management Protocol (SNMP) itself does not define which variables a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs).

The MIBs are available on the [Downloads](#) page. Refer to the *Management Center Release Notes* for information on MIBs.

Configure the agent's password:

1. Select **Administration > Settings**.
2. Select **SNMP Settings** on the left.
3. Enter the password in the **Community** text field. This password must be entered as alpha-numeric with no special characters.
4. Perform one of the following:
   - Click **Reset** to remove your current changes and revert to the default or last saved settings.
   - Click **Save** to store the settings on the server.
   - If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the new password for SNMP agent. See Community in "Configure SNMP Alerts" on page 425.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

**Configure Consent Banner**

A Notice and Consent banner provides consent information to users of computer networks, computers, and other systems and resources. Users are required to accept the terms in the banner prior to authentication. The banner is presented to users before a login process, and it requires users to acknowledge and agree to the message before they can log in or access resources on the network.

Implement the consent banner to do some or all of the following:

- Obtain users’ notice of, and consent to, lawful monitoring of usage and data collection.
- Notify users that they must concede certain expectations of privacy in order to access the network.
- Ensure users’ compliance with organization-specific policies.

Starting with Management Center1.10.1.1, the controls also allow for simple formatting within the consent field. If you are familiar with Markdown, you can use the simple options to create and format the content.

The logo displays centered above the banner text. The banner text displays within an uneditable text box. A blue **Accept** button displays below and to the right of the banner text, as shown in the example below.
Management Center Configuration & Management

Procedure

1. Select Administration > Settings.
2. Click Consent Banner to open the editing options.
3. To activate the banner, select the box next to Show consent banner.
4. Edit what displays for the consent content. The options available include:
   a. **Company Logo or Consent Image:** Click in the Consent image field. Select a file from your local system to upload. This image appears above the consent text box. (Alternatively, you can download a copy of the currently loaded image by clicking the download button, or delete the image by clicking the remove button.)
   b. **Text Formatting:** In the Consent text box, enter the text to present to users upon login to Management Center. Format the text as needed, either with Markdown (a simple formatting code) or by using the format controls at the top of the text field. The text field displays the formatting along with the formatting code for your reference.

```
You are about to log into a restricted network. You must consent to the following:
  - The lawful monitoring and use of data collection
  - No expectation of privacy of your actions while logged in
  - Full compliance with this organization's policies and regulations

Clicking the Accept button indicates you have been informed and consent to the above conditions.
```

   The code in the editing box does not show on the consent banner when you finish.

   c. **Inline Images and/or Icons:** The format controls include a button to add images. Any images you use must first be uploaded to Management Center. See "Upload Files to Management Center" on page 532 for more information.
Editor Example

Consent Banner

Show consent banner: 

Consent text:

```markdown
### Notice

You are about to log into a restricted network. You must consent to the following:

* The lawful monitoring and use of data collection.
* No expectations of privacy of your actions while logged in.
* Full compliance with this organization's policies and regulations.

Click **Accept** to continue.
```

Consent image: [company-logo.png](https://example.com)

5. Once finished with the editing, click **Save**. (Or click **Cancel** to reset the last saved settings.)
Configure Hardware Monitor Settings

To better understand how each device is reporting disk and memory usage, configure hardware monitor settings and the Disk and Memory Critical and Warning Levels.

1. Select Administration > Settings.
2. Select Hardware Monitor Settings. Hardware monitor fields display on the right. An asterisk denotes fields that are mandatory.
3. Specify the hardware Hardware Monitor threshold settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Enabled*</td>
<td>Enable or disable hardware monitor</td>
<td>true/false</td>
</tr>
<tr>
<td>Monitor Interval (min)</td>
<td>The threshold at which the hardware monitor polls the device (in minutes).</td>
<td>5</td>
</tr>
<tr>
<td>Disk Usage - Warning</td>
<td>The threshold at which the monitor polls the device for disk usage events.</td>
<td>85</td>
</tr>
<tr>
<td>Disk Usage - Critical</td>
<td>The threshold at which the monitor polls the device.</td>
<td>95</td>
</tr>
<tr>
<td>Disk Usage - Shutdown on critical?</td>
<td>Shuts down the web console when the threshold for Critical is reached.</td>
<td>true/false</td>
</tr>
<tr>
<td>Memory Usage - Warning</td>
<td>The threshold at which the monitor polls the device for memory usage events.</td>
<td>95</td>
</tr>
<tr>
<td>Memory Usage - Critical</td>
<td>The threshold at which the monitor polls the device for memory usage events.</td>
<td>99</td>
</tr>
</tbody>
</table>

4. Perform one of the following:
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server.
     If you are unable to save your changes, make sure that all required settings are specified.
   - Click Activate to cause the server to load and apply the currently saved configuration.

If you enable the hardware monitor and also enable Disk Usage - Shutdown on critical?, the web console shuts down when the threshold for critical is reached. The Management Center CLI is still available.

If you have unsaved changes, the edited settings are marked with a red triangle. See the “Pending changes” text at the top left of the dialog as an example.

Upload Files to Management Center

Use the Configuration > Files page to add files to Management Center. These files can be used for various operations, including upgrading Management Center.
All file types except .exe can be uploaded. If you upload a file with one of these extensions: .bcl, .bcsi, .nru, .nsu, .pac, .patch, .si, .txt; the file is automatically associated with the proper file type—config, image, license, text. If the file type is not one of the preceding, Management Center labels it as unknown.

You can limit the actions users are allowed to perform on this page by adding the File permission to a new or existing role.

Management Center replaces special characters in file names.

Upload Files

1. Select Configuration > Files.
2. Add the file using one of the following methods:
   - By browsing:
     a. Click Add File.
     b. Click Select File and browse to the file(s).
     c. Select the file.
     d. Click Open.
     e. Click Upload.
   - By dragging and dropping one or more files:
     a. Click Add File.
     b. Drag and drop the files into the Upload Files window
     c. Click Upload. If a file with same name already exists, the system prompts you to choose whether to upload and replace the existing file, skip the download, or to keep both and upload the file with a new name. If the upload will exceed the available space on disk, you are prompted to delete files to make room for the new file.
3. Management Center indicates the progress of the upload.

Transfer Files

Click Transfer File to retrieve files from a URL.
Files

1. Click **Transfer File**. The system displays the File Transfer window.

2. Enter the URL into the **Server URL** field.
3. Select the **File Type**.
4. Select the behavior to occur if the file already exists.
5. Click **Run Now** to start the job immediately or create a scheduled job.

**Associate File with Device Type**

If you upload an image file with the intention of upgrading one of your managed devices, you must associate the file with a device type.

1. Select the file.
2. Right click the **Device Type** field in that row and click **Edit**.
The system displays the **Edit File** window.

3. Select the device type from the **Device Type** drop-down.

4. Click **Save**.

**Edit Uploaded Files**

To edit a file, select the file and click **Edit**. The system displays the **Edit File** dialog. Here, you can edit the following:

- **Display Name**
- **File Type**
- **Device Type**
- **Description**

**Sort, Group, and Modify Uploaded File Data**

Click the arrow to the right of the column headings to sort and group uploaded files.
Hover over **Columns** to change the displayed columns. Select **Group by this field** to group the table data in accordance with that column heading. Deselect **Show in groups** to put data into a plain list.

**Delete Uploaded Files**

To delete a file, select the file and click **Delete**.

**Copy File URL**

To copy the file’s URL, click **Copy URL**. The URL opens in a small sub-window. You can then right-click the URL and select **Copy** or enter CTRL-C to copy the URL. You can then paste the URL into Management Center CLI commands (for example, installing a new image), and other options or operations that accept URLs.

**Migrate Device Metadata from Director as Management Center Scripts**

To migrate a Symantec Director device hierarchy (including overlays) into Management Center, you need to export the device metadata from Director, placing the migration file in a location that Management Center can access.

**Prerequisites:**

- Obtain or verify access to the Symantec Director CLI.
- Obtain or verify access to an HTTP, SCP, or FTP server, and ensure that you have access privileges to upload data
to it.
- Obtain or verify access to the Management Center web console.

Export Metadata from Director as an Encrypted File

1. Log into the Director CLI and go into config mode.
2. Type the following command to generate the migration file:
   
   (config)# mc-migration generate
   
   The CLI prompts you to enter a passphrase. You will be required to enter this passphrase to generate the metadata and import it in the Management Center application.
3. Enter a passphrase consisting of at least four characters and press Enter.
   
   The CLI generates the device metadata. The metadata is encrypted and compressed in a Gnu Privacy Guard (GPG) encrypted (*.tgz.gpg) file. For example: SGME-Director-to-MC-Migration-2015.03.13-154907.tgz.gpg.
   
   Make note of the filename.
4. Upload the compressed and secured file to an external HTTP, SCP, or FTP server. Enter the command:
   
   (config)# mc-migration upload fileserver
   
   where:
   
   file is the filename you recorded in the previous step.
   server is the hostname or IP address of an external server:
   
   http://hostname_or_address[:port]/path_and_filename
   ftp://hostname_or_address/path_and_filename
   scp://hostname_or_address//path_and_filename

   If necessary, copy or move the file to a location that Management Center can access.

Export Metadata from Director as an Unencrypted File

1. Log into the Management Center web console.
2. Click the Network tab.
4. On the Import from File dialog, select **Download JSON Schema** to download the schema to which the JSON file must conform.

5. Log into Director and prepare the JSON file. To help you understand the schema, refer to the example `bccm-data-sample.json` found in the download.

   Symantec recommends that you familiarize yourself with the JSON Schema as defined by the IETF in draft 4 (see http://tools.ietf.org/html/draft-zyp-json-schema-04). This will help you understand Symantec’s JSON schema for import. Symantec is not yet strictly conforming to this standard, nor is the customer’s JSON file validated against this schema. However, the intention is that Management Center strictly conforms when the IETF draft becomes a standard. In the meantime, should they exist in the JSON document, Management Center returns helpful errors to indicate problem areas and errors.

6. After your JSON document is prepared, compress it in *.tar.gz or *.tgz format.

   **Linux Example:** `tar -cvzf myjsondata.tgz data.json`

7. **(Optional)** Secure your compressed file.

   a. To secure your compressed file with Gnu Privacy Guard (GPG) encryption (*.gpg format), use config mode in Director.

      **Linux Example:** `echo 'password' | /usr/bin/gpg --batch --yes --no-tty --compress-level 0 --cipher-algo AES256 --symmetric --passphrase-fd 0 myjsondata.tgz`

      `(config)# mc-migration generate`

      The CLI prompts you to enter a passphrase. You will be required to enter this passphrase to generate the metadata and import it in Management Center.

   b. Enter a passphrase consisting of at least four characters and press Enter.

      The CLI generates the device metadata into an encrypted and compressed file (*.tgz.gpg). For example, `SGME-Director-to-MC-Migration-2015.03.13-154907.tgz.gpg`.

8. Make note of the filename.

9. Upload the compressed file to an external HTTP, SCP, or FTP server. Enter the command:

    `(config)# mc-migration upload fileserver`
Management Center Configuration & Management

where:

file is the filename you recorded in the previous step.

server is the hostname or IP address of an external server:

http://hostname_or_address[:port]/path_and_filename
ftp://hostname_or_address/path_and_filename
scp://hostname_or_address//path_and_filename

If necessary, copy or move the file to a location that Management Center can access.

Import Director Metadata as Scripts into Management Center

From the Management Center web console, import the device metadata file that is currently saved on an external server.

1. Log into the Management Center web console.
2. Click the Network tab.
4. Select the Import from file exported from an external system check box, then click Launch Import Wizard.
5. On the Import from File: Select File dialog, select the file that you want to import. The GPG encrypted file check box is selected by default for (*.gpg) files. Clear the check box if your file is not encrypted (*.tar.gz or *.tgz format).

Files must have the extensions *.gpg (Gnu Privacy Guard [GPG] encrypted compressed file), *.tar.gz, or *.tgz (unencrypted compressed files).
6. If necessary, enter the passphrase that you specified when generating an encrypted file, then click Next. An asterisk denotes fields that are mandatory.

7. Select devices and device groups to import from a hierarchy. If any device is not a member of a hierarchy, a pseudo-hierarchy is available, named Unassigned. If any errors or warnings exist, for any device, the status is shown on the right. To select all devices in all hierarchies, select All Hierarchies.
A device can only exist in one group for a given, distinct hierarchy. Devices can be members of different hierarchies.

8. The available scripts show on the Import from File: Select Scripts dialog. By default, all scripts are selected. Clear the check box for any script you do not want to import. When finished selecting scripts, click **Import**.
Any ProxySG appliances that are running SGOS 5.x are imported in a deactivated (pre-deployment) status.

9. The Import from File wizard displays the Device Import Status dialog. The Overlays Summary and list of imported overlays show at the bottom. When finished viewing the import status, click Close.

10. View the successfully migrated devices, device groups, and hierarchies in the Management Center Network tab.
11. View imported overlays by selecting **Configuration > Scripts**.

**Optional** Delete Migration File in Director

After you have successfully imported devices from Director, you can delete the migration metadata file from Director.

1. Log in to the Director CLI.
2. Type the following command:

   ```
   (config)# mc-migration delete file
   
   where `file` is the name of the migration file.
   ```

After the file is deleted, the CLI displays the `(config)#` prompt again.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group</td>
<td>&quot;Ensure Devices Belong to Device Groups&quot; on page 118</td>
</tr>
<tr>
<td>Change device information</td>
<td>&quot;Edit a Device&quot; on page 66</td>
</tr>
</tbody>
</table>
Upgrade/Downgrade System Images

When new features and improvements are made to Management Center, you can download a system image from Symantec and upgrade the appliance. If you ever experience issues with a new image, you can activate an older image to downgrade the appliance.

You can install a system image to the following devices from Management Center:

- Blue Coat ProxySG
- Advanced Secure Gateway (ASG)
- Content Analysis (CA)
- Malware Analysis (MA)
- SSL Visibility

Restrictions

- Downgrading a Content Analysis 2.x appliance is not supported.
- Upgrading SSL Visibility appliances from 3.x to 4.x requires other tasks not documented here.
- Downgrading SSL Visibility appliances from 4.x to 3.x is not supported.

Refer to the CA and SSL Visibility product documentation and release notes for information about these restrictions.

Manage System Images

Management Center stores up to six images on the system. For Management Center virtual appliances, this number also depends on the image size and boot partition (limited to 2 GB by default). The image that is marked as the default image will be loaded the next time that the appliance is rebooted.

If the maximum number of images are stored on your system and you download another image, Management Center deletes the oldest unlocked image to make room for the new image. To prevent an image from being deleted or replaced, you can lock the image.

You perform image management using Management Center CLI commands. See "# installed-systems" on page 611 for a description of the commands for adding, deleting, locking, unlocking, and viewing images.

Install a New System Image

To install a new system image, you first download the image from Symantec, place the file on a web server the Management Center appliance can access, then use a CLI command to add the file. The final step is to reboot to activate the image.

1. (Optional, but recommended) "Back Up the Management Center Configuration" on page 546.
2. Log into Symantec Support: https://support.symantec.com/ and do the following:
   2. Select Downloads > Network Protection (Blue Coat) Downloads and sign in with your credentials.
   3. From the My Products list, select Management Center.
   4. Select the model.
   5. Select the software version.
   6. Select I AGREE to the License Agreement.
   7. Check the box next to the desired file and click Download Selected Files.
3. Download the desired image.
   a. Transfer the image directly to Management Center. Select Configuration > Files and transfer the image using the Transfer File button.
   b. Download the image to a local drive, select Configuration > Files, and upload the image to Management Center.

Alternatively, you can store the image file on a web server that the Management Center appliance can access. The add image process works with any HTTP server, and HTTPS servers configured with trusted certificates. If your HTTPS server does not have a trusted certificate, place the file on an internal HTTP server.

4. Add the system image using the #installed-systems add <URL> command.
   where <URL> is the location of the image on a web server, in the following format:
   http://host/path, for example http://webserver.mycompany.com/images/542386.bcsi

   If the image was uploaded to Management Center, do the following:
   a. Copy the file URL. In the Configuration > Files page, select the image and click Copy URL. The file will have a format similar to the following:
      https://10.131.38.36:8082/fs/download/6c80d3a2cc124347aedb2a688da3859e
   b. Change the protocol in the displayed URL to HTTP and change the port to 8080. The URL should now look like this:
      http://10.131.38.36:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e

      If HTTP access to Management Center is disabled, you should change the URL to the following:
      http://127.0.0.1:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e
   c. Enter installed-systems add and paste the URL from above. Press enter to execute the command.

5. Make sure the new image is the default image. (Rebooting will install whichever image is marked as the default.)

   # installed-systems view
   A plus (+) sign indicates the default system image. If the new image is not the default, make note of the index value next to the image you want as the default.

6. If necessary, make the new image the default system image:

   # installed-systems default <index_number>
   Replace <index_number> with the image’s index ID value.

7. Reboot the hardware appliance to run the new image:

   # restart reboot

   When the appliance restarts, the network connection closes. If boot failure occurs upon an upgrade, Management Center downgrades to the previous version automatically.
View the progress of downloads in progress or the status of the last download using the `# installed-systems view-downloads` command. If you need to cancel an image download, use the `# installed-systems cancel-downloads` command.

**Downgrade to an Earlier Management Center Version**

If you are running an upgraded version of Management Center, you can downgrade (revert) to a previous version. Downgrading has the following special guidelines you must follow:

- Downgrades can be performed down two dot releases (e.g., from 1.6 to 1.4).
- All maintenance/patch releases of a version will be treated as equivalent. For example, 1.6.2.1 would be the same as any other 1.6.x release.
- Upon downgrade, newer data (data from the upgraded image that is not handled in the older version) is lost.
- Upon downgrade, newer configuration settings (settings from the upgraded image that are not handled in the older version) are lost.
- Data and configuration settings that are common to the upgraded image and downgraded image are seamlessly maintained, regardless of schema differences between versions.
- Administrator access and permissions are needed to downgrade Management Center.

To downgrade:

1. "Back Up the Management Center Configuration" below.
2. Decide which installed image to revert to. (Make sure to follow the guidelines listed above regarding release numbers.)
   ```
   # installed-systems view
   ```
   Make note of the index value next to the image you want to revert to.
3. Make an older image the default image. (Make sure to follow the guidelines listed above regarding release numbers.)
   ```
   # installed-systems default <index_number>
   ```
   Replace `<index_number>` with the image's index ID value.
4. Reboot the hardware appliance to activate the default image:
   ```
   # restart reboot
   ```
5. Before trying to use the older version, restore the Management Center backup immediately. See "Restore a Management Center Backup Configuration" on page 549.

**Back Up the Management Center Configuration**

Symantec recommends that you back up the Management Center configuration often. The backup contains Management Center database, settings, and, optionally, device reporting statistics. To save disk space on the appliance, you can export the backup to an external server as part of the backup job. Exporting backups to an external server is required before upgrading or downgrading the software image. See "Upgrade/Downgrade System Images" on page 544.
Backup Requirements

Backing up the Management Center configuration requires specific permissions. See "Reference: Understanding Job Permissions" on page 352. Additionally, sensitive data in the backup will be encrypted with an encryption key. You must have the recovery key to restore the encrypted data in the backup. See "Encrypt Sensitive System Data" on the next page for more information.

Back Up Management Center

To back up the Management Center configuration, you must create a job for it. You can either schedule the job to run on a regular basis, run immediately, or on demand at a time that you want to create a backup.

1. From Jobs > Scheduled Jobs, select New Job. The web console displays the New Job wizard. An asterisk denotes fields that are mandatory.
2. Enter a unique Name.
3. Enter a Description (perhaps the reason why a backup of Management Center is needed). Click Next.
4. From the Operation drop-down list, select Backup Management Center.
5. (Optional) Select the Exclude Statistics Monitoring Trend Data check box to exclude device reporting statistics. By excluding these statistics, the backup will be substantially smaller (perhaps by hundreds of gigabytes). Keep in mind, however, that the restored backup will not have any statistics data.
6. If you want the backup file to be exported to an external HTTP, FTP, or SCP server, select the Export to Server check box and fill in the server details:
   - Server URL: Enter the protocol (SCP, FTP, FTPS, HTTP, HTTPS) and server name and path. For example: ftp://mycompany.com/backups
   - Encryption Phrase: This is required for exporting the archive.
   - Username
   - Password
7. In the Targets screen, click Next. (No targets are required for this operation.)
8. In the Schedule screen, define a schedule for the job. See "Job Scheduling Options" on page 436 for explanations of each option. Click Finish.

Management Center retains only five backups. When the sixth backup occurs (such as in a recurring job), the oldest backup is deleted. This is a rolling five backup retention and cannot be configured. To retain additional backup configurations, you can export the backup to an external server as part of the backup job, or you can export backups later using the backup export CLI command.

Back Up Management Center Using the CLI

1. Log in to the CLI. See "Access the Management Center CLI" on page 594
2. Enter privileged mode. See "Privileged Mode Commands" on page 602.
3. At the command prompt, type the following command and press Enter:
   
   # backup create

   The CLI indicates that the backup is being created. You should see a response similar to the following:
   
   Creating backup ...
   Backing up runtime configuration and plugins ...
   Backing up database..
Encrypt Sensitive System Data

In 1.6 and later, each Management Center appliance (hardware or virtual) has a unique encryption key that is used to encrypt data in the system. The administrator generates this key in the Administration > Data Protection page. When the key is generated, a recovery key is also generated in case you later need to restore the encryption key. Make sure to save the recovery key in a safe place.

Potential Data Loss

- As part of this process, you should keep the recovery key in a safe place in the event that you need to restore the encryption key later. DO NOT LOSE THE KEY. If you lose the key, you will not be able to recover your encrypted data.
- You should not recover a key unless you are certain that you need to. If you use the Restore previous key feature and the current data in the database was not encrypted with that key, that data will not be able to be decrypted and you will have to reenter all of the device passwords.
- If the current passwords for the device were not encrypted with the previous key, you will not be able to access the information with the current passwords. You will need to reenter the device passwords before accessing the backup information.

New Management Center Appliance Recommendations

Upon receiving a new appliance, you should do the following:

1. Select Administration > Data Protection.
2. Click Generate Key.
   
   A new encryption key is created and a recovery key is displayed.
3. Record the recovery key and secure it in a safe location.
4. Click Restart System.
5. Configure the appliance.
6. Run a Management Center backup. See "Back Up the Management Center Configuration" on page 546.

This process ensures that you can restore your configuration as necessary.

Upgrade Recommendations

If you are upgrading Management Center, Symantec recommends regenerating a new key and then taking a new backup. Doing so will ensure that you have the latest protection schemes and a valid backup that can be restored to the device if necessary.

1. Select Administration > Data Protection.
2. Click Generate Key.
   
   A new encryption key is created and a recovery key is displayed.
3. Record the recovery key and secure it in a safe location.
4. Click Restart System.
5. Run a Management Center backup. See "Back Up the Management Center Configuration" on page 546.
This process ensures that you will be able to restore the previous configuration if the upgrade has issues.

**Restore a Management Center Backup Configuration**

You can restore a configuration backup after reinstalling, upgrading, or downgrading Management Center or if you want to revert to a previous configuration. You perform this operation using the command-line interface.

Restoring a backup requires shutting down services; you should perform the restore during off-hours.

**Restore Management Center Backup**

Before you restore a backup, you should view the backup files currently stored on the system to make sure that you restore the correct version. If the backup you want to restore was exported to an external server, you should import the backup file before the restore process.

1. "Access the Management Center CLI" on page 594.
2. Enter privileged mode. See "Privileged Mode Commands" on page 602.
3. At the command prompt, type the following command and press Enter:
   
   ```
   # backup view
   ```

   The CLI displays a list of all the backups that were created for this instance of Management Center. You should see a response similar to the following:

   ```
   Available Backups:
   Timestamp               Version
   1 | 2015-May-29 03:33:00 UTC 1.4.1.1 (555156)
   2 | 2015-Apr-15 09:02:00 UTC 1.3.3.1 (555000)
   ```

   The backups are listed in descending chronological order; for example, the backup with index number 1 is more recent than index 2. Each backup indicates the date and time when the backup was created, the build version, and in parentheses, the build number.

4. Once you identify the backup you want, make note of the index number.

5. (Optional) If the backup you want to restore was exported to a server and is not on the list of backups stored on the appliance, you can import it to Management Center.

   ```
   #backup import <URL>
   ```

   `<URL>` is the URL of the server and path to the backup file. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP.

6. At the command prompt, type the appropriate command.

   - To restore the latest version (the backup with the most recent timestamp):
     ```
     # backup restore latest
     ```
   - To restore a specific version:
     ```
     # backup restore <index_number>
     ```
     where `<index_number>` is the index number of the backup.

7. Press Enter. The CLI indicates that you are about to restore a backup and asks you to confirm the action:

   ```
   Warning, restoring a backup replaces all Management Center configuration.
   ```
Do you wish to proceed with restoring the backup taken on 2015-May-29 03:33:00 UTC? [Y/N]

8. Type Y to proceed. The CLI displays the progress of the restore:
   Restoring backup ...
   Decompressing ...
   Verifying backup contents ...
   Shutting down services ...
   Restoring database ...
   Restoring configuration ...
   Restarting services ...
   Completed restoring backup.

Configure Management Center Failover

Management Center supports failover using two physical appliances. One appliance is delegated as the primary and the other as the secondary. After failover is configured, the secondary replicates data from the primary appliance. During continuous replication, users can perform all normal operations on the primary failover partner. Users cannot access the secondary failover partner—it's sole purpose is to replicate actions occurring on the primary node so that it can take over if something happens to primary node.

Licensing information and system settings are not transferred during failover replication, so if you choose to configure multiple physical or virtual Management Center appliances using the native failover configuration, each appliance will require a license of its own.

If your implementation of Management Center uses virtual appliances, Symantec recommends that you use the vMotion feature of ESX to manage failover. This solution has the following benefits over the native failover option built into Management Center:

- vMotion failover ensures that only one Virtual Appliance (VA) is active at a time, and as such, only a single license is required.
- Because only one VA is active at a time, your ESX server is spared the extra system resources from running two instances of Management Center.
- Failover with vMotion is automatic. Deploying multiple Management Center Virtual Appliances with native failover requires that administrators manually switch the active primary virtual appliance.

See Verify VMware Requirements for more information.

For systems setup in failover, the data encryption key is kept in sync between the primary and secondary devices.

Replicated Data

The following data is replicated on the failover partner:

- Device data stored in the database.
- Files in the Management Center file store
- Policy and scripts (along with historical versions)
- Device backups
- PDM data from ProxySG appliances
- Data protection key
- Trusted certificates for servers; root CA installed by a user

The following data is not replicated on the failover partner:

- Management Center system settings
- Management Center backup images on the device itself

**Configuration Limitations**

During replication, configuration for both the primary and secondary failover partners is limited. Replication requires that both the primary and secondary partners run the same version of Management Center. To enforce this, the `installed-systems` CLI command is disabled on both failover partners (to deny installing and changing system images). If, for any reason, the system images do not match on the primary and secondary partners - replication is paused until the problems are resolved.

The secondary failover partner has stricter restrictions on what can be configured. In addition to not being able to manage system images, the following CLI commands are disabled on the secondary partner:

- `backup` (all commands)
- `license` (all commands)
- `http-proxy` (all commands)
- `service db-maintenance`
- `service purge-vpm-cache`
- `snmp` (all commands)
- `statistics-monitoring` (all commands)

**Device Limitations**

Because Web Security Service (WSS) devices are initially registered through a connection established only with the primary partner (which subsequently discards the credentials), WSS connections will fail if an event causes a failover to the secondary partner. In that event, you must re-authenticate to those WSS devices (Network > Edit Device > Connection Parameters).

**Failover Prerequisites**

To prepare for failover:

- Identify a Management Center appliance to act as the primary failover partner. Record the IP address and password of the "admin" account of this device.
- Identify a Management Center appliance to act as the secondary failover partner. Record the IP address of this device.
- Ensure that port 22 is open between the primary and secondary partners. Management Center failover employs an SSH connection.

**Configure Failover**

You must enable failover using the CLI.
Step 1—Configure the Primary Appliance

1. Use an SSH client to log into the CLI of the Management Center appliance that is to be the primary failover partner.
2. Enter Enable mode:
   ```
   # enable
   ```
3. Confirm that failover has not already been configured on the appliance:
   ```
   # failover view
   Failover:
   Status: Disabled
   ```
4. Make this appliance the primary failover partner:
   ```
   # failover make-primary
   ```
   At this point, the secondary is not configured so the command output is similar to the following:
   ```
   Failover
   Status: ERROR: Secondary not configured
   Primary*: 198.51.100.20
   Secondary: not configured
   Last status update 1 second(s) ago
   (*)& this Management Center
   ```

Because the secondary failover partner has not been configured, the failover icon displays with an exclamation mark:

This icon also displays if failover has been configured and the secondary is unresponsive.

Step 2—Configure the Secondary Appliance

Before beginning this procedure, complete all tasks required for the secondary appliance to service requests (set up authentication, etc.).

1. Use an SSH client to log into the CLI of the Management Center appliance that is to be the secondary failover partner.
2. Enter Enable mode:
   ```
   # enable
   ```
3. Confirm that failover has not already been configured on the appliance:
   ```
   # failover view
   ```
Failover:
Status: Disabled

4. Make this appliance the secondary failover partner:

During this process, the services on both the primary and secondary appliances are unavailable.

```
# failover make-secondary
```

Enter the IP address for primary server []: 198.51.100.20
Warning: Initial failover data transfer may take a long time to complete. To complete the failover setup, allow for transfer to finish and do not disable failover on 10.169.21.81 (primary) or 10.169.21.82 (secondary) during this operation. Services on 10.169.21.81 (primary) will not be available while initial failover setup is performed.

Are you sure you want to continue? y

Please authenticate to primary server...
admin@198.51.100.20's password:
Shelving operational data on secondary...done.
Stopping services on secondary...done.
Stopping services on primary...done.
Retrieving snapshot of primary's data...

The password is not saved and is not reused for further replication process.

5. Verify that failover has been successfully configured:

```
# failover view
```

Failover:
Status: Healthy (0 second replication delay)
Primary: 198.51.100.20
Secondary*: 198.51.100.24

If failover has been successfully configured, the failover icon displays in the web UI banner:

You can also mouse over the failover icon to review the failover status.
Switch to Secondary When the Primary is Unresponsive

If the primary failover partner is unresponsive, you must:

1. Make the secondary failover partner active. Do this by entering the command:
   
   # failover make-primary

2. Reactivate statistics monitoring.
   
   At this point, the secondary is active and is now the primary failover partner.

3. Fix the problems with the original primary device.

4. Make the original primary device (the device that was unresponsive) the new secondary failover partner:
   
   # failover make-secondary

Failover is now successfully reconfigured.

Step 1—Make Secondary Partner Active

Issue the `failover make-primary` command to make the secondary appliance the primary failover partner. If the original primary device later becomes responsive, you can make it the secondary failover partner, thus preserving the failover capability.

`# failover make-primary`

System is configured as secondary, promoting state to primary will break replication.

Are you sure you want to promote state to primary? [y/N]

Restoring operational data...done.

Failover:

Status: ERROR: Secondary not configured

Primary*: 198.51.100.24

Secondary: not configured

Last status update 2 second(s) ago

(*) this Management Center

Step 2—Reactivate Statistics Monitoring

After making the secondary failover partner active, you must reactive the statistics monitoring job. This job instructs devices that have PDM Export (statistics monitoring) enabled to send updates to the new primary device.
1. Select **Jobs > Scheduled Jobs**.
2. Click **New Job**. The system displays the New Job: Basic Info dialog.
3. In the Basic Info dialog, enter a name for your job. An asterisk denotes fields that are mandatory.
4. Enter a description of the job. Good descriptions help to differentiate jobs when they have similar names.
5. Click **Next**.
6. In the Operation dialog, select **Reactivate Statistics Monitoring**.
7. Click **Next**.
   The system displays the **Targets** dialog. Management Center automatically finds all applicable targets.
8. Click **Next**.
   The system displays the **Schedule** dialog. Optionally, enter a schedule.
9. Click **Finish**.

**Disable Failover**

Use the `failover disable` command to disable failover.

```
# failover disable
```

Failover:
Status: Healthy (0 second replication delay)

Primary: 198.51.100.20
Secondary*: 198.51.100.24

Last status update 2 second(s) ago
(*) this Management Center

Are you sure you want to disable failover? [y/N]

Restoring operational data...done.
Failover:
Status: Disabled
Update the Management Center License

The Management Center license contains all of the features for which you have purchased a subscription. The documentation covers all features, including ones that you may not have purchased.

You can update your existing license from the Network Protection Licensing Portal (NPLP), download the license from a web server or workstation, or install it manually.

1. To view license status or to update or install a license, select Administration > License.
2. To view detailed license component information, select the License Components tab.

Use the passphrase field when you are installing a license you generated with a passphrase; the passphrase is required for VA Offline licensing.

3. To determine how you will install the license, select the Install New License tab. See the following sections for instructions.
4. (Optional) To troubleshoot the license installation, do the following:
   - To check the status of a license, run the CLI command license view.
   - To verify network settings, run the CLI command show interface.
   - To verify site accessibility, run the CLI command ping with the following sites:
     - ping bto-services.es.bluecoat.com
     - ping validation.es.bluecoat.com
   - To update the license, run the CLI command license get-from-bluecoat.
   - Try to update the license again, after running the CLI command restart reboot.
5. (Optional) From a web browser, log into Management Center. If the web console loads, the license was installed successfully.
   If the web console does not load, run the CLI command license view to determine if the license was installed and is valid.

Install the license from BTO

You must install the license from NPLP (formerly BTO) using the license get-from-bluecoat CLI command at least once before you can install it using the web console.

1. Select Administration > License.
2. Click the Install New License tab.
3. Select Install from BTO.
4. Enter your NPLP User ID and Password.

The Network Protection Licensing Portal (NPLP) was formerly known as BTO.

5. Click Install License.
6. Click Refresh to display the updated license information in the License Components table.
Install from URL

Before you can install your license you must first get the license file (*.bcl or *.bin) and save it to a location on a web server or workstation that the VA can access.

1. Select Install from URL. The web console displays a text field.
2. Enter the location (a valid URL) of the license file into the field.
3. Click Install License.
4. Click Refresh to display the updated license information in the License Components table.

Paste license text from a text editor

Before you can install your license you must first get the license file (*.bcl or *.bin) and save it to a local directory. Open the license file in a text editor (such as Notepad) and make sure you save the file.

1. Select Paste license text. The web console displays a text box.
2. Copy and paste the license from the text editor to the box.
3. Click Install License.
4. Click Refresh to display the updated license information in the License Components table.

Verify License Components from the Web Console

Management Center has a flexible license model. Components can be licensed, and are exposed dependent upon the license type and component name. You can view the validity of licensed components, add more devices to your license, and view the serial number and appliance model of the hardware appliance. Install or update your licenses directly from NPLP while logged into the web console.

1. To verify the license components, type and status, log in to the web console.
2. Select Administration > License. From the License Component tab you verify the following General Information about the license:
   - Manufacturer (Symantec Corporation)
   - Number of Maximum Devices allowed
   - Serial Number
   - Appliance Model
   - Status
   - Component Name
   - Activation date
   - Expiration date
   - License Type
Troubleshoot and Resolve Issues

This section discusses troubleshooting steps and advanced procedures for Management Center.

The following topics provide information for resolving common issues:

- "Reset or Restore Admin Account Passwords" on page 380
- "Upgrade/Downgrade System Images" on page 544
- "Encrypt Sensitive System Data" on page 548
- "Back Up the Management Center Configuration" on page 546
- "Restore a Management Center Backup Configuration" on page 549
Audit Transactions

To access the Audit Log Viewer, click Administration > Auditing.

By default, recent transactions are displayed on the first page of records. If they are not on the first page, or if you are looking for historical data, you can navigate to different pages or limit the number of records to locate the correct ones. For instructions, see "Customize the Audit Log" on page 562.

Records do not display in the Audit Log Viewer immediately after transactions occur; refresh the web console to see most recent records. You can click the Refresh icon at the bottom of the screen to update the most recent entries.

To understand and analyze the data recorded for each transaction, refer to the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Time</td>
<td>The date (in YYYY-MM-DD format) and time (in 24-hour notation) the transaction was completed.</td>
</tr>
<tr>
<td>Operating User</td>
<td>The user who performed the operation. If no user is associated with the operation, SYSTEM is displayed.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Record Type</td>
<td>The transaction level: AUDIT or EVENT. An audit record is a system-level transaction; an event record is a user-level transaction. For more information, see &quot;Understand Transaction Types&quot; on the next page. This column is hidden by default.</td>
</tr>
<tr>
<td>Object Type</td>
<td>The type of object on which the operating user performed the action.</td>
</tr>
<tr>
<td>Operation Type</td>
<td>The operation that was completed.</td>
</tr>
<tr>
<td>Info 1 - Info 5</td>
<td>Additional reference fields for the record. Not all transaction types have additional information. Columns Info 3 through Info 5 are hidden by default.</td>
</tr>
</tbody>
</table>
Understand Transaction Types

The Audit Log records two levels of transactions:

- Event—High-level transactions that occur as a result of a user action, such as adding or deleting a device
- Audit—Low-level internal system actions, such as deleting connection information

Each record contains the target of the operation, the operation detected, the user who executed the operation, and additional data depending upon transaction type.

In the previous example, the Object Type is Role and the AUDIT transactions are changes at the system and admin levels. You might find that in most cases, EVENT records provide enough detail about transactions and their effects on the system. Filters were applied to the record type.
Customize the Audit Log

Because the Audit Log records all transactions on multiple levels, the log can grow very quickly—especially if you many devices are managed in Management Center and there is a high level of user activity. Although the Audit Log is designed to make it easy for you to locate the records you want, you can customize the display further to help you locate specific records, isolate records from a certain date or time, filter records pertaining to specific users or objects, and more.

Use the following methods in conjunction to customize the Audit Log display to suit your purposes.

When you make the following changes in the Audit Log Viewer, the changes do not persist beyond the current browser session; the next time you log in to the web console, you must go through the same steps to change the viewer again.

Show or hide columns

You can show columns that you hid, or columns that are not visible by default, such as Record Type and Info 3 through Info 5. You can hide some columns if you want a more general look at the log or if your screen size is limited.

To see all information available in the Audit Log and ensure that you can see an appropriate level of detail, you can show all columns first and then choose which ones, if any, you want to hide.

1. On any column header, click the arrow. The web console displays a list of options.
2. Select an option to show the column.
   - Clear an option to hide the column.
3. Click anywhere outside of the list to close it.
   - The Audit Log shows/hides the columns you specified.

Sort columns

Because the Audit Log displays records in descending chronological order by default, you can re-arrange them to analyze the data more effectively. By default, the records are sorted in descending order of Operation Time (latest to earliest).

1. Click the header of the column you want to sort.
   - If the header displays an up arrow, the data is arranged in ascending order (A-Z, earliest to latest).
   - If the header displays a down arrow, the data is arranged in descending order (Z-A, latest to earliest).
2. Click the header again to reverse the sort order.

In the following example the columns are sorted by Operation Type, so all Authentications are displayed first.

Filter records

To limit the amount the data that the log displays and focus only on specific records, apply filters using the drop-down lists on the right. Depending on the transaction level, you may need to filter pages of records. The filters limit the record type. To narrow the search, apply one or more filters.
If applying a filter results in too few records or not the right records, remove or change some filters. To reset the filters to default, click **Clear**.
Configure Housekeeping Settings

Configure general housekeeping settings. When these settings are activated, they affect what is displayed in the Audit Log Viewer and how big audit logs can grow.

If you have unsaved changes, the edited settings are marked with a red triangle. See the “Pending changes” text at the top left of the dialog as an example.

1. Select Administration > Settings.
2. Click Housekeeping on the left.
3. Select the default housekeeping settings. An asterisk denotes fields that are mandatory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run every n hours.* Default is 12.</td>
<td>The value represents (in hours) how often to run a full audit.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Number of days of audit records to keep.* Default is 120.</td>
<td>The value represents the number of days that audit records are kept.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Number of days of job execution records to keep.* Default is 120.</td>
<td>The value represents the number of days that job executions records are kept.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Number of days of closed alert records to keep.* Default is 120.</td>
<td>The value represents the number of days that alerts are kept after being closed.</td>
<td>numeric using up and down arrows</td>
</tr>
</tbody>
</table>

4. Perform one of the following:
   - Click Reset to remove your current changes and revert to the default or last saved settings.
   - Click Save to store the settings on the server.
     - If you are unable to save your changes, make sure that all required settings are specified.
   - Click Activate to cause the server to load and apply the currently saved configuration.

Configure Diagnostics Logging

Use this page to set the logging levels. The Master Log includes all of the General and Device Plugin data. To reduce the size of the Master Log or to produce a targeted log, configure the levels accordingly. The level you choose determines the amount of information provided in each log. For example, debug logs can later be used to send diagnostic information to Support. The logging levels are described in the following table.

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEBUG</td>
<td>Logs detailed informational events and is most useful when you are attempting to diagnose problems.</td>
</tr>
<tr>
<td>INFO</td>
<td>Logs high-level informational messages only.</td>
</tr>
<tr>
<td>WARN</td>
<td>Logs potentially harmful events.</td>
</tr>
<tr>
<td>ERROR</td>
<td>Logs all errors that do not cause the system to restart.</td>
</tr>
</tbody>
</table>
Management Center Configuration & Management

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>Disables logging. The Master Log cannot be disabled.</td>
</tr>
<tr>
<td>ALL</td>
<td>Logs everything. Applicable only to the Master Log.</td>
</tr>
</tbody>
</table>

When you enable a log, data is written to a specific log file. For example, if the Master log is set to INFO or above, messages are written to `log.log`. If the Master Log is set to DEBUG, all messages are written to `debug.log` and also to `log.log` (messages for INFO and above). All other logs send data to a log of the same name, for example, `security.log` and `network.log`.

**Configure Diagnostic Logging**

1. Select **Administration > Settings > Diagnostics**.

   The system displays the Diagnostics window. An asterisk denotes fields that are mandatory.

   **Diagnostics**
   
   **Master Logging Level:**
   
   Security Logging Level:
   
   Networking Logging Level:
   
   Device Management Logging Level:

   **General**
   
   **Device Plugins**
   
   **Content Analysis Plugin:**
   
   **Malware Appliance Plugin:**
   
   **PocketShaper Plugin:**
   
   **Reporter Device Plugin:**
   
   **SG Device Plugin:**
   
   **SSLV Device Plugin:**

2. Specify the **Master Logging Level, General, and Device Plugin** settings.
3. Do one of the following:
   - Click **Save** to store the settings on the server.
     If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.
Required Ports, Protocols, and Services

Management Center uses the following ports while operating. Ensure that you allow these ports when setting up Management Center.

### Inbound Connections to Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>8080</td>
<td>TCP</td>
<td>No</td>
<td>User’s client</td>
<td>Management Center web console</td>
</tr>
<tr>
<td>SSL</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>User’s client</td>
<td>Management Center API</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>User’s client</td>
<td>Management Center CLI</td>
</tr>
<tr>
<td>SSL</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>User’s client</td>
<td>Management Center API</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9009</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics. Starting with Management Center 1.7, Port 9009 is disabled unless HTTP is enabled via the security http enable command.</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9010</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics over HTTPS</td>
</tr>
</tbody>
</table>

### Outbound Connections from Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>10389</td>
<td>TCP</td>
<td>Yes</td>
<td>LDAP server</td>
<td>Authentication</td>
</tr>
<tr>
<td>LDAPS</td>
<td>389</td>
<td>TCP</td>
<td>Yes</td>
<td>LDAP server</td>
<td>Authentication</td>
</tr>
<tr>
<td>Active Directory</td>
<td>10389</td>
<td>TCP</td>
<td>Yes</td>
<td>Active Directory server</td>
<td>Authentication</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1812</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Authentication</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1813</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Accounting</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>TCP</td>
<td>Yes</td>
<td>SMTP server</td>
<td>SMTP alerts</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>162</td>
<td>UDP</td>
<td>Yes</td>
<td>Trap receiver</td>
<td>SNMP traps</td>
</tr>
<tr>
<td>HTTP Proxy</td>
<td>8080</td>
<td>TCP</td>
<td>Yes</td>
<td>HTTP Proxy</td>
<td>Updates</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
<td>UDP/TCP</td>
<td>No</td>
<td>NTP server list</td>
<td>Time sync to customer-configured NTP time server</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Configurable?</td>
<td>Destination</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>-----------</td>
<td>---------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Symantec</td>
<td><a href="https://support.symantec.com">https://support.symantec.com</a> License activation, Web Application Protection (WAP) subscription, the latest release information and documentation</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP/TCP</td>
<td>No</td>
<td>DNS server</td>
<td>FQDN lookups</td>
</tr>
<tr>
<td>MA</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Malware Analysis</td>
<td>Health monitoring and backup</td>
</tr>
<tr>
<td>PacketShaper</td>
<td>80/443</td>
<td>TCP</td>
<td>No</td>
<td>PacketShaper</td>
<td>Health Monitoring (unencrypted/encrypted)</td>
</tr>
<tr>
<td>Reporter</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Reporter</td>
<td>Reporter API (unencrypted/encrypted)</td>
</tr>
<tr>
<td>ProxySG</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance monitoring and management</td>
</tr>
<tr>
<td>Management Center</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>Management Center</td>
<td>Management Center communication with failover partner</td>
</tr>
<tr>
<td>VPM</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>Visual Policy Manager</td>
</tr>
<tr>
<td>CA</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Content Analysis</td>
<td>Health Monitoring (unencrypted/encrypted)</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9009</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics. Starting with Management Center 1.7, Port 9009 is disabled unless HTTP is enabled via the security http enable command.</td>
</tr>
<tr>
<td>ProxySG</td>
<td>9010</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance</td>
<td>ProxySG appliance Performance Statistics over HTTPS</td>
</tr>
<tr>
<td>SSL Visibility</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>SSL Visibility</td>
<td>Health monitoring and configuration synch</td>
</tr>
</tbody>
</table>

**Required IP Addresses and URLs**

Ensure connectivity from Management Center to the following URLs.
## Determine Which Version You are Using

To aid in troubleshooting, you might need to determine the version and build of Management Center that is currently running.

Refer to the *Management Center Release Notes* to identify issues or limitations that your build might include.

1. In the web console banner, click > About. The web console displays the Management Center - About dialog. The dialog displays information about the Management Center version. See the table following this procedure.

<table>
<thead>
<tr>
<th>URL</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>199.116.168.195</td>
<td>TCP</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td>validation.es.bluecoat.com/phs.cgi</td>
<td>HTTPS</td>
<td>443</td>
<td>Validates the license every 5 minutes. After successful validation, validation occurs every hour.</td>
</tr>
<tr>
<td>bto-services.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Validates the license.</td>
</tr>
<tr>
<td>device-services.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>services.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>abrca.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Symantec CA.</td>
</tr>
<tr>
<td>appliance.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Trust package downloads.</td>
</tr>
<tr>
<td>subscription.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Subscription services.</td>
</tr>
<tr>
<td>upload.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Upload diagnostic reports to Symantec support.</td>
</tr>
<tr>
<td>sgapi.es.bluecoat.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Universal VPM policy.</td>
</tr>
</tbody>
</table>
Build Information Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The Management Center version.</td>
</tr>
<tr>
<td>Build</td>
<td>The number of the installed build.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the appliance.</td>
</tr>
</tbody>
</table>

Automate Password Reset Process

As an administrator on Management Center, you need to configure settings so that users can request a password reset if they forget their password.

1. Select Administration > Settings > General.
2. Set the Is Reset Password enabled? field to true.
3. For Reset Password Email Subject, modify the email subject line, if desired.
4. For Reset Password Email Message, modify the body of the email that is automatically sent to users when they click the Reset Password link. For example, you can add a person's name to the signature instead of the generic Management Center.
   - The message contains two substitution variables: {fullname} and {password}. Management Center automatically replaces {fullname} with the user's first and last name and replaces {password} with a temporary password.
5. Click Save to store the settings on the server.
6. Make sure an email server is configured. See "Configure Mail Settings" on page 528.
When the email is sent with the temporary password, the user’s account is marked so the administrators know that the password is only temporary. The temporary password will expire.
Prevent Licensing Issues on a Virtual Appliance

To prevent licensing issues, ensure that the VA is allowed network access to the license validation server at https://validation.es.bluecoat.com. See "Verify Web Console Access" on page 41.

If communication with the server fails, the license may be suspended. Unless you have purchased a VA offline license, constant Internet connection is required for Management Center to communicate regularly with the license validation server to confirm that the serial number is valid.

Duplicate Serial Numbers

If the license validation server detects duplicate serial numbers, your license is invalidated and the license health status goes to a critical state. Verify your license in NPLP and contact Symantec Support if you continue to have problems.

Expiring Licenses

Management Center health goes into a Warning state when the license is 30 days from expiring. For example, if the license will expire on January 30th, the Messages option in the web console banner displays Warning-level alerts, such as the following, starting on January 1st.

![License Alert]

Component 'Device Inventory' will expire on 2018-01-30

The web console banner displays an alert for each licensed component.

Once the license expires, Management Center goes into an Error state and remains in that state for another 15 days or until the license is updated (whichever occurs first). For example, starting on January 30th, the Messages option in the web console banner displays Warning-level alerts for each licensed component until the license is renewed. Once the license is renewed, the warning is marked as complete and removed from the Alerts page. See "Manage Alerts" on page 413 for more information.

If you do not renew the license within 15 days after the expiration date, you will be unable to load the web console. You must renew the license through the CLI using # license get-from-bluecoat or # license get-from-url.

Stop or Restart Services

To troubleshoot some issues, you might need to stop or restart Management Center services. You will need to restart the services after you install or update a Management Center license.

Stop Management Center Services

You can start or stop the Management Center, report generator, or statistics monitoring services.

1. "Access the Management Center CLI" on page 594.
2. Enter privileged mode by typing enable at the command prompt.
3. Enter your enable password and press Enter.
4. At the # prompt, type the following command and press Enter:
   
   ```
   # service stop-service [management-center | report-generator | statistics-monitoring ]
   ```
   
   The CLI displays the command prompt.

**Restart Services**

1. "Access the Management Center CLI" on page 594.
2. Enter privileged mode by typing `enable` at the command prompt.
3. Enter your enable password and press Enter.
4. At the # prompt, type `restart services` and press Enter.
   The CLI displays the command prompt.

⚠️ You cannot access the web console while the services are restarting; however, you can try accessing the web console a few minutes after issuing the command.

**Test Network Connectivity**

Verify that your network is set up correctly by using the `ping` command or the `tracepath` command in the CLI. Be sure to specify a hostname or IP address that you know is reachable and working.

1. "Access the Management Center CLI" on page 594.
2. Enter Privileged mode. "Privileged Mode Commands" on page 602.
3. Ping an IP address:
   ```
   # ping <hostname or IP address>
   ```
4. Trace the path between the host and a destination IP address:
   ```
   # tracepath <destination>
   ```

If you receive an error message, check your network configuration.
Upload System Diagnostics

To help Symantec Technical Support troubleshoot a Management Center issue, you can send diagnostics information to an external server using a supported protocol (FTP, HTTP, HTTPS, or SCP).

1. Log in to the CLI. See "Access the Management Center CLI" on page 594.
2. (If required) Enter the privileged mode password and press Enter.
3. Enter the appropriate command to upload the diagnostics:

   FTP

   # service upload-diagnotics ftp://<username:password>@host/path

   where <username:password> is the username and password to authenticate to the server and host/path is the path to where you want to save the file.

   HTTP

   # service upload-diagnotics http://host/path

   where host/path is the path to where you want to save the file.

   HTTPS

   # service upload-diagnotics https://host/path

   where host/path is the path to where you want to save the file.

   SCP

   # service upload-diagnotics scp://<username:password>@host/path

   where <username:password> is the username and password to authenticate to the server and host/path is the path to where you want to save the file.

   Using Your SR Case Number

   # service upload-diagnotics <case_number>

   Upload the diagnostics to Symantec Support with your existing case number.

View Hardware Diagnostics and Memory Resources

Use the Hardware Diagnostics screen to check on how much memory and storage space is being used by Management Center system components and processes. In addition, you can monitor various hardware sensors to spot potential problems with CPUs, fans, power supplies, and so forth (not applicable to virtual appliances).
Management Center Configuration & Management

- **System Metrics** – Details about memory usage of the CPUs and Management Center processes
- **Storage Usage** – Additional memory settings
- **Data Storage** – Amount of data used by each feature
- **Database Storage** – Amount of storage used for each database (Management Center, Device Statistics, Reporter)
- **Temperature Sensors** – The results of temperature monitoring for the chassis, CPU, and other components that produce heat in the appliance
- **RPM Sensors** – Reports the speed at which the fans on the appliance spin
- **Voltage Sensors** – Reports the voltage, status and state of components for which the appliance has a voltage sensor such as CPU cores, power supply, and others
- **Other Sensors** – Reports status of optional hardware components, such as extra power supplies

Byte counts for memory usage are approximations, not precise values.

To view hardware diagnostics for your appliance:

1. Select **Administration > Hardware Diagnostics**.
2. Click **Refresh** to view the most current appliance status totals and usage.
Problems and Errors

The following are error messages that you might encounter in Management Center.
Read Messages and Alerts

In the web console banner, the Messages icon displays alerts to communicate that a change was made, such as a confirmation of device activation. Alerts indicate the severity level of the change; for example, Messages displays a green Message-level alert when you add a device and a red Error-level message when device activation fails.

If you have unread alerts, the Messages icon in the banner displays the number of unread alerts and the status of the alert with the highest severity level.

To read messages, in the web console banner, click Messages.

To filter alerts, click Errors, Warnings, or Messages at the bottom of the dialog. To understand more about colors and status, see "About Color-Coded Status Indicators" on page 34.

"Could not enable statistics collection due to unexpected server failure" when activating a device

Problem: When you activate a device, you receive the alert "Statistics collection failed. Could not enable statistics collection on <device> due to unexpected server failure". When you added the device, you had selected Collect statistics for this device.

Resolution 1: Statistics collection requires SGOS 6.3.x. If the ProxySG appliance is not running SGOS 6.3.x or later, disable statistics collection by editing the device details and clearing Collect statistics for this device. You can enable statistics collection for the device again later if you upgrade SGOS to a supported version.

Resolution 2: Connection settings are incorrect. Verify device connection parameters and edit the device details.
"Import batch contains duplicate device name violation" when importing multiple devices

**Problem:** When you import devices, you receive the error "Import batch contains duplicate device name violation."

**Resolution:** Each device in the import file must have a unique name. Management Center detects duplicate device names even if you select only one or none of the devices for importing, and regardless of their placement in the hierarchy.

Rename duplicate devices in the import file and import them again. Alternatively, remove devices that you do not want to add from the file and import devices again.

"Local Changes Detected" error when installing policy

**Problem:** When you click **Install Policy**, the Policy Editor displays a **Local Changes Detected** message:

![Local Changes Detected](image)

**Resolution:** To resolve this conflict, click **Compare** to see the differences between the policy on the device and the policy you want to install. See "Compare the Device Policy Version with Current Policy Version" on page 332 for information.

Then, click **Install Policy** to overwrite the version on the device, or click **Cancel** to keep the version on the device.

User has "access denied" error when running a job

**Problem:** A user runs a job manually (through the **Run Now** option) or using the **Immediate** schedule option, but the job completes with an "access denied" error.

**Resolution:** Check the user's permissions; if they do not have sufficient permissions for the operation, they cannot run a manual or immediate job for the operation. For more information, see "Reference: Understanding Job Permissions" on page 352.

"Multi-tenant policy support is not enabled for this device" when installing policy

**Problem:** Attempts to install policy to a ProxySG appliance fail and you receive the message "Error: Multi-tenant policy is
Management Center Configuration & Management

not enabled for this device”.

**Resolution 1:** Multi-tenant policy was introduced in SGOS 6.6.x; if the device is running an earlier version of SGOS, you cannot install multi-tenant policy to it. If the device is running SGOS 6.6.x, proceed to the next resolution.

**Resolution 2:** The device does not have the Multi-Tenant Policy license or the license is invalid. If this is the case, contact your Symantec sales point of contact or Symantec customer care for assistance.

To determine if the appliance has the license:

1. Log in to the ProxySG Management Console.
2. Select **Maintenance > Licensing**.
3. In the list of Licensed Components, look for **Multi-Tenant Policy**. If the license is installed and valid, proceed to the next resolution.

**Resolution 3:** Multi-tenant policy is not enabled on the device. To enable it, enter the following commands:

```
# (config) general
# (config general) multi-tenant enable
ok
```

**Review Open Source Attributions**

This topic describes how to download the open source attributions used in Management Center.

1. Log into Management Center.
2. In the right-side of the banner, click the down arrow (highlighted below) > **About**.

3. Click **Legal Notices - Open Source Copyright Attributions**.
4. Click the link for the zip file and save it to local disk.
Organize Scripts by Attribute

This use case describes how to use attributes to logically organize your scripts. This technique can be useful when you have a large number of scripts and want to better organize them. Think of the attributes as folders for your scripts. By adding different attributes, you can organize your scripts in different ways.

In this example, we want to organize scripts by their purpose, but you can organize them in other ways as well.

1. Select Administration > Attributes > Device Scripts.
2. Click Add Attribute to create a new attribute definition.
The new attribute’s name is **Purpose** because we want to logically arrange the scripts by their purpose.

Ensure that **Displayed as a default column** is checked so this attribute will automatically display on the script list grid.

3. Click **Save**.

4. Select **Configuration > Scripts**. You will see the **Purpose** header on the grid.
If you want to move the **Purpose** column, you can drag it to a different position.

5. Hover the mouse cursor over the **Purpose** header to display the down arrow and click it.

6. Select **Group by this field**.
7. Select a script and click **Edit**.

8. Select the **Attributes** tab and enter a value in the **Purpose** field.
9. In this example, we have used **Test, Iteration 1**, and **Iteration 2**. You can see how the grid now organizes the scripts around their attribute values.

<table>
<thead>
<tr>
<th>Purpose: Iteration 1</th>
<th>ProxySG</th>
<th>1.4</th>
<th>admin</th>
<th>Iteration 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local_DB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose: Iteration 2</th>
<th>ProxySG</th>
<th>1.3</th>
<th>Admin23</th>
<th>Iteration 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>script1/test</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>script1/obj</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>script1/obj2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can also setup the attribute to be a picklist if you want to have predefined values.

**Restrict Access Only to a Specific Object Included in a VPM Layer**

This topic describes how to restrict user access to an object included in the VPM Web Access Layer. The intention of the policy is allow users to edit the whitelist, but preclude them from altering other policy in the VPM.

Although this can be accomplished with CPL, it is easier to create a shared object, restrict access to that object, and then include the object in the VPM policy.

**Step 1—Create the URL List Object**

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Fill in required fields. An asterisk denotes fields that are mandatory.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose **URL List**.
Step 1—Create New Shared Object

1. Select Configuration > Configuration & Management>
   Management Center Configuration & Management>
   Configuration & Management>
   Reference ID (*).
2. Enter a Reference ID that you can filter for when building policy.
   - The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
3. Description - Enter a meaningful description to help you when reusing this fragment.
4. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute’s value for this policy fragment. See “Add Attributes” on page 401.
5. Click Finish. The URL list displays in the editor.

Step 2—Add URLs

1. Select Configuration > Shared Objects.
2. Select or edit the desired URL list. The system displays the URL list editor.
3. Enter the URL in the URL field and click Add.
4. Alternatively, paste in multiple URLs:
   a. Create a URL list and copy the URLs.
   b. Click Paste URLs. The system opens the Paste URLs: Enter URLs dialog.
      
      ![Paste URLs dialog](image)

      c. Copy the URLs into the Paste URLs: Enter URLs dialog. Press CTRL+V or right-click and click Paste. The URLs are added to the list.
      d. Click Next. The system opens the Paste URLs: Validate dialog.
      e. Click Finish.

5. Click Save.

**Step 3—Add a Whitelist Editing Role**

1. Select Administration > Roles and click Add Role.

2. In the Add Role: Basic Info dialog, enter a name for the role. In this example, you might use "Whitelist Editor."

   ![Add Role: Basic Info dialog](image)

   If you authenticate users against LDAP, Active Directory or RADIUS, create a role in sync with the directory service.

3. (Optional) Enter a description.

4. Click Next.

5. In the Add Role: Permissions dialog, click Add Permission.

6. From the Object drop-down list, select Policy.

7. From the Action drop-down list, delete All Operations and select Edit Contents.

8. In the Filter drop-down list, select the URL whitelist you created in steps 1 and 2.
Step 4—Assign Users to the Whitelist Editing Role

1. Select Administration > Users.
2. In the Users left pane, select the user whose roles you want to change. The user’s details display.
3. Click Edit. The web console displays the Edit User dialog.
4. Click Assign Roles. The dialog displays a list of all the roles in the system. Roles to which the user is not assigned are listed under Available Roles. Roles to which the user is currently assigned are listed under Assigned Roles.
5. Select the Whitelist Editor role from Available Roles and, using the arrow, add it to the Assigned Roles list.

9. Click Finish.
6. Click **Save**. The web console banner displays an alert indicating that the user was saved.

Roles are linked to user sessions. If you edit users' roles while they are logged in to the web console, instruct them to log out and log in again to see the effects of the change.

**Step 5—Create the VPM Policy Object**

Skip to step 6 if you are going to add your URL list to an existing policy object.

To add a VPM policy object, complete the following steps.

1. Select **Configuration > Policy**.
2. Click **Add Policy**. The system displays the Create New Policy: Basic Information dialog. An asterisk denotes fields that are mandatory.
3. Enter a name for the policy object.
4. Select **VPM** for the **Policy Type**.
5. Enter a **Reference ID**. Although entering a reference ID is not required, it is useful for filtering objects when building policy. If you do not enter a reference ID, the system assigns a default ID based on the policy name you enter. Imported policy objects are assigned a default ID.

**The Reference ID must begin with a letter, and must contain only letters, numbers and "_".**

6. Enter a description in the **Description** field. Although entering a description is not required, the description helps differentiate versions of the same policy.
7. If you are to include shared objects, verify that **Replace Substitution Variables** is enabled. See "Use Substitution Variables in Policies and Scripts" on page 202 for more information.
8. Click **Next**.
9. Enter or select values for the defined attributes.
10. Click **Finish**.

**Step 6—Add the URL List to the VPM Policy**

On the desired line number, right click the field under **Destination** and select **Set** from the menu.

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Click the **Included Objects** tab.
4. Any lists already included in the policy show on the **Included Objects** list. You may only reference shared objects if they are associated with the policy. To add available lists:
   a. Click **Add Object**.
   b. Select the additional lists to add to the policy, then click **OK**.

   **You can search for lists using the **Keyword Search**.**

5. Make note of the reference ID for the object(s) you want to set.
6. (Optional) If you want to limit the lists to specific revisions in order to avoid unintentional changes, you can lock the revision version.
7. (Optional) Select any lists to remove and click **Delete**.

If any of the lists are in use, you need to launch the VPM Editor to remove or change the rules that reference them in the policy.

8. Once finished editing the available shared objects for the policy, click **Save**.
9. Click **Launch VPM Editor**.
10. Select or create the desired policy layer.
11. On the desired line number, right click the field under **Destination** and select **Set** from the menu.

12. Select the desired list:
• By the reference ID from the objects list.

• For a category, select any VPM object that lists categories. In this example, a new Request URL Category object is selected.
Shared objects are read-only. You cannot use the **Edit** option when setting the destination object. If you do try to edit it, it gets overwritten the next time you open the VPM editor.

13. (Optional) Set the desired action condition by right-clicking under the **Action** field.
14. When finished setting the destination and conditions, click **Save policy**. (Optional) To exit the VPM Editor without saving changes, close the VPM Editor and then click **Do not Save Policy**.
15. Enter a brief description of the policy changes in the **Save Changes** field, click **OK**, then click **Close**.
16. Close the VPM Editor.
17. Back in Management Center, on the VPM policy, click the **Info** tab.
18. Ensure that **Replace substitution variables** is selected, then click **Save**.

For more information about adding or editing VPM Shared Objects, see [Create Shared Objects](#).

You are now ready to install the policy. From this point on, any user with the correct permissions can edit the list as needed without having to open the VPM.
Management Center REST API

Management Center 1.6.1.1 and later include a new REST API. You can use this API if you want to access Management Center without using the UI or want to trigger Management Center operation without using the UI. This REST API has the ability to:

- Access and raise alerts.
- View registered devices, device health, and other monitoring variables.
- View jobs and job execution status.
- Start and cancel jobs.
- Show basic device information like version, disk usage, name of device.

No special policy or licensing is required to use this feature. API activities are recorded in the audit log.

Limitations

The REST API has the following requirements:

- JSON is the only supported payload.
- HTTPS is required to access the API.
- BASIC authentication is the only supported authentication method for providing user credentials for the API.
- You cannot add devices. A bulk device import already exists.

Documentation

Access the REST API documentation at the following URL:

https://MC_IP:8082/help/api

For example:

https://198.51.100.18:8082/help/api/

Or extract this archive package on your network or local workstation for offline viewing.

Troubleshooting

Confirm that the user has the proper permissions:

- REST API permissions (included in default administrator role).
- Appropriate permissions for the data or operation. For example, the user must have the Device permission if they want to use the Device API to list devices.
Management Center includes a command-line interface (CLI) that allows you to perform basic administrative tasks. A PDF of the Management Center CLI command documentation is available in the documentation section of the Symantec support site.

- "Access the Management Center CLI" on the next page—Describes how to access the CLI via an SSH connection.
- "CLI URL Syntax" on page 595—Describes the valid syntax for commands that require a URL path
- CLI Command Reference: List—Navigate links to view command descriptions and syntax.
Access the Management Center CLI

Log on to the CLI through an SSH connection or through the Management Center VMware console.

For hardware appliances, access the CLI through the serial console.

Log on using SSH

1. Install an SSH client. This procedure uses PuTTY as an example; your steps might be slightly different.
2. Open PuTTY and specify the following information:
   - **Host Name (or IP address)**—The IP address that you specified for
   - **Port**—22
3. (Optional) Specify a name for the connection and click Save to save the settings.
4. Click Open. The SSH window opens, with a login prompt.
5. At the login as: prompt, type admin and press Enter.
6. At the admin@IP_address's password: prompt, type your password and press Enter. The console displays the CLI banner.

Log on through the VMware console

Use the VMware console or SSH if you are logging into a Virtual Appliance.

1. In the VMware client, browse to the VM in the inventory.
2. Select the VM, right-click, and select Open Console.
   The console displays the CLI console and prompts you to press Enter three times.
3. Press Enter three times. The console displays the CLI banner.
CLI URL Syntax

All CLI commands that accept a URL as a download source or upload destination are formatted as:

```
protocol://host/path
```

For example, the SCP protocol must use the format:

```
scp://host/path
```

If path is a directory, it must end with a forward slash (/).

The following protocols are supported, although some commands do not support all of the protocols:

- `ftp://hostname[:port]/path`
- `ftps://hostname[:port]/path`
- `http://hostname[:port]/path`
- `https://hostname[:port]/path`
- `scp://hostname[:port]/path`

Notes

- URLs cannot contain spaces. If the hostname or path contains a space, you must use the URL-encoded characters instead: `%20`.
  
  For example, enter the following URL
  
  `http://yourserver.com/d/backup 2.tgz.gpg`

  as


- The `@` symbol is available for use in server credentials for the following commands:
  
  - `backup import`
  - `installed-systems add`
  - `license get-from-url`
  - `service upload-diagnostics`
  - `security ssl import server-certificate`
Standard Mode Commands

Standard mode is the default mode when you log onto the CLI. In standard mode, you can view configuration settings, but not change them.

> enable  .......................................................................................................................... 596
> exit .................................................................................................................................. 596
> help ................................................................................................................................... 597
> ping ................................................................................................................................... 597
> show .................................................................................................................................. 598
> tracepath .......................................................................................................................... 600

> enable

Use this command to enter privileged mode. Privileged mode commands enable you to view and change your configuration settings.

By default, you are not required to enter a password for privileged mode. You can configure a password for privileged mode using the #security enable-password CLI command.

See "Privileged Mode Commands" on page 602 for information on commands available in privileged mode.

Syntax
> enable

Example
Management Center> enable
Management Center#

> exit

Exit the CLI and return to the banner, where you can choose to enter the CLI or Management Center setup.

Syntax
> exit

Example
Management Center> exit
Copyright (c) 2015, Symantec Corporation.
Welcome to the Symantec Management Center CLI
Management Center Configuration & Management

Version: 1.3.0.2 Release id: 655010

-----------------------------------MENU-----------------------------------
1) Command Line Interface
2) Setup

-----------------------------------

Enter option:

> help

Display a list of all commands and a brief description of each. Alternatively, use ? to display the list.

This command is also available in privileged mode.

Syntax

> help

or

> ?

Example

Management Center> help
enable Turn on privileged commands
exit Exit command line interface
help (or ?) Display this help
ping Ping utility
show Show system information
tracepath Trace path utility

> ping

Verify whether a particular destination exists and is responding to requests by sending ICMP echo packets.

This command is also available in privileged mode.

Syntax

> ping <hostname or IP address>
Example

Management Center> ping 192.0.2.0

PING 192.0.2.0 (192.0.20.0) 56(84) bytes of data
64 bytes from 192.0.2.0: icmp_seq=1 ttl=125 time=6.43 ms
64 bytes from 192.0.2.0: icmp_seq=2 ttl=125 time=2.34 ms
64 bytes from 192.0.2.0: icmp_seq=3 ttl=125 time=2.71 ms
64 bytes from 192.0.2.0: icmp_seq=4 ttl=125 time=2.31 ms
--- 192.0.20.0 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.319/3.454/6.437/1.729 ms

> show

Display system information.
This command is also available in privileged mode.

Syntax

> show [subcommands]

Subcommands

> show clock

Displays the current system time information (time, date, and timezone) set for Management Center along with UTC time for reference. Works the same as > show timezone.

Example

Management Center> show clock
    UTC time : 2017-02-02 03:50:51+00:00 UTC
    Local time : 2017-02-02 03:50:51+00:00 UTC
    Timezone : UTC
    NTP : disabled

> show http-proxy

Displays HTTP proxy status (enabled or not) and configuration (host, port, user name, password).

> show installed-systems

Lists the images that are currently installed on the system and each image's software version number, release build number, and when the image was last booted.

> show interface

Displays interface and network settings, including IP address, subnet mask, gateway, and DNS servers.

> show license

Lists the component names of all licenses installed on the system and, for each license, displays the status (Valid, Invalid, Expired, Unknown), date the license was activated, expiration date, and type (such as Subscription or Demo).
Management Center Configuration & Management

> **show setupinfo**

Display system configuration, such as IP address and DNS servers. This reflects the settings specified during initial configuration of Management Center.

**Example**

Management Center> show setupinfo

Network settings:
- IP address: 10.169.21.51
- Subnet mask: 255.255.254.0
- IP gateway: 10.169.21.1
- DNS server: 10.167.4.55
- DNS server: 10.167.4.50
- NIC media setting: auto

HTTP Proxy settings:
- Enabled: false
- HTTP Proxy host:
- HTTP Proxy port:
- Username:
- Password:

> **show snmp**

Displays the community string and whether remote read access is enabled or disabled.

> **show status**

Displays the following system statistics (example only):

- Configuration
- General status
- RAID status (displays for HW appliances only)
- Service status

**Example**

Management Center> show status

Configuration:
- Memory installed: 7858 megabytes
- Memory free: 4388 megabytes
- CPUs installed: 2
- MAC: 00:50:56:b5:73:80

General status:
- System started: 2015-08-18 15:27:48UTC
- CPU utilization: 0

Service status:
- BCCM: start/running
- Statistics Monitoring: start/running

> **show timezone**
Displays the current system timezone information (time, date, and timezone) set for Management Center, along with UTC time for reference. Works the same as > show clock.

Example

Management Center> show timezone
   UTC time : 2017-02-02 03:50:51+00:00 UTC
   Local time: 2017-02-02 03:50:51+00:00 UTC
   Timezone : UTC
   NTP      : disabled

> show version

Display information such as system version, build version, and serial number.

Example

Management Center> show version
   Version:       Blue Coat Management Center 1.9.1.1
   Release id:    199309 x86_64 (Debug)
   Serial number: [###########]
   NIC 0 MAC:     00:00:00:AA:BB:CC

> tracepath

Identifies the route packets take to reach a destination. The command executes until the entire route to the host is traced; alternatively, you can press you press Control+C to return to the command prompt while the trace is in progress.

This command is also available in privileged mode.

Syntax

> tracepath <hostname or IP address>

Example

Management Center> tracepath google.com
   1: 192.0.2.0 (192.0.2.0) 0.131ms pmtu 1500
   1: server1-company.com (192.0.2.1) 0.725ms
   1: server1-company.com (192.0.2.1) 0.429ms
   2: 172.16.167.17 (172.16.167.17) 0.581ms
   3: 216.16.227.26 (216.16.227.26) 2.310ms
   4: network.net (216.16.232.121) 2.817ms
   5: 216.16.255.193 (216.16.255.193) 2.269ms
   6: 24.153.3.141 (24.153.3.141) 3.517ms
   7: 64.71.241.97 (64.71.241.97) 6.934ms
Management Center Configuration & Management

8: 69.63.248.89 (69.63.248.89) 19.716ms
9: no reply
Privileged Mode Commands

Privileged mode provides a set of commands that enable you to view, manage, and change configuration settings.

Enter privileged mode from standard mode by using the `enable` command. The prompt changes from a `>` to a `#`, indicating that you are in privileged mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># appliance-name</td>
<td></td>
</tr>
<tr>
<td># backup</td>
<td></td>
</tr>
<tr>
<td># clock</td>
<td></td>
</tr>
<tr>
<td># diagnostic-systems</td>
<td></td>
</tr>
<tr>
<td># disable</td>
<td></td>
</tr>
<tr>
<td># exit</td>
<td></td>
</tr>
<tr>
<td># failover</td>
<td></td>
</tr>
<tr>
<td># help</td>
<td></td>
</tr>
<tr>
<td># http-proxy</td>
<td></td>
</tr>
<tr>
<td># installed-systems</td>
<td></td>
</tr>
<tr>
<td># license</td>
<td></td>
</tr>
<tr>
<td># pcap</td>
<td></td>
</tr>
<tr>
<td># ping</td>
<td></td>
</tr>
<tr>
<td># restart</td>
<td></td>
</tr>
<tr>
<td># restore-defaults</td>
<td></td>
</tr>
<tr>
<td># rsyslog-output</td>
<td></td>
</tr>
<tr>
<td># security</td>
<td></td>
</tr>
<tr>
<td># service</td>
<td></td>
</tr>
<tr>
<td># show</td>
<td></td>
</tr>
<tr>
<td># shutdown</td>
<td></td>
</tr>
<tr>
<td># snmp</td>
<td></td>
</tr>
<tr>
<td># static-route</td>
<td></td>
</tr>
<tr>
<td># statistics-monitoring</td>
<td></td>
</tr>
<tr>
<td># subscriptions</td>
<td></td>
</tr>
<tr>
<td># tracepath</td>
<td></td>
</tr>
</tbody>
</table>
# appliance-name

Change the Management Center appliance name. Changing the appliance name updates all areas where the appliance name is referenced, including the CLI prompt and devices references, the hostname attached to syslog entries, and the SNMP sysname.

**Syntax**

```
# appliance-name [subcommands]
```

**Subcommands**

```
# appliance-name set <appliance_name>
```

Reconfigures the name of the appliance with one that you specify. `<appliance_name>` is the name of the appliance. The `<appliance_name>` must be between 1-64 characters in length and consist of the following character types: alphanumeric, hyphen, underscore, and periods.

When you set the appliance name, the CLI prompt changes to reflect the new name. For example:

Management Center# appliance-name set sv_lab_b
Changing the appliance name will restart the services.
Are you sure you want to change the appliance name? [y/N] y
Restarting services...
Success
sv_lab_b#

To restore the CLI prompt to "Management Center", enter the following command:

```
# restore-defaults configuration
```

**# appliance-name view**

Displays the current appliance name.

**Notes**

- Unless it is further changed by the user, the appliance name does not change after it has been manually configured except when Management Center is downgraded to a version that does not support a configurable appliance name.

- After upgrading from a build that does not allow appliance name configuration to one that does, the SNMP sysname defaults to 'BCMC' which differs from the default appliance name. The SNMP sysname will retain this value until an appliance name is configured, after which the SNMP sysname will correspond with the configured appliance name.
After downgrading to a build that does not allow appliance name configuration, the SNMP sysname defaults to 'BCMC' and the appliance name returns to the default value for that build.

The default appliance name for Management Center builds that do not support a configurable appliance name is based on the build version and changes when the user upgrades or downgrades the appliance.

The appliance name is not included with the backup data. You must manually configure the appliance name after restoring the appliance configuration.

After upgrading the appliance from a version that does not support appliance name configuration to one that does, the default appliance name will be the same as the default appliance name of the first image that was ever run. Exceptions to this are listed below and whichever occurred most recently will be the one in effect:

- A factory reset was previously executed while running image X: the default appliance name after the upgrade will be the appliance name from image X.
- The appliance was previously downgraded from an image Y that supported appliance name configuration to image Z that does not. In this instance the default appliance name after the current upgrade will be the same as the default appliance name of image Z.

Example of changing the appliance name to MC_One:

```
Management Center# appliance-name set MC_One
Changing the appliance name will restart the services.
Are you sure you want to change the appliance name? [y/n]
Updating sysname string to MC_One
Reloading snmpd:
```

# backup

Back up the Management Center configuration, and view, export, and restore existing backups.

Syntax

```
# backup [subcommands]
```

Subcommands

```
# backup create [full|partial]
# backup create full
Create a full system backup.
# backup create partial
Create a backup that does not include statistics monitoring trend data.
```

Back up the current Management Center configuration.

```
# backup delete <index_number>
```
Delete the specified configuration backup.

Use the backup view command to determine the index number to use.

```
# backup export <index_number> <URL>
```

Export the specified backup to a destination server. You must enter a passphrase to secure the backup.

Use the backup view command to determine the index number to use. `<URL>` is the URL of the destination server and path. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP. See "CLI URL Syntax" on page 595 for information on how to format the URL.

```
# backup import <URL>
```

Import a backup from the specified server. To import the backup, you must enter the passphrase that was specified during the backup export.

<URL> is the URL of the external server and path. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP. See "CLI URL Syntax" on page 595 for information on how to format the URL.

```
# backup restore <index_number>
```

Restore a Management Center backup, specified by the index number.

Use the backup view command to determine the index number to use.

```
# backup restore latest
```

Restore the most recent configuration backup.

```
# backup restore-data <index_number>|latest
```

Restore the configuration and data from a backup. Can be used to transfer configuration and data from one Management Center to another. The serial number, license, CLI password, and network configuration is not restored since this is not applicable when transferring the configuration and data to another unit.

```
# backup view
```

View existing configuration backups.

Transfer Configuration and Data to Another Appliance

To transfer configuration and data from one Management Center appliance to another:

1. On the first Management Center: use the backup create command to back up the configuration.
2. Use the backup export command to upload the backup to a Web, FTP, or SCP server.
3. Log in to the second Management Center appliance, and use the backup import command to download the backup from the server specified in step 2.
4. Restore the backup using the backup restore-data command.

Example

Management Center# backup view

Available Backups:

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-May-26 03:33:00 UTC</td>
<td>1.4.1.1 (555777)</td>
</tr>
</tbody>
</table>
# clock

View the system time settings in the Management Center configuration, and set the specific date and time it displays. The system time displays on various things that may include a timestamp to show the history of action, including:

- Management Center web console
- Policy object revision history
- Audit logging
- System logging
- Statistics monitoring

The system does not include clock settings in a backup of Management Center.

While Management Center uses the system (local) time, the timestamp may be displayed in the UTC timezone for some things. See `# timezone` for more information.

## Syntax

```
# clock [subcommands]
```

## Subcommands

```
# clock set [year|month|day|hour|minute|second] <number>
```

Set the local time on the Management Center system.

The CLI prevents any invalid entries. For example, if you are trying to enter in February 29th during a leap year (such as 2020), it works, but if it is entered for a year that is not a leap year (such as 2017), the system returns an error.

```
# clock view
```

Displays the current system time information (time, date, and timezone) set for Management Center, along with UTC time for reference. Works the same as `# show clock`, but is not available in disable mode.

## Examples

```
Management Center# clock view
  UTC time    : 2017-02-22 03:50:51+00:00 UTC
  Local time  : 2017-02-22 03:50:51+00:00 UTC
  Timezone    : UTC
  NTP         : disabled

Management Center# clock set day 23
Management Center# clock view
  UTC time    : 2017-02-23 03:51:31+00:00 UTC
  Local time  : 2017-02-23 03:51:31+00:00 UTC
  Timezone    : UTC
  NTP         : disabled
```
Management Center Configuration & Management

Management Center#  clock set day 29
29 is not valid for month(02) and year(2017). Acceptable value is between 1 and 28.
Failed to set system clock.

# diagnostic-systems
Upgrade and manage diagnostic systems. To switch between diagnostic and system images, press the SPACEBAR during the boot countdown.

⚠️ Upgrading and managing diagnostic systems is for Management Center hardware releases only.

Syntax

# diagnostic-systems  [subcommands]

Subcommands

# diagnostic-systems add <URL>
Downloads and installs the specified diagnostic image. The user is shown progress (bytes downloaded) which they can safely stop watching by entering Ctrl+C. They may resume watching the download progress by running diagnostic-systems view-downloads.

# diagnostic-systems view
Displays the list of diagnostic images installed on the appliance.

#diagnostic-systems view-downloads
Displays running progress of the diagnostic image currently being downloaded. If no image is being downloaded, it displays the status of the last download request. The user can stop watching the progress by entering Ctrl+C.

#diagnostic-systems delete <index>
Deletes the specified diagnostic image from the appliance. Locked systems cannot be deleted.

#diagnostic-systems lock <index>
Locks the specified diagnostic image, preventing it from being deleted.

#diagnostic-systems unlock <index>
Unlocks the specified diagnostic image, allowing it to be deleted.

# disable
Return to standard mode in the CLI.

Syntax

# disable
Example

Management Center# disable

# exit

Exit the CLI and return to the banner, where you can choose to enter the CLI or Management Center setup.

To return to standard mode from privileged mode, use the `disable` command. See "# disable" on the previous page for information.

Syntax

# exit

Example

Management Center# exit

Copyright (c) 2015, Symantec Corporation
Welcome to the Symantec Management Center CLI

Version: 1.4.1.1 Release id: 555000

---------------------------MENU---------------------------

1) Command Line Interface
2) Setup

---------------------------

Enter option:

# failover

Configures Management Center failover. Management Center supports failover using two physical appliances. One appliance is delegated as the `primary` and the other as the `secondary`. After failover is configured, the secondary replicates data from the primary appliance. During continuous replication, users can perform all normal operations on the primary failover partner. Users cannot access the secondary failover partner—its sole purpose is to replicate actions occurring on the primary node so that it can take over if something happens to primary node. See "Configure Management Center Failover" on page 550 for more information.

Syntax

# failover [subcommands]
Subcommands

# failover view
Display current failover settings.

# failover make-primary
Configures the appliance to be the primary partner in the failover group.

# failover make-secondary
Configures the appliance to be the standby partner in the failover group.

# failover disable
Disables all failover settings.

Example

# failover view
Failover:
Status: Healthy (0 second replication delay)
Primary: 198.51.100.20
Secondary*: 198.51.100.24

# help
Display a list of all commands and a brief description of each. Alternatively, use ? to display the list.
This command is also available in standard mode.

Syntax

#help
or
#

#?

Example

Management Center# help
backup Create, view and restore backups
disable Turn off privileged commands
exit Exit command line interface
help (or ?) Display this help
installed-systems Upgrade and manage installed systems
license Install and update the Management Center license
ping Ping utility
restart Restart the system or services
security Manage certificates, passwords and access to privileged commands
service Diagnostic and service support
show Show system information
tracepath Trace path utility

# http-proxy

Configure Explicit HTTP Proxy settings.

Syntax

# http-proxy [subcommands]

Subcommands

> show http-proxy
Display network settings and HTTP Proxy settings, such as IP address, DNS servers, HTTP Proxy host IP address and HTTP Proxy port number.

# http-proxy enable
Enables use of the proxy.

# http-proxy disable
Disables use of the proxy.

# http-proxy configure
Configures proxy settings, such as Proxy host, port, username and password.

Example

Management Center> http-proxy configure

Network settings:
IP address: 10.169.0.219
Subnet mask: 255.255.0.0
IP gateway: 10.168.0.1
DNS server: 1.1.1.1
NIC media setting: auto

HTTP Proxy settings:
Management Center Configuration & Management

Enabled: true
HTTP Proxy host: 10.168.0.207
HTTP Proxy port: 8080
Username: user1
Password: *****

# installed-systems

Upgrade and manage installed systems.

⚠️ Before upgrading the Management Center image, set the default system image to the currently running image.

Syntax

# installed-systems [subcommands]

Subcommands

# installed-systems add <URL>

Download and install a system image.

<URL> is the location on a server where image resides, in the following format:

http://host/path

# installed-systems default <index_number>

Specify the default system image. The default system image will be run after the next reboot.

<index_number> is the number of the image. Use installed-systems view command to determine the image to use.

# installed-systems delete <index_number>

Delete the specified system image.

<index_number> is the number of the image. Use installed-systems view command to determine the image to use.

# installed-systems view

Display the installed system images, with version, build number, and last boot time. The command also indicates the running image and default image, which will be run upon the next reboot.

# installed-systems view-downloads

View the progress of downloads in progress or the status of the last download. If no systems have been downloaded, the CLI responds No systems are being downloaded.

# installed-systems cancel-downloads
Management Center Configuration & Management

Cancel the progress of all downloads in progress. The CLI displays a list of active downloads, along with the message Are you sure you want to cancel image download? [Y/N]. If the download cancellation is confirmed, the CLI responds System image download canceled. If there are no downloads in progress, the CLI responds No image downloads in progress.

After the cancellation, use # installed-systems view-downloads to verify the information confirmation to continue with the cancellation or abort. If active downloads are canceled, if no systems have been downloaded, the CLI responds.

Example of canceled image download:

Management Center# installed-systems cancel-downloads
Are you sure you want to cancel image download? [Y/N] y
System image download cancelled.
Management Center# installed-systems view-downloads
Download URL: <URL>
Download Status: Download cancelled
Download bytes: 0

#installed-systems lock <index_number>
Lock the specified system image so that it cannot be deleted.

# installed-systems unlock <index_number>
Unlock the specified system image so that it can be deleted.

Example

Management Center# installed-systems view
Installed System Images:

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Last boot time</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>*1</td>
<td>1.4.4.1</td>
<td>2015-05-14 19:42:51 UTC</td>
<td>Locked</td>
</tr>
<tr>
<td>+2</td>
<td>1.4.0.1</td>
<td>2015-03-09 11:22:11 UTC</td>
<td>Unlocked</td>
</tr>
</tbody>
</table>

(*) running system image
(+): default system image (will be run on next reboot)

# license

Install a Management Center license or view the status of the last license download.

The CLI prompts you to enter your credentials when you install the license for the first time.

Syntax

#license [subcommands]
Subcommands

`#license get-from-bluecoat`

Install a new license or update the existing license from the Network Protection Licensing Portal (NPLP). The CLI only prompts you for your NPLP username and password if you are installing a new license on a VA appliance.

This command displays the download progress until download is complete.

`#license get-from-url <URL>`

Update the existing license from a license file on a local server. The command prompts for an optional passphrase, which is used to decode birth certificates embedded in license files.

This command displays the download progress until download is complete. See "CLI URL Syntax" on page 595 for information on how to format the URL.

`#license view`

View general information such as appliance serial number, information on licensed components, and status of the last attempted license download, including any download in progress.

If you are running a Management Center VA and have not purchased the Offline VA support option, issuing the `license view` command requires connectivity to the Symantec license validation server. If you issue the command without Offline VA support and Management Center is unable to contact the license validation server, the CLI displays the error:

"Cannot communicate with license validation server"

For more information, refer to the KB article You receive a "Cannot communicate with license validation server" error in Management Center.

⚠️ If you are running a version of Management Center that contains features available only through license components, contact your sales engineer to ensure that you have the correct license.

Example

Management Center# `license view`

General Information

Manufacturer: Bluecoat Systems Inc.
Serial Number: ##########
Appliance Number: MC-S400-20

License Component Information

<table>
<thead>
<tr>
<th>Status</th>
<th>Component Name</th>
<th>Activation</th>
<th>Expiration</th>
<th>License Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Management Center</td>
<td>2015-05-01</td>
<td>2016-04-30</td>
<td>Subscription</td>
</tr>
<tr>
<td>Valid</td>
<td>Performance Monitoring</td>
<td>2015-05-01</td>
<td>2016-04-30</td>
<td>Subscription</td>
</tr>
<tr>
<td>Valid</td>
<td>Device Configuration</td>
<td>2015-05-01</td>
<td>2016-04-30</td>
<td>Subscription</td>
</tr>
<tr>
<td>Valid</td>
<td>Device Inventory</td>
<td>2015-05-01</td>
<td>2016-04-30</td>
<td>Subscription</td>
</tr>
<tr>
<td>Valid</td>
<td>Policy Management</td>
<td>2015-05-01</td>
<td>2016-04-30</td>
<td>Subscription</td>
</tr>
</tbody>
</table>
The PCAP utility enables you to capture packets of Ethernet frames entering or leaving Management Center. Packet capturing allows filtering on various attributes of the frame to limit the amount of data collected. The collected data can then be transferred to the desktop for analysis via service diagnostic upload.

To view the captured packets, you must have a tool that can read Packet Sniffer Pro 1.1 files such as Wireshark or Ethereal.

Packet captures are limited to 100 MB. The files rotate once the 100 MB limit is reached.

**Syntax**

```
# pcap [subcommands]
```

**Subcommands**

```
# pcap filter
```

Specifies filters to use for PCAP. If you set a filter and subsequently change it while the PCAP is running, the change will not be applied until you restart the packet capture.

Subcommands:

```
# pcap filter clear
```

Clears all pcap filters.

```
# pcap filter set-host ipv4_address | hostname
```

Captures data only between Management Center and the specified host.

```
# pcap filter set-port port
```

Captures data only on the specified port.

```
# pcap filter view
```

Displays the filters currently enabled.

```
# pcap info
```

Reports current state of the packet capture.

```
# pcap start
```

Starts the capture.

```
# pcap stop
```

Stops the capture.
Management Center Configuration & Management

Example

Management Center# **pcap info**
Packet capture information:
Current state: Running
Filtering: port 80
Packets captured: 15020

# **ping**

Verify whether a particular destination exists and is responding to requests by sending ICMP echo packets.
This command is also available in standard mode.

Syntax

# **ping <hostname or IP address>**

Example

Management Center# **ping 192.0.2.0**
PING 192.0.20.0 (192.0.20.0) 56(84) bytes of data
64 bytes from 192.0.20.0: icmp_seq=1 ttl=125 time=6.43 ms
64 bytes from 192.0.20.0: icmp_seq=2 ttl=125 time=2.34 ms
64 bytes from 192.0.20.0: icmp_seq=3 ttl=125 time=2.71 ms
64 bytes from 192.0.20.0: icmp_seq=4 ttl=125 time=2.31 ms
--- 192.0.20.0 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.319/3.454/6.437/1.729 ms

# **restart**

Restart the Management Center VA or services.

Syntax

# **restart** [subcommands]

Subcommands

# **restart reboot**

Reboot the virtual appliance. When the appliance shuts down, the network connection closes and you must start a new CLI session.

# **restart services**

Restart Management Center services.
Example
Management Center\# \texttt{restart reboot}
Management Center\#

Broadcast message from admin@bccm_main-6-x86_64.localdomain

\begin{center}
(/dev/pts/0) at 23:27 ...
\end{center}

The system is going down for reboot NOW!

\section*{\# \texttt{restore-defaults}}

Restore factory defaults on the appliance/device running Management Center. This command is only available using the serial console.

Syntax
\begin{center}
\texttt{\# restore-defaults [subcommands]}
\end{center}

Subcommands
\begin{itemize}
\item \texttt{\# restore-defaults factory-defaults}
\begin{itemize}
\item Reboots the appliance/device after restoring factory defaults is complete.
\end{itemize}
\item \texttt{\# restore-defaults factory-defaults-halt}
\begin{itemize}
\item Halts the appliance/device after restoring factory defaults is complete.
\end{itemize}
\item \texttt{\# restore-defaults factory-defaults-shutdown}
\begin{itemize}
\item Powers off the appliance/device after restoring factory defaults is complete.
\end{itemize}
\item \texttt{\# restore-defaults reset-admin}
\begin{itemize}
\item Resets the UI admin password to admin/admin.
\end{itemize}
\item \texttt{\# restore-defaults configuration}
\begin{itemize}
\item Resets the UI configuration back to defaults. Retains all other data.
\end{itemize}
\end{itemize}

Example
Management Center \# \texttt{restore-defaults reset-admin}

This operation will restore admin password on UI to default. Management Center service will be unavailable during this operation.

Are you sure you want to restore UI admin password? [y/N]

\section*{\# \texttt{rsyslog-output}}

Configure the remote servers where remote syslog output can be sent.
Management Center Configuration & Management

Syntax

# rsyslog-output [subcommands]

Subcommands

# rsyslog-output add
Add new syslog server configuration.

# rsyslog-output configure
Configure existing syslog server.

# rsyslog-output delete
Delete syslog server configuration.

# rsyslog-output disable
Disable use of remote syslog output.

# rsyslog-output enable
Enable use of remote syslog output.

# rsyslog-output view
View configured syslog servers.

Examples

Management Center# rsyslog-output add
   Enter syslog server host []: my-remote-host
   Enter syslog server port [514]:
   Enter syslog server protocol (TCP|UDP) [TCP]:

Management Center# rsyslog-output disable

Management Center# rsyslog-output view

Warning - Remote syslog server output is disabled.

<table>
<thead>
<tr>
<th>Host</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>my-remote-host</td>
<td>514</td>
<td>UDP</td>
</tr>
</tbody>
</table>

Management Center# rsyslog-output delete 1

   Remove syslog server configuration (Host "my-remote-host", Port 514, Protocol UDP)? [y/N] y

# security

Specify security options for Management Center including basic certificate management using ssl.
Syntax

# security [subcommands]
# security ssl [subcommands]

Subcommands

# security allowed-hosts

Subcommands:

  # security allowed-hosts add
  # security allowed-hosts delete
  # security allowed-hosts view

Limits access to a specific host such that it can be accessed only by the specified hostname, and not its IP address. For example, consider a Management Center instance with the following properties:

- Hostname: mc.example.com
- IP address: 192.0.2.10

The administrator then enters the following command:

# security allowed-hosts add mc.example.com

After the preceding command is run, users will only be able to access the Management Center by typing mc.example.com in the browser address bar. If users type 192.0.2.10 in the address bar, they will receive a 403 Forbidden error.

You can also specify an IP address instead of a hostname. If you specify an IP address, users can only access the device using the IP address and will receive an error if the hostname is used.

The security allowed-hosts command has no effect on Management Center failover pairs.

# security enable-password

Turns on the password for privileged commands. If you turn on the password, you must enter an enable password to enter privileged mode.

<password> is the enable password you specify.

# security generate-ssl-certificate

Generate a new SSL certificate for Management Center. When an SSL certificate expires, you can use this command to generate a new one.

If you change the SSL certificate, statistics monitoring will fail unless you install the certificate on your monitored appliances. See Statistics Monitoring Over HTTPS for more information.

# security http

Subcommands:
### Management Center Configuration & Management

```bash
# security http enable
# security http disable
# security http view
```

Enables or disables HTTP access to port 8080. The command also controls access to statistics monitoring port 9009. By default, HTTP is disabled. You can enable HTTP in the following cases:

- You want to install system images without a secure connection on managed devices.
- You want to monitor appliances over HTTP port 9009.

```bash
# security icmp
```

Subcommands:

```bash
# security icmp enable
# security icmp disable
```

Enables or disables ICMP echo. By default, ICMP is disabled. Management Center will respond to pings after ICMP is enabled.

```bash
# security password
```

Change the password used to access the CLI. To change the password, you must enter the current password, and then specify and confirm the new password.

```bash
# security reset-password
```

Resets the password used to access the CLI for the admin account. This command is only available through the serial console. To restore the default password for the admin UI account, see "# restore-defaults" on page 616.

```bash
# security unset-enable-password
```

Turns off the password for privileged commands. If you turn off the password, you can enter privileged v1.0 mode without having to enter an enable password.

```bash
# security ssl
```

Subcommands:

```bash
# security ssl client-authentication disable
```

Disable X.509 client authentication.

```bash
# security ssl client-authentication password-requirement
```

Subcommands:

```bash
# security ssl client-authentication password-requirement enable
# security ssl client-authentication password-requirement disable
```

Enables or disables the requirement for users to enter their password during SSL mutual authentication. The behavior is as follows:
- **enable**: All users are forced to enter their password when accessing Management Center.
- **disable**: When the password requirement is disabled, a user does not have to enter a password to access Management Center if the system determines the certificate is valid, and finds the user in the local user database or the LDAP system, if configured.

The default is **enable**.

This method only supports the local or LDAP authentication schemes. You can use active directory but only if you set it up using the LDAP settings (Administration > Settings > LDAP). This is because a service account is needed to look up users because the system no longer has the user password.

To validate certificates, you must create a regular expression to evaluate the information in the certificate's SubjectAltName field. The subjectAltName data is compared to a regex set by the `security ssl client-authentication set-regex` command, which is used to extract the portion of the value to use as the user's identity. That value is then used to find the user in the local or LDAP authentication service. Refer to the following for more information:

- "# security ssl client-authentication set-regex" below
- "Use Certificate Subject Alternative Name Data for Certificate Validation" on page 370
- "Authenticate Users with SSL Mutual Authentication" on page 366

# security ssl client-authentication set-mandatory

Users must use X.509 client authentication. If X.509 client authentication fails, no connection is established.

When configured, all traffic requires a certificate. For example, to access file service requests and API’s, client authentication is mandatory.

#security ssl client-authentication set-optional

If X.509 client authentication fails, users can log in using the standard Management Center login page. Issuing this command requires Management Center to restart.

# security ssl client-authentication set-regex

Sets the regex command used to extract the certificate's name or data set in the certificates Subject Alternative Name (`subjectAltName`); the default is `CN=(.*?), .`

Subcommand:

**default**

Resets the principal regex to the default.

Subject alternative name example:

- "# security ssl client-authentication set-regex" below
- "Use Certificate Subject Alternative Name Data for Certificate Validation" on page 370 for more information.

# security ssl client-authentication view
View current X.509 client authentication settings.

```
# security ssl import external-certificate <name> <URL>
```

Downloads the certificate from the specified URL and installs it to the truststore with the specified name. Certificates are not case sensitive. See “CLI URL Syntax” on page 595 for information on how to format the `security ssl import external-certificate <name> <URL>`.

```
# security ssl import server-certificate <URL>
```

Downloads the certificate from the specified URL and installs it to the keystore, replacing the appliances SSL certificate if it exists. This command does not restart the MC services; users must do so manually by running `restart services`. See "CLI URL Syntax" on page 595 for information on how to format the URL.

If you change the SSL certificate, statistics monitoring will fail unless you install the certificate on your monitored appliances. See Statistics Monitoring Over HTTPS for more information.

```
# security ssl list external-certificates all
```

Displays the names of all certificates in the truststore. Certificate names are not case sensitive.

```
# security ssl list external-certificates system
```

Displays the names of all system certificates in the truststore. Certificate names are not case sensitive.

```
# security ssl list external-certificates user
```

Displays the names of all user added certificates in the truststore. Certificate names are not case sensitive.

```
# security ssl list server-certificates
```

Displays the names of all server certificates in the keystore. Currently, there will only ever be one, and it will be named `defaultcertkey`.

```
# security ssl delete external-certificate <name>
```

Delete the specified certificate from the truststore. System certificates cannot be deleted.

```
# security ssl delete server-certificate
```

Deletes the appliances certificate being used for SSL. This command does not restart the MC services; users must do so manually by running `restart services`.

```
# security ssl view external-certificate <name>
```

Displays details of the certificate in the truststore with the given name. Details include owner, issuer, expiration date and fingerprints. Certificate names are not case sensitive.

```
# security ssl view server-certificate
```

621
Displays details of the certificate in the keystore with the given name. Details include owner, issuer, expiration date and fingerprints. Certificate names are not case sensitive.

```
# security ssl hsts enable
```

Enables the HTTPS Strict Transport Security (HSTS) protocol.

```
# security ssl hsts disable
```

Disables the HTTPS Strict Transport Security (HSTS) protocol.

Example

```
Management Center # security unset-enable-password
```

```
Management Center #security ssl import external-certificate < name> <URL>
```

1. Import an external certificate from a server using the public key. This allows Management Center to connect to an external server without using a username or password for authentication.

2. Name the certificate.

3. Go to the URL of the server, and copy and paste the URL into the subcommand.

4. Click Return. While the certificate downloads, the CLI displays the details of the connection to the server and inspects the certificate for details such as:
   - Owner
   - Issuer
   - Serial Number
   - Valid from date
   - Valid until date
   - Certificate fingerprints
   - Extensions

   When the download is complete, the CLI queries:

```
Are you sure you want to import this as a trusted certificate? [y/N]
```

```
# service
```

The service command allows you to view disk usage and troubleshoot the following:

- Disk space or possible file corruption issues
- Enable verbose logging
- Upload diagnostic data to Symantec using an open support case
- Possible VPM cache corruption issues
Perform Disk Maintenance

Clean your disk by using the `service db-maintenance` command and subcommand. This is used for manual database cleanup and re-indexing. While running this maintenance command, both Management Center and statistics monitoring are unavailable.

**Syntax**

```
#service db-maintenance
```

Automated disk space cleanup occurs when Management Center reaches 85% of disk utilization. This automated cleanup removes backed up dump files and all but the latest Management Center backup. This automated cleanup is not as thorough as performing disk maintenance manually. Management Center and statistics monitoring remain available and running.

Enable Verbose Logging

To enable verbose debug logging, execute the command `service enable-verbose-logging`. When you have completed capturing what you want, stop the logging by executing the command `service disable-verbose-logging`. You can then export the debug log from the web console or include the log in a support case upload.

**Syntax**

```
#service enable-verbose-logging
#service disable-verbose-logging
```

You should enable verbose logging to include more debug-level details in system logs, which can be used to troubleshoot issues you may have encountered. Because the system log is included in the diagnostics upload to Symantec Support, enabling verbose logging includes debug-level logs in the diagnostics archive.

View Disk Usage

View your current disk usage before performing disk maintenance.

**Syntax**

```
#service disk-usage
```

Purge VPM Cache

If you receive a message when starting the Visual Policy Manager Editor from the web console that a jar mismatch exists, you will need to purge the VPM cache. This happens rarely, such as if there is a network failure while jars are being transferred between devices.

Purge all Visual Policy Manager .jar files by using `purge-vpm cache` command.

**Syntax**

```
#purge-vpm cache
```
Rebuild Repository Index

Run this command to restore the structure of system indexes for device backups, scripts, or policy objects as directed by Symantec support personnel.

Syntax

```
#service rebuild-repository-index
```

Start or Stop Service

Start or stop Management Center services.

```
#service stop-service [management-center | report-generator | statistics-monitoring ]
```

Stops the specified service.

```
#service start-service [management-center | report-generator | statistics-monitoring ]
```

Starts the specified service.

Use the `show status` command to view the current status of the services.

```
Management Center# show status
Configuration:
Memory installed: 7858 megabytes
Memory free: 3274 megabytes
CPUs installed: 2
MAC: 00:50:56:b5:8a:e1
Birth Certificate: Installed
General status:
System started: 2017-02-24 06:50:58MST
CPU utilization: 0
Service status:
  BCCM : start/running
  Statistics Monitoring : start/running
  Report Generator : stop/waiting
Failover:
  Status: Disabled
```

Upload Diagnostics Data

Upload diagnostics data to a destination server or directly to Symantec if you have an open support case.

Syntax

```
#service upload-diagnostics [subcommands]
```

Subcommands

```
# service upload-diagnostics [subcommands]
```
Management Center Configuration & Management

SCP: scp://<host>/<path>
FTP: ftp://<host>/<path>
FTPS: ftps://<host>/<path>
HTTP: http://<host>/<path>
HTTPS: https://<host>/<path>

# service upload-diagnostics <case_number>

Upload the diagnostics to Symantec Support with your existing case number.

<case_number> is the number for your open Symantec Support case.

# show

Display system information.

This command is also available in standard mode.

Syntax

# show [subcommands]

Subcommands

# show clock

Displays the current system time information (time, date, and timezone) set for Management Center along with UTC time for reference. Works the same as # show timezone. It is also similar to # timezone view and # clock view, with the exception that # show clock works in disable mode and these other two cannot.

Example

Management Center # show clock
UTC time : 2017-02-02 03:50:51+00:00 UTC
Local time : 2017-02-02 03:50:51+00:00 UTC
Timezone : UTC
NTP : disabled

# show http-proxy

Displays HTTP proxy status (enabled or not) and configuration (host, port, user name, password).

# show installed-systems

Lists the images that are currently installed on the system and each image's software version number, release build number, and when the image was last booted.

# show interface

Displays interface and network settings, including IP address, subnet mask, gateway, and DNS servers.

# show license
Lists the component names of all licenses installed on the system and, for each license, displays the status (Valid, Invalid, Expired, Unknown), date the license was activated, expiration date, and type (such as Subscription or Demo).

```
# show setupinfo
```

Display system configuration, such as IP address and DNS servers. This reflects the settings specified during initial configuration of Management Center.

**Example**

```
Management Center# show setupinfo

Network settings:
  IP address:              10.169.21.51
  Subnet mask:             255.255.254.0
  IP gateway:              10.169.21.1
  DNS server:              10.167.4.55
  DNS server:              10.167.4.50
  NIC media setting:       auto

HTTP Proxy settings:
  Enabled:                 false
  HTTP Proxy host:         
  HTTP Proxy port:         
  Username:                
  Password:                
```

```
# show snmp
```

Displays the community string and whether remote read access is enabled or disabled.

```
# show status
```

Displays the following system statistics (example only):

- Configuration
- General status
- RAID status (displays for HW appliances only)
- Service status

**Example**

```
Management Center# show status

Configuration:
  Memory installed:    7858 megabytes
  Memory free:         4388 megabytes
  CPUs installed:      2
  MAC:                 00:50:56:b5:73:80

General status:
  System started:      2015-08-18 15:27:48UTC
  CPU utilization:     0

Service status:
  BCCM : start/running
  Statistics Monitoring : start/running

Resync Status: 5 % complete
```
Management Center Configuration & Management

Name: raid1
UUID: asldfkjalkdfkljkkjkwjf:044a840:18765bvjdc
Events: 5

# show timezone

Displays the current system timezone information (time, date, and timezone) set for Management Center, along with UTC time for reference. Works the same as # show clock. It is also similar to # timezone view and # clock view, with the exception that # show timezone works in disable mode and these other two cannot.

Example

Management Center# show timezone
UTC time    : 2017-02-02 03:50:51+00:00 UTC
Local time  : 2017-02-02 03:50:51+00:00 UTC
TimeZone    : UTC
NTP         : disabled

# show version

Display information such as system version, build version, and serial number.

Example

Management Center# show version
Version: Blue Coat Management Center 1.9.1.1
Release id: 199309 x86_64 (Debug)
Serial number: [##########]
NIC 0 MAC: 00:00:00:AA:BB:CC

# shutdown

Shut the hardware or virtual appliance down.

Syntax

# shutdown

Example

Management Center# shutdown
Are you sure you want to shutdown the system? [y/N]

# snmp

Enables you to disallow remote read access or only allow read-only remote access. You can set the community string and view the SNMP settings for SNMP traps.

You can view SNMP settings in the standard "> show" on page 598 command.
Syntax

# snmp [subcommands]

Subcommands

# disable-remote-read-access
Disallows remote read access

# enable-remote-read-access
Allows read-only remote access.

# set-community
Set the community string (you cannot use the default).

# view
View SNMP settings.

Example

Management Center# snmp view
Community String: 2cc72a6160
Remote Read Access: Disabled

# static-route
Configures the static network route settings for available network interfaces. The static routes are made up of destination IP addresses, subnet masks, and gateway IP addresses.

Syntax

# static-route [subcommands]

Subcommands

# static-route add <nic_interface>
Adds a static network route entry to the specified NIC interface.

# static-route delete <nic_interface> <staticroute_entry>
Deletes the specified static network route entry.

# static-route update <nic_interface> <staticroute_entry>
Reconfigures the specified static network route entry.

# static-route view <nic_interface>
Displays the static network route entries for the available NICs. Specifying the <nic_interface> will display all the static route indexes created for a given NIC.
Example of adding a static network route entry to nic0_0:

Management Center# static-route add nic0_0
Enter the IP address for destination network []: 172.16.50.1
Enter the subnet mask for destination network []: 255.255.255.0
Enter the IP address for gateway []: 172.16.50.254

# statistics-monitoring

Shut the hardware or virtual appliance down.

Syntax

# statistics-monitoring [subcommands]

Subcommands

# statistics-monitoring set-per-hour-lifetime

Set per hour trend data lifetime. Must be entered in number of days.

# statistics-monitoring set-per-minute-lifetime

Set per hour trend data lifetime. Must be entered in number of days.

# statistics-monitoring view

View current statistics monitoring lifetime settings, record statistics, and disk usage data.

Example

# statistics-monitoring view
Total devices: 2
Reporting devices: 1

Data characteristics:
Lifetime Records Disk Usage
minute 7 days 131240 113 MB
hour 366 days 50927 26 MB

# subscriptions

Download and view the current status of Symantec subscriptions.

In Management Center 1.6.1.1, the subscriptions command controls only the Web Application Protection (WAP) subscription. To use Web Application Firewall (WAF) features, you must ensure that Management Center can connect to https://subscription.es.bluecoat.com to download the WAP subscription bundle. If the WAP subscription cannot be downloaded, the Blacklist and Analytics Filter rules table in the Security Profile will not be
available. However, all other WAF features should still be available and functioning. The WAP subscription cannot currently be loaded when Management Center is in offline mode.

Syntax

`subscriptions [subcommands]`

**Subcommands**

`subscriptions application-protection`

Downloads the application-protection subscription update.

`subscriptions application-protection download-force`

Downloads the application-protection subscription update, even if an instance of the identical update already exists.

`subscriptions application-protection view`

View the application-protection status.

**Example**

Management Center# `subscriptions application-protection view`

License Type: Subscription

Licensed Until: 2017-01-05

Subscription Validity: Valid

Data Validity: Valid

Last Download Information:

Time: 2016-03-08T14:54:30.944+0000

URL: https://subscription.es.bluecoat.com/application-protection/database

Status: Success

The download URL is not configurable.

**# tracepath**

Identifies the route packets take to reach a destination.

The command executes until the entire route to the host is traced; alternatively, you can press you press Control+C to return to the command prompt while the trace is in progress.

This command is also available in standard mode.

**Syntax**

`# tracepath <hostname or IP address>`
Example

Management Center# tracepath google.com
1: 10.169.21.52 (10.169.21.52) 0.131ms pmtu 1500
1: server1-company.com (10.169.21.1) 0.725ms
1: server1-company.com (10.169.21.1) 0.429ms
2: 172.16.167.17 (172.16.167.17) 0.581ms
3: 216.16.227.26 (216.16.227.26) 2.310ms
4: network.net (216.16.232.121) 2.817ms
5: 216.16.255.193 (216.16.255.193) 2.269ms
6: 24.153.3.141 (24.153.3.141) 3.517ms
7: 64.71.241.97 (64.71.241.97) 6.934ms
8: 69.63.248.89 (69.63.248.89) 19.716ms
9: no reply

# verify-hardware

Displays all hardware system information for the appliance running Management Center. This command helps when diagnosing any problems encountered during installation or initial configuration.

Syntax

# verify-hardware [subcommands]

To diagnose problems with the hardware, see "# diagnostic-systems" on page 607

Example

Management Center #verify-hardware
Serial number: 4313320063
System model: Symantec 1000
RAM:
  16384 MB
  CPU0_DIMM_A1 8192 MB DDR3
  CPU0_DIMM_A2 8192 MB DDR3
Number of physical CPUs: 1
Number of cores: 4
CPU Type: Intel(R) Xeon(R) CPU E5-2418L 0 @ 2.00GHz

631
Storage:
- sda 7 GB ATP IG SlimSATA
- sdb 7 GB ATP IG SlimSATA
- sdc 1000 GB ST91000640SS
- sdd 1000 GB ST91000640SS
- sde 1000 GB ST91000640SS
- sdf 502 MB ATP IG eUSB

Network: nic0_0 Intel Corporation I350 Gigabit Network Connection (00:d0:83:09:6b:c4)

# timezone

View the clock timezone settings in the Management Center configuration, and set the specific timezone it displays. This affects any logging process that uses system time. Changing the Management Center system timezone using this command should not affect the dates or times shown in the web console.

The system does not include timezone settings in a backup of Management Center. A system reset to default settings restores the timezone to the default timezone (UTC).

Syntax

# timezone [subcommands]

Subcommands

# timezone list [<area>|<area/location>]

Search for available timezones in specific areas.

An incomplete entry searches for items beginning with the last letter entered. The command executes with or without an argument ( [<area>|<area/location> ]). Without an argument, the timezone areas show. With an argument, one of four things happen:

- If you specify an area, it shows all timezones in that area.
- If the search string matches only one timezone, it shows the local time for that match.
- If the search string matches multiple timezones, it shows the timezones that match.
- If the search string does not match any of the known valid timezones, the user receives a message that no matches are found.

# timezone set [<area>/<location>]

Sets the local timezone for the system.

The CLI automatically completes an entry if only one timezone matches from the list of valid timezones shown from the # timezone list command. The system only allows a timezone to be set if it is in the available list. Any other values are rejected.

Using this subcommand restarts any Management Center services, such as the UI, statistics monitoring, and system logging. If you attempt to set the timezone to the one already being used, the system informs you that it is already set and the command does not make changes or restart any services.
Management Center Configuration & Management

# timezone view

Displays the current system timezone information (time, date, and timezone) set for Management Center, along with UTC time for reference. Works the same as `show timezone`, but is not available in disable mode.

Examples

Management Center# timezone list
Africa
America
Antarctica
Arctic
Asia
Atlantic
Australia
Europe
Indian
Pacific
UTC

Management Center# timezone list america/d
America/Danmarkshavn
America/Dawson
America/Dawson_Creek
America/Denver
America/Detroit
America/Dominica

Management Center# timezone set america/denver
Management Center# timezone view
   UTC time : 2017-02-22 20:19:54+00:00 UTC
   Local time : 2017-02-22 13:19:54-07:00 MST
   Timezone : America/Denver
   NTP : disabled

Management Center# timezone set denver
'denver' is not a valid time zone.
(Use "timezone list" for supported time zones)
Failed to set system time zone.

Management Center# timezone set america/den
Time zone is already set to 'America/Denver'

Management Center# timezone set america/da
'americad/a' is not a valid time zone.
Possible matching time zones are:
America/Danmarkshavn
America/Dawson
America/Dawson_Creek
(Use "timezone list" for supported time zones)
Failed to set system time zone.
Management Center# timezone view
UTC time : 2017-02-23 03:51:31+00:00 UTC
Local time : 2017-02-23 03:51:31+00:00 UTC
Timezone : UTC
NTP : disabled