

Symantec Management Center Configuration & Management Guide

Management Center v2.4.1.1
Guide Revision: 4/8/2020



Management Center Configuration & Management

TOC

Management Center Overview	25
Access Management Center Software Downloads and Documentation	27
Product Documentation	27
Release Notes, Software Images, MIBs	27
<i>Download Software</i>	27
Contact Us	28
Web Console Overview	29
<i>Dashboard</i>	30
<i>Network</i>	31
<i>Configuration</i>	31
<i>Jobs</i>	31
<i>Reports</i>	31
<i>Administration</i>	32
<i>Example</i>	33
Log into the Web Console	35
Navigate the Web Console	37
Verify Web Console Access	39
Move Items	40
<i>Drag an Item From One Area to Another</i>	40
<i>Drag a Selected Device to a Device Group</i>	41
Date Filters	42
Required Ports, Protocols, and Services	43
<i>Important Notice</i>	43
Inbound Connections to Management Center	44
Outbound Connections from Management Center	44
Required IP Addresses and URLs	46
Access the Management Center CLI	46
<i>Requirements</i>	47
<i>Procedure</i>	47
Encrypt Sensitive System Data	47
<i>Caution: Potential Data Loss</i>	48
Special Character Replacement	49
Management Center Solutions	51
Manage Devices	52

Add and Monitor Devices	52
Customize the Network View	54
Configure Device Connection Security Level (SSL Context)	58
<i>Pre-Configured SSL Contexts</i>	59
<i>Specify an SSL Context</i>	59
<i>Create an SSL Context</i>	60
<i>Verify Certificate Trust</i>	60
<i>Example</i>	60
<i>Edit an SSL Context</i>	60
<i>Delete an SSL Context</i>	60
<i>FIPS Mode Considerations for SSL Context</i>	61
Resolve Device Errors	61
<i>Are Any Devices in an Error State?</i>	61
<i>Which Devices are in an Error State?</i>	61
<i>What Exactly is the Error on the Device?</i>	62
<i>Changes in Management Center 1.9.x and Later (Device Serial Number Errors)</i>	63
Reactivate Statistics Monitoring	63
<i>Schedule</i>	64
<i>Event</i>	64
Add Multiple Devices at Once	66
<i>Import Devices Using a CSV File</i>	66
<i>Determine Your Next Step</i>	68
View and Edit Device Information	69
<i>Determine Your Next Step</i>	72
Verify Device Details	73
View Device Certificate Data	73
<i>Important Notes</i>	73
<i>View Certificate Data</i>	74
<i>View Individual Device Certificate Data</i>	75
Perform an Operation on a Managed Device	77
Collect Device Certificates	78
<i>Schedule</i>	79
<i>Event</i>	80
Launch a Device Console	81
Install the ProxySG Admin Console	82
<i>Admin Console Requirements</i>	83
<i>Admin Console Notes</i>	83
<i>Step 1—Download the Admin Console Installation Package</i>	83
<i>Step 2—Install the Installation Package on Management Center</i>	84
<i>Step 3—Launch the Admin Console</i>	85
Access the CLI of a Managed Device	85
Set Boot Image	88
<i>Schedule</i>	90

Event	90
Upgrade System Images on Managed Devices	91
Restrictions	91
Install System Image	92
Schedule	94
Event	95
Troubleshooting	95
Restart a Device	95
Compare Device Configurations	96
Schedule	98
Event	99
Viewing Notes	100
Remove Unused Tenant Policy	100
Search for Managed Devices	102
Search by Name or IP Address	102
Browse the Hierarchy	102
Configure Hierarchy for Devices and Device Groups	103
Change Device Password	107
Device Notes	107
Change Password	108
Synchronize Devices	109
Important Notes	109
What to Synchronize	110
Advanced Synchronization Options	110
Schedule	114
Event	114
Purge Statistics	115
Put Device in Read-Only Mode	117
Stop Managing a Device	120
RMA a Device	121
View Security Analytics API Key	122
Retrieve the API key	123
Reference: Device Communication	123
ProxySG Appliance SSH Ciphers	123
All Other Appliances	123
Supported Key Exchange in Management Center Operations that use SSH/SCP	124
Receive Alert Error Notifications	124
Management Center Alerts	124
Alerts for Managed Devices	126
Device Alert Events	127
Next Steps — Configure SNMP and SMTP Notification	128
Configure SMTP Alerts	129
Configure SNMP Alerts	131

Restrictions	131
Configure SNMP settings for Management Center	131
<i>Configure Alerts for Device Errors</i>	133
About Alerting	133
Enable Alerting	133
View Alerts	134
<i>Manage Alerts</i>	134
<i>Create Alerts</i>	142
<i>Edit Alerts</i>	144
Monitor Device Health	147
Device Statistics Notes	151
Metrics	151
Resolve Device Errors	151
<i>Change Device Health and Statistics Monitoring State</i>	151
Schedule	153
Event	154
<i>Enable Device Health and Statistics Monitoring</i>	155
<i>About Pre-Deployed and Deactivated Devices</i>	160
<i>View System Metrics</i>	161
The System Metrics Tab	161
The Health Checks Tab	162
The Backup Tab	162
Determine Your Next Step	163
<i>View Device License Information</i>	163
Add Device Group Attributes	164
<i>Enable Attribute Group Inheritance</i>	165
Add a Device Group	166
<i>Edit a Device Group</i>	168
<i>Ensure Devices Belong to Device Groups</i>	169
<i>Add a Group to Represent Chassis or Cloud Services (Device Cluster)</i>	170
Procedure—Add Device Cluster	171
<i>Drag and Drop Device Groups</i>	172
Back Up Device Configuration Now	174
Next Steps	177
<i>Regularly Back Up a Group of Devices</i>	177
<i>Use Device Information for Backup Job Image Metadata</i>	179
<i>View Device Backups</i>	181
<i>Restore Device Backups</i>	183
<i>Schedule Device Back Up</i>	185
Schedule	187
Event	188
Next Steps	189
<i>Import Device Backups</i>	189
Supported Devices	189
<i>Export Device Backups</i>	191
Schedule	193

Event	193
<i>Set the Number of Backup Slots</i>	195
<i>SSL Visibility Appliance - What is Backed up and Synchronized?</i>	195
Policy	195
PKI	196
Users	196
Platform	196
Alerts	196
Remote authentication	196
Use WAF Policy To Protect Servers From Attacks	199
<i>Requirements</i>	200
<i>Recommended Reading</i>	201
<i>Solution Steps</i>	201
About WAF Policy	202
About the Default Tenant	203
About Tenant Determination	203
Reference: Conditions and Examples	204
Manage Tenants	206
WAF Policy Use	207
Specify Tenant Determination Rules	210
WAF Policy Use	210
Configure WAF Security Rules	215
WAF Policy Use	215
Configure WAF Application Objects	229
WAF Policy Use	229
Analyze and Refine WAF Policy (Mitigate False Positives)	236
WAF Policy Use	236
Analyze and Refine WAF Policy Workflow	236
Manage WAF Security Policy	237
WAF Policy Use	237
Verify WAF Policy Compliance With PCI DSS Requirement 6.6	241
WAF Application	242
WAF Security Profile	243
Non-Compliance	244
Distribute Configurations to Devices	245
Create and Distribute Configurations Using Scripts	246
Next Steps	247
<i>Compare Versions of the Script</i>	248
<i>Customize Object Filters</i>	249
<i>Execute Scripts</i>	251
Direct from a Script	251
From a Job Operation	252

<i>Add Error Handling for Scripts</i>	252
<i>Filter by Attributes and Keyword Search</i>	256
Search by Keyword	257
Procedure	257
Can quotes be used in a search?	257
How do you search for whole words?	257
How do you search for partial words?	258
Example Searches	258
IPv4 127.0.0.1	258
IPv6 "0:0:0:0:0:1"	258
Hostnames	258
What if the search finds no match?	258
What if the search succeeds in finding matches?	258
How do you clear the search results?	258
<i>Import Script from a Device</i>	259
Determine Your Next Step	260
<i>Restore a Version of Script</i>	261
<i>View Script Information</i>	262
<i>Optimize a Script for Use on Other Devices</i>	264
Define the Local Variable	265
Reference the Variable	265
<i>Add a Script Operation (Includes, If Statements, and Error Handling)</i>	267
<i>Apply Logical Expressions to Scripts and Policy</i>	268
Define simple if else logic flow	270
Define advanced if else logic flow with foreach	270
<i>Use Substitution Variables in Policies and Scripts</i>	271
Use in Shared Policy	271
Syntax	272
Examples	272
Supported Variables	273
Specify a Default Substitution Value	275
Syntax	275
Example	276
Use Regular Expressions	276
Syntax	276
Example	276
<i>Preview a Script With Variables Replaced</i>	276
<i>Organize Scripts by Attribute</i>	278
<i>Schedule the Execution of a Configuration Script</i>	281
Before You Begin	281
Schedule Script Execution	282
Schedule	283
Event	283
Create and Distribute Policy	285
<i>Use Content Policy Language (CPL) to Create Policy</i>	292
Working with CPL Policy Fragments	293
Determine Your Next Step	294
Create a CPL Policy Object	295

Determine Your Next Step	296
Add or Edit CPL Policy Sections	298
Refine Existing CPL Policy	302
Manage CPL Policies	304
Work with CPL Policy Sections	306
Layout Modes	306
Single Pane Layout	306
Modular Layout	306
Navigate sections	307
Collapse a section	308
Collapse all sections	308
Move sections	308
Find a Policy Section	309
If the search finds no match	309
If the search finds matches	309
Clear the search results	310
Change the Order in which Policy Rules are Evaluated	311
Use Substitution Variables in Policies and Scripts	312
Use in Shared Policy	312
Syntax	313
Examples	313
Supported Variables	314
Specify a Default Substitution Value	316
Syntax	317
Example	317
Use Regular Expressions	317
Syntax	317
Example	317
<i>Launch Legacy or Web-Based VPM</i>	318
Legacy VPM—Set Up and Enable Java in Your Browser	319
Launch Legacy Visual Policy Manager (Java)	321
Legacy VPM Requirements	321
Launch the Legacy VPM	322
Add a VPM Policy Object	323
Select Reference Device for VPM Policy	325
Determine Your Next Step	326
View VPM Policy Source	326
Restrict Access Only to a Specific Object Included in a VPM Layer	327
Launch Web-Based VPM	337
Web-Based VPM Shared Include Example	338
<i>Create Shared Objects</i>	341
Create a CPL Policy Fragment	344
Create URL List (URL Policy Exceptions)	345
Enabling and Disabling URLs	349
URL List Example	349
Step One - Create the URL List Object	350

Step Two - Add Allowed URLs	350
Step Three - Add the URL List to the ASUP Policy	351
Manage URL and Category List Triggers	353
URL List Triggers	353
Category List Triggers	355
Include a Shared Policy Object in CPL or VPM Policy	355
Work with Categories	363
Create Category Lists	363
Category List Example	368
Step One - Create the Category List Object	368
Step Two - Select Categories that Should be Denied	368
Step Three - Add the Category List to the ASUP Policy	370
Use Category List Templates	374
Update Symantec Global Intelligence Network (BCIS/BCWF) Category Lists	380
Create Custom Categories	382
Enabling and Disabling URLs	385
Custom Category Example	386
Step One - Create the Category Object	386
Step Two - Add URLs	387
Step Three - Add the Category to the ASUP Policy	387
Create a Local Content Filter Database	388
Supported Local Category Syntax	390
Local Category Limitations	390
Define and Manage Local Categories	391
Optional Step - Import Categories	391
Edit a Category	392
View Database Versions	392
Compare Database Versions	393
Record the Local Database Direct URL	394
Local Database URL Protocol Note	394
Manual Deployment - SSL Visibility	395
Manual Deployment - ProxySG and Advanced Secure Gateway	396
(Optional) Scripted Configuration - ProxySG and Advanced Secure Gateway	396
Create a Local Database File	397
Example 1	397
Example 2	398
Create SSL Visibility List Policy	398
Create SSL Visibility URL List Policy	408
Create IP Address List	417
Enabling and Disabling IP Addresses	421
SSL Visibility	421
ProxySG	422
<i>Deploy Tenant Policy</i>	423
Manage Tenants	426
WAF Policy Use	426
Create a VPM Tenant Policy Object	431
Determine Your Next Step	432

Import VPM Tenant Policy from Source Device	432
Determine Your Next Step	435
Schedule Removal of Unused Tenant Policy	435
Schedule	437
Event	437
<i>Apply a Single Policy to Both On-Premises and Cloud Users</i>	438
Prerequisites	438
SSL Requirements	439
Solution Steps	439
Add a Universal VPM Policy Object	440
Transform Existing VPM Policy into Universal VPM Policy	441
Refine and Validate Universal VPM Policy	442
Legacy VPM Requirements	442
Procedure	443
Deploy Universal CPL Policy	445
Analyze the CPL Universal Policy	446
Select Reference Device for Universal CPL Policy	449
Determine Your Next Step	449
<i>Install or Import Policy</i>	450
Preview Policy Before Installing It	450
Install Policy	451
Policy Installation Methods	451
Install Policy	451
Schedule	452
Event	453
Install to Target	454
Install Multiple Policies	455
Import Policy or Shared Objects	457
Universal VPM Policy Considerations	463
Import from Device	463
Determine Your Next Step	464
Import External Policy	465
Schedule	467
Event	467
Distribute ProxySG Policy to Multiple Devices	468
<i>View Policy</i>	469
View Policy Versions	469
View Existing Policy Information	472
View Deployed Policy for each Device Slot	477
View Devices Associated with Policy	478
<i>Configure Policy</i>	479
Add or Remove Devices Associated with Policy	480
Add Targets	480
Remove Targets	482
Determine Your Next Step	482
Check Consistency between Policy and Devices	483
Determine Your Next Step	485

Create Job to Check Consistency of Policy	485
Schedule	486
Event	486
Compare Different Versions of the Same Policy	488
View Effective Policy for each Slot on a Device	490
How the effective policies are assigned	490
Compare the Device Policy Version with Current Policy Version	491
Determine Your Next Step	491
Export Policy or Shared Objects to Local Disk	491
Restore a Version of Policy	493
Use Specific Attribute Values to Control Access to Policy	493
Procedure	494
<i>About Universal Policy Enforcement</i>	495
Create Shared Objects	495
Permissions Reference	498
Reference: Permissions Interdependencies	499
Reference: Permissions Filters Object and Attributes	513
Reference: Understanding Job Permissions	517
User runs a job immediately after configuring it or manually using Run Now	517
User configures a job scheduled in the future	517
Configure Users, Roles, and Attributes	519
Manage Management Center Users	520
Add Users and Grant Permissions	520
Add Local Users	524
View All Users and Associated Roles and Permissions	527
About the User Permissions Overview Report	527
User Permission Overview Example	528
About the User Permissions Report	529
Add Users from an Existing Directory or Service	530
Authenticate Users Against LDAP	531
Authenticate Users Against Active Directory LDAP	535
Authenticate Users Against RADIUS	538
Authenticate Users and User Groups using Existing Directory Service	541
Authenticate Users with SSL Mutual Authentication	542
Note	546
Use Certificate Subject Alternative Name Data for Certificate Validation	548
View, Edit, or Delete User Accounts	550
View User Information	550
View User Permissions	550
Edit User	551
Delete a User	552
Change and Reset Passwords	553
Change Your Password	554

Reset Password	556
Prerequisites	556
Manually Reset a User's Web Console Password	558
Expire a User's Web Console Password	558
Reset or Restore Admin Account Passwords	560
Management Center 2.1.x	560
Manage User Groups	561
Add User Groups	561
Edit a User Group	563
View Group Permissions and Roles	563
View Group Members	564
Delete a User Group	564
Manage User Sessions	566
Define Roles	567
About Roles	567
Procedure	568
Duplicate an Existing Role	569
Edit an Existing Role	570
Grant Permissions	572
Update Access When a User's Job Changes	574
Update a User's Roles	574
Filter Devices or Device Groups in a Permission	575
Restrict Access to Reporter Reports and Data	576
Users Associated With Multiple Roles	582
Manage Attributes	583
About Attribute Inheritance	583
Configure Device Group Inheritance	583
Work With Attributes	583
Add Attributes	584
Edit Attributes	587
Set User-Defined Device Attributes for Access Control	589
Hide Attribute Value	590
Encrypted Attribute Feature Limitations	590
Add Encrypted Attributes	590
Verifying Encrypted Attributes	592
Filter and Keyword Search	594
Procedure	594
Search by Keyword	595
Can quotes be used in a search?	595
How do you search for whole words?	595
How do you search for partial words?	596
Example Searches	596
IPv4 127.0.0.1	596
IPv6 "0:0:0:0:1"	596
Hostnames	596
Search	596

What if the search finds no match?	596
What if the search succeeds in finding matches?	596
How do you clear the search results?	597
Preview or Download Logs	598
Available Logs	598
Other Logs	599
Log Types	599
Create and Manage Jobs	600
Add a Job	600
Composite Jobs	601
Device Management	601
Policy and Configuration	601
Reports	602
System Management	602
Add Job That Includes Multiple Jobs (Multistep Job)	602
Schedule	603
Event	604
Add Job That Includes Multiple Operations (Multistep Device)	604
Schedule	606
Event	607
Collect Sysinfo	608
Schedule	609
Event	610
Restore Device to Factory Defaults	610
Schedule	611
Event	612
Schedule Device Restart	612
Schedule	613
Event	614
Save Device Configurations	614
Schedule	616
Event	617
Schedule Reporter Reports	618
Schedule	619
Event	620
Schedule SWG-VR Data Collection	620
Schedule	621
Event	622
Schedule Statistics Monitoring Reports	622
Schedule	623
Event	624
Schedule Summary Report Job	624
Schedule	626
Event	626
Back Up the Management Center Configuration	627
Important Backup Notes	627

Backup Requirements	627
Back Up Management Center	627
Schedule	628
Event	629
Back Up Management Center Using the CLI	630
<i>Schedule File Transfer</i>	630
Schedule	631
Event	631
Share a Job With Another Management Center Appliance (Export/Import)	632
Job Scheduling Options	637
Monitor Jobs	640
Edit a Job	641
View Current Jobs	642
Cancel a Currently Running Job	644
View and Manage Job History	645
View and Filter Job Progress	646
Organize Jobs with Folders	647
Job Operations	648
 Management Center Reports	656
Statistics Monitoring Reports	656
Reporter Reports	656
View Consolidated Reports	657
Integrate Reporter into Management Center	659
Add a Device	660
Step 1: Create WSS Integration Token	671
Step 2: Add WSS in Management Center	671
View a Reporter Report	674
Create Geovisual Reporter Reports	682
Create GeoVisual Maps	684
Run a Summary Report	685
View Reporter Report Details	687
Run a Reporter Report in the Background (Or to Archive)	689
Reference: Report Descriptions	691
Search for Specific Report Data (Search and Forensic Report)	702
Reporter Graph Types and Views	707
Create a Custom Reporter Report	708
Edit Custom Reporter Reports	718
Additional Information	721
Date Filters	721
Customize Reporter Report Options	722
Change the number of items displayed per page	726

Change the grouping of the report (that is, change the focus of the report).	726
Create a two-level report	728
Create Custom Report Groups	728
Set Time Zone for Reporter Reports	730
<i>Determine Why A Reporter Database Does Not Display</i>	731
View Statistics Monitoring Reports	732
<i>Reference: Statistics Monitoring Reports in Management Center</i>	736
<i>Modify Options for Statistics Monitoring Reports</i>	739
<i>Change the Scope of a Statistics Monitoring Report</i>	741
Filter on Devices or Device Groups	743
Zoom In and Out on Reports	743
<i>Display a Full Statistics Monitoring Report</i>	744
Determine Your Next Step	744
<i>Statistics Monitoring Graph Types</i>	745
<i>Statistics Monitoring Over HTTPS</i>	745
<i>Remove Orphan Device Count in Statistics Monitoring Dashboard</i>	746
Syntax	746
Work with Reports	747
<i>Create a Shared Statistics Monitoring or Reporter Custom Report</i>	748
Allowed User Operations	748
Find Shared Custom Reports	749
Create a Shared Custom Report	749
<i>Add a Custom Logo to Downloaded Reports</i>	750
Logo Size	750
Procedure—Add Custom Logo to Reports	751
Remove Custom Logo	751
<i>Customize Report Widgets</i>	752
Collapse Report Widgets	752
Move Report Widgets	752
Remove Report Widgets	752
Change Date Range for Reporter Widgets	752
Add Reports	752
Close a Report	753
Close the Active Report	753
Close a Report on Another Widget	753
<i>Modify Display of Table Data</i>	753
<i>View Raw Report Data</i>	756
<i>Set Bandwidth Cost for Reports</i>	756
<i>Reports: Save as PDF</i>	756
Manage Dashboards	758
Notes	758
Dashboards and Widgets	761
<i>Dashboards</i>	761
<i>Widgets</i>	762

Add a Widget to the Current Dashboard	762
Add the Bookmarked Devices Widget	764
Change the Dashboard Layout or Refresh Rate	765
Administrat e Management Center	767
Define Management Center Settings	767
Configure General System Settings	769
<i>View Audit Log</i>	770
<i>Specify Explicit Proxy Settings</i>	772
<i>Configure Diagnostics Logging</i>	773
<i>Configure Housekeeping Settings</i>	776
<i>Configure Mail Settings</i>	776
<i>Configure the SNMP Agent Password</i>	777
<i>Management Center: SNMP Monitoring Best Practices</i>	778
<i>MIBs Used With Management Center</i>	778
<i>BLUECOAT-SG-SENSOR-MIB</i>	779
<i>Listing SENSOR-MIB Values From the CLI</i>	781
<i>HOST-RESOURCES-MIB</i>	782
<i>Interfaces Group MIB (IF-MIB)</i>	783
<i>SNMPv2-MIB</i>	787
<i>BLUECOAT-INFO-MIB</i>	788
<i>BCSI-MC-RESOURCES-MIB</i>	789
<i>SNMP Traps</i>	789
<i>Additional Information</i>	789
<i>Legal Notice</i>	789
<i>Add Packages to Management Center</i>	790
<i>Configure Consent Banner</i>	791
<i>Procedure</i>	792
<i>Editor Example</i>	794
<i>Configure Hardware Monitor Settings</i>	795
<i>Set HTTPS Server Certificate Hostname for Secure Device Communication</i>	796
<i>Set a Hostname</i>	796
Management Center Mail Settings	796
Upload Files to Management Center	797
Migrate From Director to Management Center	803
<i>Determine Your Next Step</i>	810
Upgrade Management Center	811
<i>Upgrade Best Practice</i>	811
<i>Manage Management Center System Images</i>	811
<i>Special Notes Regarding Management Center 2.x Software Image Installation:</i>	812
<i>Upgrade Management Center Failover Pair</i>	813
<i>Upgrade from 2.2.x or 2.3.x</i>	813
Downgrade Management Center	815

Restore a Management Center Backup Configuration	817
Restore Management Center Backup	817
Configure Management Center Failover	818
Important Failover Notes	819
Replicated Data	819
Configuration Limitations	821
Device Limitations	821
Failover Prerequisites	821
Configure Failover	822
Switch to Secondary When the Primary is Unresponsive	825
On the Secondary Failover Partner:	825
On the Original Primary Device:	826
Upgrade the Failover Pair	827
Configure SNMP Alert or SMTP Trap for Failover Alerts	829
Example SNMP Trap Configuration	830
View Failover Health Check Logs	831
Disable Failover	831
Update the Management Center License	832
Next steps	836
Automate Password Reset Process	837
Display Local Time on Management Center	838
Display Local Time on Management Center User Interface	838
Federal Information Processing Standards (FIPS) Mode	839
What Happens When FIPS Mode is Enabled in Management Center 2.1.1.2	840
FIPS Cryptographic Algorithms for Management Center 2.1.1.2	841
Cryptographic Restrictions for Products Managed by Management Center	842
Enable FIPS Mode on Management Center	843
FIPS 140-2 Non-Proprietary Security Policy Documents	843
Enable FIPS Mode	843
What Happens When FIPS Mode is Disabled in Management Center 2.1.1.2	844
Troubleshoot and Resolve Issues	845
Audit Transactions	846
Understand Transaction Types	848
Customize the Audit Log	849
Determine Which Management Center Version You are Using	851
Build Information Fields	852
Configure Management Center to Trust Its Image Store	852
Install Management Center Certificates on Content Analysis to Establish SSL Trust	854
Step 1: Collect Management Center Certificates	854
Step 2: Install Management Center Certificate(s) on the Content Analysis Appliance:	855

Can't Connect to Device After Upgrading to 2.x	856
A Device is Unassigned to a Device Group	857
User has "does not support" error when adding target device to edited policy	857
Prevent Licensing Issues on Management Center Virtual Appliances	858
Duplicate Serial Numbers	858
Expiring Licenses	858
Stop or Restart Services	859
Stop Management Center Services	859
Restart Services	859
Test Network Connectivity	860
Upload System Diagnostics	861
View Hardware Diagnostics and Memory Resources	862
Problems and Errors	863
<i>Read Messages and Alerts</i>	<i>864</i>
<i>"Could not enable statistics collection due to unexpected server failure" when activating a device</i>	<i>865</i>
<i>"Import batch contains duplicate device name violation" when importing multiple devices</i>	<i>865</i>
<i>"Local Changes Detected" error when installing policy</i>	<i>865</i>
<i>User has "access denied" error when running a job</i>	<i>866</i>
<i>"Multi-tenant policy support is not enabled for this device" when installing policy</i>	<i>866</i>
Review Open Source Attributions	867
Tips and Use Cases	869
Management Center REST API	870
 Limitations	870
 Documentation	870
 Troubleshooting	871
CLI Command Reference	872
 Access the Management Center Command Line Interface (CLI)	873
 CLI URL Syntax	875
Notes	875
 CLI Output Processing	876
Syntax	876
Example	876
<i>help</i>	<i>880</i>
Syntax	880
Example	880
<i>ping</i>	<i>881</i>
Syntax	881
Examples	881

<i>fips-mode</i>	882
Syntax	882
SubCommands	882
Configure Mode Commands	882
<acl></acl>	883
Syntax	883
Notes	883
Examples	883
<appliance-name></appliance-name>	884
Syntax	884
Notes	884
Examples	885
authentication	885
Syntax	885
Notes	886
Examples	886
backup	886
Syntax	886
SubCommands	886
Transfer Configuration and Data to Another Appliance	888
Example	888
clock	889
Syntax	889
Examples	889
device-communication	889
Syntax	889
Example	890
dns	890
Syntax	890
Notes	890
Examples	890
failover	890
Syntax	891
SubCommands	891
Example	892
fips-mode	893
Syntax	893
SubCommands	893
health-monitoring	893
Syntax	893
health-monitoring view	894
Syntax	894
Examples	895
installed-systems	895
Syntax	895
Examples	898
interface	898
Syntax	898
Notes	898

Examples	898
<i>ip</i>	899
Syntax	899
Examples	899
<i>ipv6</i>	900
Syntax	900
Examples	900
<i>login-banner</i>	900
Syntax	900
Examples	901
<i>licensing</i>	901
Syntax	901
Examples	902
<i>ntp</i>	903
Syntax	903
Notes	904
Examples	904
<i>password-policy</i>	905
Syntax	905
Notes	907
Examples	907
<i>proxy-settings</i>	907
Syntax	908
Examples	908
<i>security</i>	908
Syntax	909
Example	909
<i># service-action</i>	913
Perform Disk Maintenance	913
Syntax	913
Purge VPM Cache	913
Syntax	914
Rebuild Cache Repository Index	914
Syntax	914
Remove Orphan Device Count in Statistics Monitoring Dashboard	914
Syntax	914
<i>snmp</i>	914
Syntax	914
<i>snmp agent</i>	915
Syntax	915
Examples	915
<i>snmp community</i>	915
Syntax	916
Examples	916
<i>snmp system</i>	916
Syntax	916
Examples	916
<i>snmp usm local</i>	917
Syntax	917

Examples	917
<i>snmp usm remote</i>	918
Syntax	918
<i>snmp vacm group access</i>	918
Syntax	918
Examples	918
<i>snmp vacm group member</i>	919
Syntax	919
Examples	919
<i>splunkforwarder</i>	919
Syntax	919
Examples	919
<i>ssh generate</i>	920
Syntax	920
Example	920
<i>ssh ciphers</i>	920
Syntax	920
Example	920
<i>ssl</i>	920
Syntax	920
Notes	922
Examples	922
<i>ssl create</i>	923
Syntax	923
Examples	924
<i>ssl delete</i>	924
Syntax	924
Example	924
<i>ssl edit</i>	924
Syntax	925
Examples	925
<i>ssl inline</i>	926
Syntax	926
Examples	927
<i>ssl view</i>	928
Syntax	928
Examples	929
<i>statistics-monitoring</i>	930
Syntax	930
Example	930
<i>timezone</i>	931
Syntax	931
Supporting Commands	931
Examples	931
<i>upload</i>	932
Syntax	932
Example	932

Legal Notice

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Copyright © 2020 Broadcom. All Rights Reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Wednesday, April 8, 2020

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.

Note: You can also view a list of [Management Center solutions](#).

Feature	Benefit
Management Center provides centralized management for up to 1000 devices.	Eliminate the need to manage each remote device manually, reducing management costs.
Groups devices based on location, department, purpose, and other attributes that you specify.	Delegate administrative duties and deploy policies for specific groups. Enables administrators to assign attributes for managed devices that have different purposes within their network.
Roles have greater flexibility, enabling user groups with the same permissions to access and manage policies and devices within their specific organization.	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).
Manages internal and external user accounts for Management Center.	Users only access the functional areas and perform tasks required for their jobs.
Facilitates creating and deploying policy to multiple devices simultaneously. Includes Visual Policy Manager and consistency checking between policies and devices	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.
Manage attributes for devices, device groups, policy and device scripts	Use attributes to define custom metadata for devices, device groups, policy and device scripts. Filter on attributes to refine searches for all objects.

Feature	Benefit
Create, edit and execute scripts. Includes the ability to compare script versions and to import a script from a managed device	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.
Audit log records user and system event history	Be aware of all user actions in the system and support organizational accountability.
Default Reporting (Reports on device performance)	Management Center provides centralized reporting for managed devices. Statistics Monitoring reports are included by default and include: <ul style="list-style-type: none"> ■ Devices ■ WAN Optimization Reports
Advanced Reporting (Reporter 10.x integration)	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: <ul style="list-style-type: none"> ■ Security reports ■ Web Application reports ■ User Behavior reports ■ Bandwidth Usage reports 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.
Storing device backups on an external server	Enables administrators to export backups to external servers using any of the following 4 protocols: FTP, HTTP, HTTPS, or SCP
Job scheduling to automate repetitive tasks	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.
Hardware appliance support	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.

Access Management Center Software Downloads and Documentation

Access the latest *Management Center Release Notes* and *Management Center Configuration Guide* from Symantec.

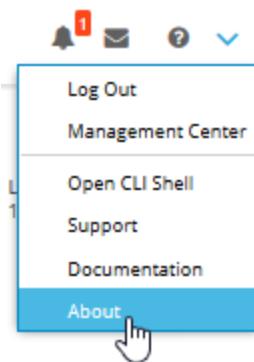
Product Documentation

<http://techdocs.broadcom.com/content/broadcom/techdocs.html#web-and-network-security>

Release Notes, Software Images, MIBs

To download software images and license keys, you need the following:

- The serial number of your appliance. To locate the serial number, go to the Management Center banner and click **About**. View the serial number under Chassis FRU Info. The serial number can also be found on the front panel LCD screen.



- For additional instructions, refer to the [Getting Started](#) guide.

Download Software

Refer to the [Getting Started](#) guide for more information.

Contact Us

We appreciate your comments about this guide. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this guide.

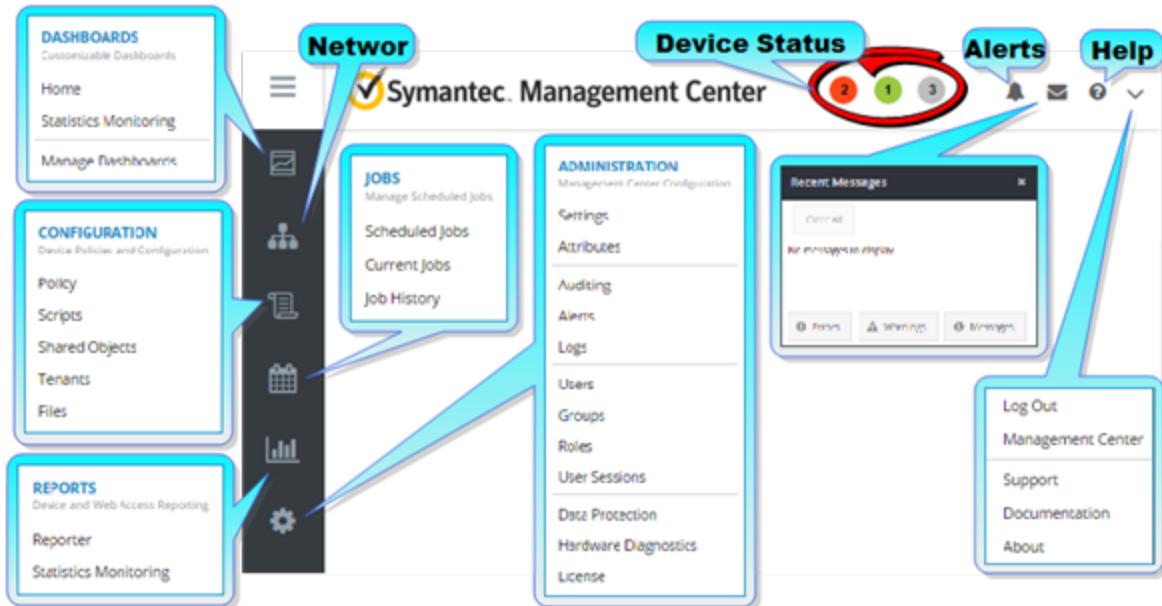
To send feedback on this or other Symantec product documentation, write to us at documentation.inbox@broadcom.com.

Web Console Overview

The web console is the user interface for Management Center.

Note: Depending on a user's permissions, not all of the tabs may be visible to a particular user. See "Reference: Permissions Interdependencies" on page 499 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.
- **Messages** display when you or other users complete certain tasks in Management Center. See "Read Messages and Alerts" on page 864.
- **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, serial number, appliance identifier (Enterprise licensed appliances only), and links to open source 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 758 and customize the data that you want to monitor for managed devices. See "Change the Dashboard Layout or Refresh Rate" on page 765, "Dashboards and Widgets" on page 761, and "Add the Bookmarked Devices Widget" on page 764

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. See "Add and Monitor Devices" on page 52.

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 245.

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 600.

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
- 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 864 for more information.

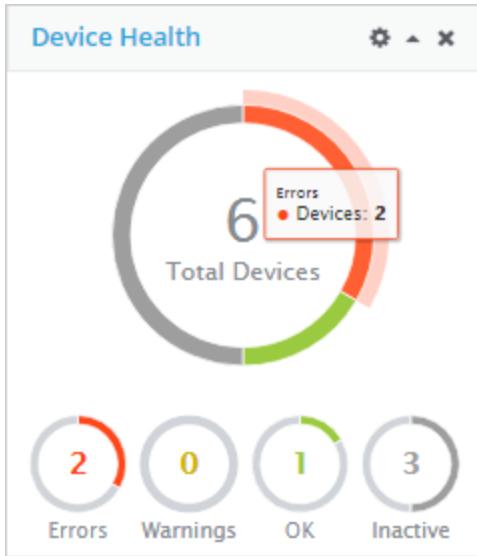
- **Banner**

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



- 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 147.

- 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 642.

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

Management Center Configuration & Management

Status	Color	How it applies to devices	How it applies to alerts
Error	 red	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 "View Current Jobs" on page 642.	An error occurred, preventing an event from completing. Example: During the device registration process, the connection test failed.
Warning	 yellow	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 "Monitor Device Health" on page 147.	An error might occur if you do not take preventative action. Example: The ProxySG appliance's Subscription Communication Status metric is in critical state.
OK (device)	 green	Components on the device are operating within normal parameters. The job has completed successfully. See "View and Manage Job History" on page 645.	A task was completed or a change was made. Example: The ProxySG appliance's SGOS Base License Expiration is in warning state.
Message (alert)			Example: A user account was added.
Inactive	 gray	The device is pre-deployment or deactivated. See "About Pre-Deployed and Deactivated Devices" on page 160 for information.	Not applicable.

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*.

Note: 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.

Tip: 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 791.

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

Tip: The default username/password is **admin/admin**. To restore the default admin password, see "Reset or Restore Admin Account Passwords" on page 560.

3. You can request a password reset. Click **Reset Password**. For more information, see "Reset

Management Center Configuration & Management

"Password" on page 556. For added access control, administrators should enable password reset settings for users with the correct permissions. See "Automate Password Reset Process" on page 837.

Please sign in with your Symantec Management Center account credentials.

Username

Password [Reset Password](#)

log in

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

See "Web Console Overview" on page 29 and "Dashboards and Widgets" on page 761.

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 a side bar. 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 on the left side of the interface. Hover over an icon to view information about that tab. Each tab is logically organized 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.

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

Management Center Configuration & Management

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:

- 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:

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.

Note: If you are creating a Management Center KVM instance, you must complete Configure Access to the Management Center KVM Instance before trying to verify web console access.

Note: 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`

Note: You cannot change the port number.

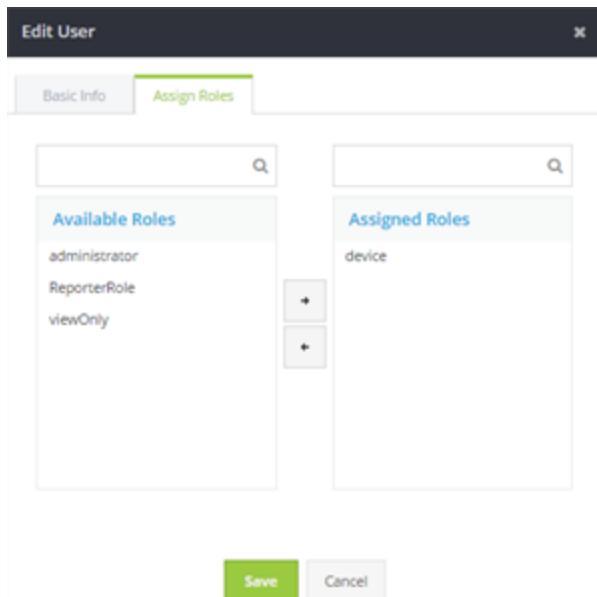
The web browser displays the login screen.

If the web console does not load, run the `# licensing 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:

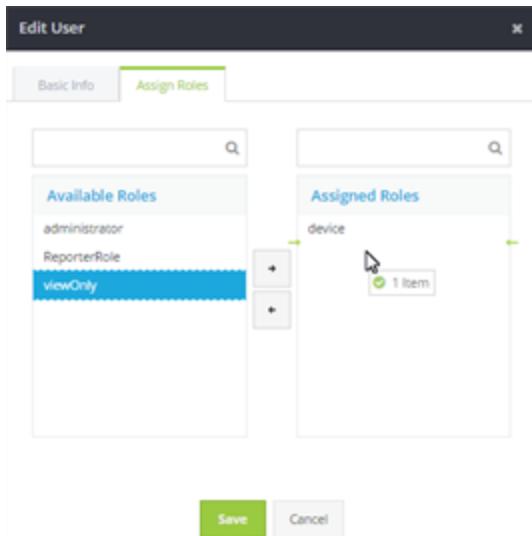


If the list of items is long, you can scroll down to locate the item to move. You can also search using the search field above it.

The web console allows several ways to move items.

Drag an Item From One Area to Another

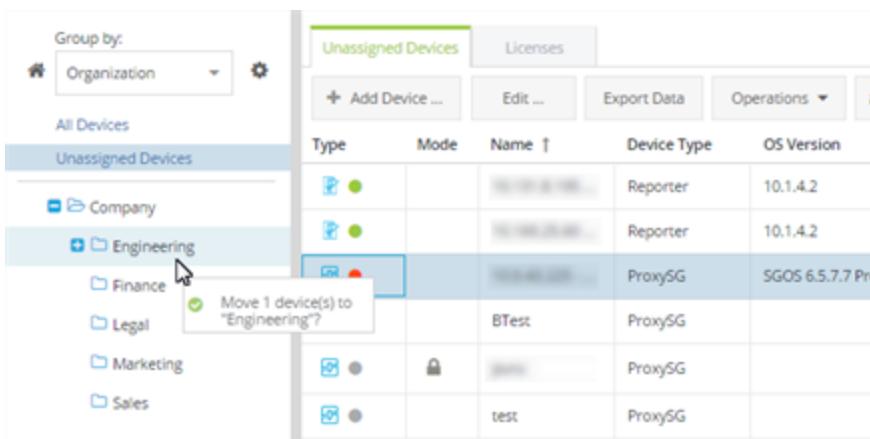
For example, to add a role to a user, select the role under Available Roles. Click and hold; the pointer turns into a hand cursor . Drag the role to Assigned Roles. The dialog displays a green line under Assigned Roles and the pointer turns into a pointer cursor , indicating that the role can be moved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



Release the mouse button to move the role.

Drag a Selected Device to a Device Group

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 169.
2. Selected 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**.



Date Filters

When filtering by date, different time increments may display, depending on the type of date filter that you select. The list below describes each date filter and its associated time increments.

Filter	Time Increments	Description
Quick Pick	1 Day 7 Day 30 Day 90 Day YTD	
Current	hour day week month year	Displays the current <time increment> of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the data that is displayed in the report reflects a month's data for the current month of May.
Previous	hour day week month year	Displays the previous <time increment> of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the data that is displayed in the report reflects a month's data for the previous month of April.
Current and Previous	hour day week month year	Displays the current <time increment> and the previous <time increment> of data based on the beginning and ending cycle of that increment. For example: If you filter on the current and previous month, and the current month is May, the data that is displayed in the report reflects data for both April and May.

Filter	Time Increments	Description
Before	Calendar picker	Displays an absolute date on a calendar. Displays all data for that report that exists in the database before the date chosen.
Since	Calendar picker	Displays an absolute date on a calendar. Displays all data for that report that exists in the database after the date chosen.
Custom	Calendar picker	Displays a calendar picker to choose the beginning and end of the data.
All Dates	No dates are filtered	Displays all data for all dates stored in the database. When choosing this option, all absolute dates disappear and no calendar picker is available.

Required Ports, Protocols, and Services

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

Important Notice

As of Saturday, April 11, 2020, The following Symantec: A Division of Broadcom licensing services IP address changes take effect.

Service Host	Symantec IP Address (Old)	Broadcom IP Address (New)
validation.es.bluecoat.com	155.64.49.136	192.19.237.101
bto-services.es.bluecoat.com	155.64.49.131	192.19.237.99
device-services.es.bluecoat.com	155.64.49.132	192.19.237.100
download.bluecoat.com	155.64.49.133	192.19.237.102
services.bluecoat.com	155.64.49.135	192.19.237.103
abrc.BLUECOAT.COM	155.64.49.137	192.19.237.69

Inbound Connections to Management Center

Service	Port	Protocol	Configurable?	Source	Description
Web UI	8080 8082	TCP	No	User's client	Management Center web console.*
CLI	22	TCP	No	User's client	Management Center CLI shell access
Web API	8082	TCP	No	User's client	Management Center API via HTTPS
Statistics Collector	9009	TCP	No	Blue Coat ProxySG appliance/Advanced Secure Gateway/SSL Visibility	Performance Statistics data sent by monitoring assets via HTTP.*
Statistics Collector	9010	TCP	No	ProxySG appliance/Advanced Secure Gateway/SSL Visibility	Performance Statistics data sent by monitoring assets via HTTPS.*
Management Center Failover	2025	TCP	No	Alternate Management Center appliance in a failover cluster.	Used to transmit state and other pertinent information between primary and secondary Management Center appliances in a failover pair.

*Ports 8080 and 9009 are disabled by default on new deployments. If you upgrade from version 1.x to version 2.x and ports 8080 and 9009 were previously enabled in version 1.x (with the security http enable command) they will remain open after the upgrade to 2.x.

Outbound Connections from Management Center

Service	Port	Protocol	Configurable?	Destination	Description
LDAP	10389	TCP	Yes	LDAP server	Authentication
LDAPS	389 636				
Active Directory	10389 389 636	TCP	Yes	Active Directory server	Authentication
RADIUS	1812	UDP/TCP	Yes	RADIUS server	Authentication

Management Center Configuration & Management

Service	Port	Protocol	Configurable?	Destination	Description
RADIUS	1813	UDP/TCP	Yes	RADIUS server	Accounting
SMTP	25	TCP	Yes	SMTP server	SMTP alerts
SNMP Trap	162	UDP	Yes	Trap receiver	SNMP traps
HTTP Proxy	8080	TCP	Yes	HTTP Proxy	Updates
NTP	123	UDP/TCP	No	NTP server list	Time sync to customer-configured NTP time server
HTTPS	443	TCP	No	Symantec	<p>https://support.symantec.com</p> <p>License activation, Web Application Firewall (WAF) subscription, the latest release information and documentation</p>
DNS	53	UDP/TCP	No	DNS server	FQDN lookups
ProxySG/ASG	22	TCP	No	ProxySG appliance/Advanced Secure Gateway	ProxySG appliance monitoring and management
ProxySG/ASG	8082	TCP	No	ProxySG appliance/Advanced Secure Gateway	System image upload
SSH access to managed devices	22	TCP	No	All managed devices	Device scripts support for appliances with SSH access, CLI shell.
SCP access to external servers	22	TCP	No	All managed devices and other hosts Management Center exports data to	Importing and exporting data—Management Center and device backups, diagnostics, PCAP transfer
MA	443	TCP	No	Malware Analysis	Health monitoring and backup
PacketShaper	80/443	TCP	No	PacketShaper	Health Monitoring (unencrypted/encrypted)
Reporter	8080/8082	TCP	No	Reporter	Reporter API (unencrypted/encrypted)
Management Center	2025	TCP	No	Alternate Management Center appliance in a failover cluster.	Used to transmit state and other pertinent information between primary and secondary Management Center appliances in a failover pair.

Management Center Configuration & Management

Service	Port	Protocol	Configurable?	Destination	Description
CA	8080/8082	TCP	No	Content Analysis	Health Monitoring (unencrypted/encrypted)
SSL Visibility	443	TCP	No	SSL Visibility	Health monitoring and configuration synch

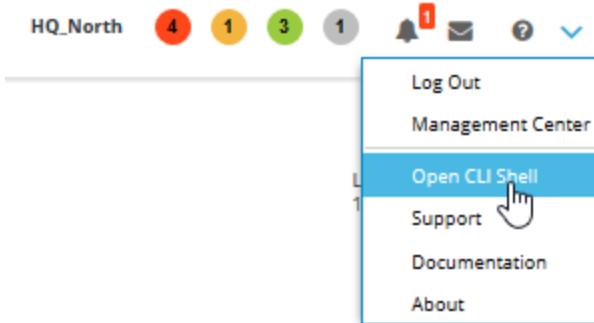
Required IP Addresses and URLs

Ensure connectivity from Management Center to the following URLs.

URL	Protocol	Port	Description
199.19.250.195 199.116.168.195	HTTPS TCP	443	Web Security Service policy updates.
validation.es.bluecoat.com	HTTPS TCP	443	Validates the license every 5 minutes. After successful validation, validation occurs every hour.
bto-services.es.bluecoat.com	HTTPS TCP	443	Validates the license.
device-services.es.bluecoat.com	HTTPS TCP	443	License related.
services.es.bluecoat.com	HTTPS TCP	443	License related.
abrca.bluecoat.com	HTTPS TCP	443	Symantec CA.
appliance.bluecoat.com	HTTPS TCP	443	Trust package downloads.
subscription.es.bluecoat.com	HTTPS TCP	443	Subscription services.
upload.bluecoat.com	HTTPS TCP	443	Upload diagnostic reports to Symantec support.
sgapi.es.bluecoat.com	HTTPS TCP	443	Universal VPM policy.

Access the Management Center CLI

You can access the Management Center CLI from the pull-down in the user interface banner.



Note: You can also "Access the CLI of a Managed Device" on page 85.

Requirements

Users must have the <Management Center, CLI> permissions to use this feature.

Procedure

1. Go to the Management Center home or dashboard



2. In the banner, click the pull-down and select **Open CLI Shell**.

A new browser window opens.

3. Manually log into the Management Center CLI shell.

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.

Caution: 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 627.

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 627.

This process ensures that you will be able to restore the previous configuration if the upgrade fails.

Special Character Replacement

Management Center intentionally replaces some non-displayable characters, quotes, and so on, to normalize file names. This is done to create a consistent download behavior for systems receiving the files. Management Center could preserve these characters but they would not be accepted by the receiving system.

Special Character	Replacement Character
/	-
\n	None. Removed.
\r	None. Removed.
\t	None. Removed.
\0	None. Removed.
\f	None. Removed.
`	None. Removed.
?	-
*	-
\\"	-

Management Center Configuration & Management

Special Character	Replacement Character
<	-
>	-
	-
'	None. Removed.
"	None. Removed.
:	-

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 832

"Create and Distribute Policy" on page 285

"Apply a Single Policy to Both On-Premises and Cloud Users" on page 438

"Set HTTPS Server Certificate Hostname for Secure Device Communication " on page 796

"Use WAF Policy To Protect Servers From Attacks" on page 199

"Add and Monitor Devices" on page 52

"Create and Manage Jobs" on page 600

"Add Users and Grant Permissions" on page 520

"Monitor Device Health " on page 147

"Manage Dashboards" on page 758

"Integrate Reporter into Management Center" on page 659

"View Consolidated Reports" on page 657

"Modify Display of Table Data" on page 753

"Migrate From Director to Management Center" on page 803

"View Audit Log" on page 770

"Define Management Center Settings" on page 767

"Authenticate Users with SSL Mutual Authentication" on page 542

"Upload Files to Management Center" on page 797

"Regularly Back Up a Group of Devices" on page 177

"Back Up the Management Center Configuration" on page 627

Manage Devices

Refer to the following topics for assistance.

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 66 or "Migrate From Director to Management Center" on page 803.

Other actions and considerations:

- To enable secure communication with devices, see "Set HTTPS Server Certificate Hostname for Secure Device Communication " on page 796.
- To run operations on managed devices, see "Perform an Operation on a Managed Device" on page 77.
- You can manage up to 500 devices in Management Center.

The screenshot shows the Symantec Management Center interface. The top navigation bar includes 'Groups' (highlighted with a yellow box A), 'Health' (highlighted with a yellow box A), 'Licensing' (highlighted with a yellow box A), and 'MC1.PUBSLAB' (highlighted with a yellow box C). The main toolbar features 'Add' (highlighted with a yellow box B), 'Edit' (highlighted with a yellow box B), 'Sort' (highlighted with a yellow box B), 'Operations' (highlighted with a yellow box D), and various icons for search and refresh. The left sidebar has 'Device Groups' (highlighted with a yellow box E) and 'Unassigned Devices' (highlighted with a yellow box E). The central area displays a table titled 'Devices (3)' with columns: Name, Status, Mode, OS Version, IP Address, CPU, Memory, and Actions. The table shows three rows of data. A vertical 'Filters' panel is on the right. A yellow box F points to the 'Actions' column in the table.

Name	Status	Mode	OS Version	IP Address	CPU	Memory	Actions
1	green circle		10.1.5.4			60%	<input checked="" type="checkbox"/> <input type="checkbox"/>
1	red circle with 1		SGOS 6.7.3.5 Reverse P...		1%	24%	<input checked="" type="checkbox"/> <input type="checkbox"/>
1	green circle		10.2.1.4			1%	<input checked="" type="checkbox"/> <input type="checkbox"/>

Key

A — Switch views to view health or licensing device data.

B — Add new device or group. See "Add a Device" on page 660 and "Add a Device Group" on page 166.

C — View device warnings and errors at a glance. See "Monitor Device Health" on page 147, "Resolve Device Errors" on page 61, and "Web Console Overview" on page 29 for more information.

D — See "Perform an Operation on a Managed Device" on page 77.

E — Filter by group. See "Add a Device Group" on page 166 and "Configure Hierarchy for Devices and Device Groups" on page 103.

F — Edit or delete devices. See "View and Edit Device Information" on page 69.

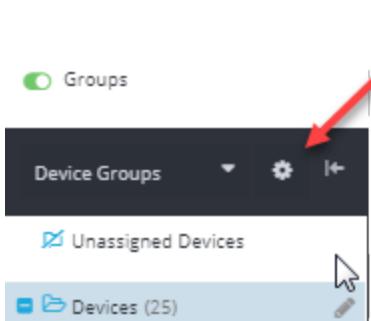
About Hierarchy and Group Views

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)
- 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. Click the gear icon to view and manage hierarchies. See "Configure Hierarchy for Devices and Device Groups" on page 103.



Customize the Network View

You can customize the **Network** tab to make it easier to keep track of specific devices or device groups. When you make display changes, change column widths or order, etc., the changes are preserved even if you refresh the grid or log out.

The Network view shows information of the network, with the group folders in a section to the left and detailed information of the folders and devices displayed in a list. Each list item shows status, device type (including folders), OS version, IP address, user-defined description, and more. Click groups to drill down in the hierarchy.

Switch Between Health and Licensing Status Views

Click **Health** or **Licensing** to view corresponding device information.

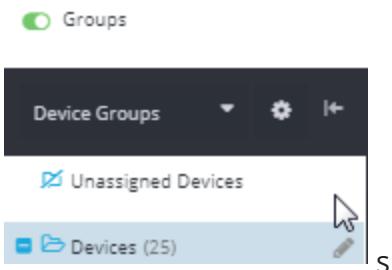


Toggle Group Association

When the **Groups** toggle is off, Management Center displays a flat list of devices. When the **Group**

Management Center Configuration & Management

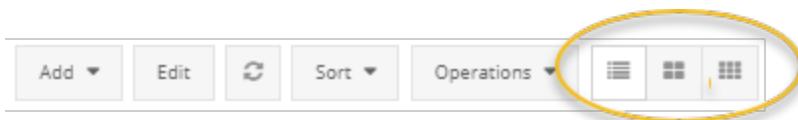
toggle is on, Management Center displays the group hierarchy in the left panel and a list of devices associated with the group in the right panel. Select a device group to show the device members.



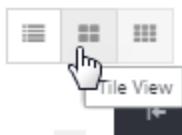
Click the gear icon to view and manage hierarchies. See "Configure Hierarchy for Devices and Device Groups" on page 103.

Change the Representation of Displayed Data

Click the Grid, Tile, or Icon view to change how the system represents the displayed data. Hover over a box in the tile or icon views to view device details. Right click a device box to perform device operations. For example, to launch the console. See "Perform an Operation on a Managed Device" on page 77.



Hover over the icon to identify each view.

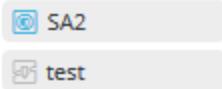


Grid

Displays data in line-by-line, vertical order. This is the default view.

Tile

Displays the data as device boxes labeled with the device icon and name (and warning or error state if present).



Icon

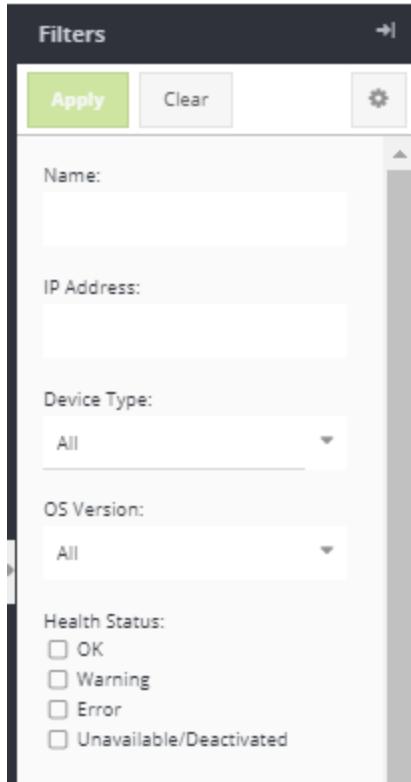
Displays small device boxes labeled with the device icon and color coded to the current health status. This view can be useful if you have a lot of devices.



Filter devices by status

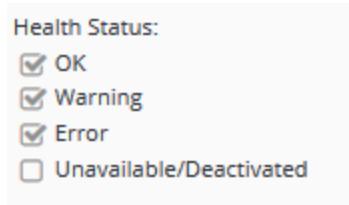
1. Select **Network**.
2. Go to the **Filters** panel on the right-side of the page. Enter filter criteria or select or clear the check boxes for statuses that you do not want to display. Click **Apply**.

Management Center Configuration & Management



For more information about colors and status indicators, see "About Color-Coded Status Indicators" on page 32.

In the following example, the **Inactive** status is not checked; thus, only devices with **Error**, **Warning**, and **OK** status (that is, devices that are activated) are displayed.



Change Displayed Columns

1. Select **Network**.
2. Select any column heading drop-down arrow.

3. Select **Columns** and select or deselect the available columns.

The screenshot shows a table header with columns: Type, Mode, Name, Device Type, and OS Ver. To the left of the table, there's a context menu with options: Sort Ascending, Sort Descending, Columns (which is currently selected and expanded), and Reset Columns. The 'Columns' submenu lists all the columns from the table header plus two more: Description and Memory. Each column has a checkbox next to it. The checkboxes for Type, Mode, Name, Device Type, OS Version, and CPU are checked, while Description and Memory are not checked.

The system displays the added columns. See also "Modify Display of Table Data" on page 753.

Configure Device Connection Security Level (SSL Context)

An SSL context is a collection of ciphers, protocol versions, trusted certificates and other TLS options. Since it is very common to have multiple connections with the same settings, they are put together in a context and the relevant SSL connections are then created using this context.

This feature enables you to use a global SSL context that applies to all devices, or to assign a context on a per-device basis. For example, you might want some devices to use a more secure SSL context setting than that used by other devices.

Once an SSL context has been configured, all HTTP-based connections use that SSL context to negotiate HTTPS connections, with the following exceptions:

- ProxySG appliance: The SSL context is used only for uploading system images to the ProxySG appliance.
- Web Security Service : Permanently configured with the “cloud-services” SSL context.

Note: The SSL context feature is available in both FIPS and Non-FIPS modes.

Pre-Configured SSL Contexts

The appliance is pre-configured with the SSL contexts shown in the following table, each with a specific purpose.

SSL Context	Keyring	CCL	Description
bluecoat-licensing	bluecoat-appliance	bluecoat-licensing	Used for connections to the Symantec licensing servers.
bluecoat-remote-access	bluecoat-appliance	bluecoat-appliance	Used for remote diagnostics services.
bluecoat-services	bluecoat-appliance	bluecoat-services	Used for connections to the Symantec subscription and heartbeat servers.
cloud-services	bluecoat-appliance	bluecoat-appliance	Used for Web Security Service connections. This context uses the existing bluecoat-appliance keyring and CCL. You cannot remove it but you can edit it.
default	None	browser-trusted	Used for ingress connection configuration (ports 8082 and 9010), secure authentication services (CCL only applies), and for device connections in FIPS mode (when no other is specified). You cannot remove the default SSL context but you can edit it.

You can create other profiles for your own purposes or edit the profile to suit the environment.

Note: If you are using one of the pre-defined SSL contexts other than default, Management Center performs strict certificate and hostname verification. This means that the device's signing certificate must be included in the CCL specified in the SSL Context.

Specify an SSL Context

Using this feature, you can specify an SSL context in the following ways:

- Globally, using the device-communication CLI command.
- Per-device, using the SSL context option in the device's Connection Parameters when adding or editing a device (**Network > devicename > Edit > Connection Parameters**). If a global SSL context is set, the device-specific SSL context overrides the global setting.

If a global and individual device SSL context is not set, Management Center:

- FIPS mode: Uses the default SSL context.
- Non-FIPS mode: Trusts all certificates and does not perform hostname verification.

Create an SSL Context

Use the `create ssl-context` CLI command to create an SSL context:

```
(config-ssl)# create ssl-context <context_id> [keyring <keyring_id>] [ccl <ccl_name>] [protocol [ <protocol> ... ]] [cipher-suite [ <cipher-suite> ... ]]
```

See "ssl" on page 920 for more information.

Verify Certificate Trust

To verify certificate trust in the SSL connections, you must specify a CA certificate list (CCL) when creating or editing the SSL context. If no CCL is specified, certificate trust is not validated.

Example

```
(config-ssl)# edit ssl-context mysslcontext ccl beTRUSTED_RSA
```

Edit an SSL Context

Use the `edit ssl-context` CLI command to edit an SSL context.

```
(config-ssl)# edit ssl-context <context_id>
```

Delete an SSL Context

Use the `delete ssl-context` CLI command to delete an SSL context.

```
(config-ssl)# delete ssl-context <context_id>
```

FIPS Mode Considerations for SSL Context

If Management Center is in FIPS mode, the following considerations apply to the SSL context feature:

- When the Management Center is in FIPS mode, HTTP connections to devices are not allowed.
- The FIPS-compliant SSL context accepts only FIPS-compliant configuration. The associated CA certificate list, keyring, and CCL need to be FIPS compliant.
- When FIPS mode is enabled, only FIPS-compliant objects—CA certificate lists, keyrings, and CCLs are available as configuration choices. All non-FIPS-compliant objects are unavailable.
- If you do not specify an SSL context in FIPS mode, Management Center uses the default SSL context.

Refer to the Management Center [documentation](#) for more information about running Management Center in FIPS mode.

Resolve Device Errors

One of the main benefits of using Management Center is to monitor all of your devices from a central location. Without having to log in to each device on your network, you can see if any of your devices have errors, and if so, quickly drill down to pinpoint the problem (unresponsive device, expired license, DNS server cannot be reached, CPU utilization at a critical threshold, and so forth).

Are Any Devices in an Error State?

An error (red) status indicates a component on the device is failing, or is far outside normal parameters, and requires immediate attention. Look at the **Device Status Totals** in the banner; the number inside the red circle indicates how many devices are in an error state.



Which Devices are in an Error State?

Just click inside the red circle to see a list of all devices in an error state. The devices are listed in the Network tab.



The screenshot shows a table with columns: Name, Status, Mode, OS Version, IP Address, CPU, Memory, Actions, and WSS. Two rows are visible. The first row has a blue background and shows 'SGOS 6.7.3.100 Proxy E...' in the OS Version column. The second row has a white background and shows '10.2.1.1' in the IP Address column. The 'Status' column contains red circles with '0 1'. The 'Actions' column has edit and delete icons. A 'Filters' button is on the right.

Name	Status	Mode	OS Version	IP Address	CPU	Memory	Actions	WSS
...	0 1		SGOS 6.7.3.100 Proxy E...				edit delete	
...	0 1			10.2.1.1			edit delete	

Note: When you click a status circle, Management Center is actually setting filters. (Notice the check mark next to Error in the **Filter by** area.) To return the list to displaying all devices, select the check box next to each state.

What Exactly is the Error on the Device?

1. Click inside the red circle in the **Device Status Totals** in the banner. The **Network** tab displays all devices with an error (red) status.

Note: Make note of the Device Type; Management Center is able to display more details about some devices (such as ProxySG appliances) than others.

2. In the device list, select a device and click **Edit** or select the device hyperlink.
3. The **Dashboard** tab lists the errors and warnings found on the device. For example, *McAfee, Inc. expired 6/30/15* or *Unable to reach device*.
4. **Depending on the type of error or warning, you can explore details by clicking the System Metrics and Health Checks sections. Scroll through the items, looking for red and yellow highlighted rows.**

Health Checks			
Name	Info	State	UP/DOWN
DNS Server (1)			
dns.	Successes: 344628	OK	UP
External Services (5)			
drtr.rating_service	Successes: 33579	OK	UP
icap.cas	Failures: 198828	Check failed	DOWN
icap.proxyav	Failures: 397656	Check failed	DOWN
icap.proxyav1	Failures: 396744	Check failed	DOWN
icap.proxyav2	Failures: 198828	Check failed	DOWN
Forwarding (1)			
fwd.Test	Failures: 238547	Check failed	DOWN

- In the **Operations** pulldown, click **Launch Console** to investigate the device directly and fix the problem.

Changes in Management Center 1.9.x and Later (Device Serial Number Errors)

If a monitored device in MC 1.9.x (or later) reports a different serial number, the device will show a health warning. Prior to 1.9.x, the system would ignore the serial number change. A serial number change might occur for various reasons, including:

- A device was returned (RMA) and replaced.
- A different device was deployed to an IP address that Management Center was monitoring, but the credentials stayed the same.
- You re-imaged a VA and gave it a different serial number when setting it up again.

To resolve the warning without losing your configuration, go to the **Network** page and follow steps 6 to 10 in the [RMA the device](#) topic (you don't actually need to return the device to Symantec).

Reactivate Statistics Monitoring

This operation reactivates statistics data collection on monitored devices. Data collection will be reactivated on all devices that have statistics monitoring enabled, but are not currently sending data to Management Center.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Reactivate Statistics Monitoring**.
3. **Job Results:**
 - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).
4. **Schedule:**

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

5. **Name:**

- Verify or change the name and add an optional description.

6. Click **Save**.

Add Multiple Devices at Once

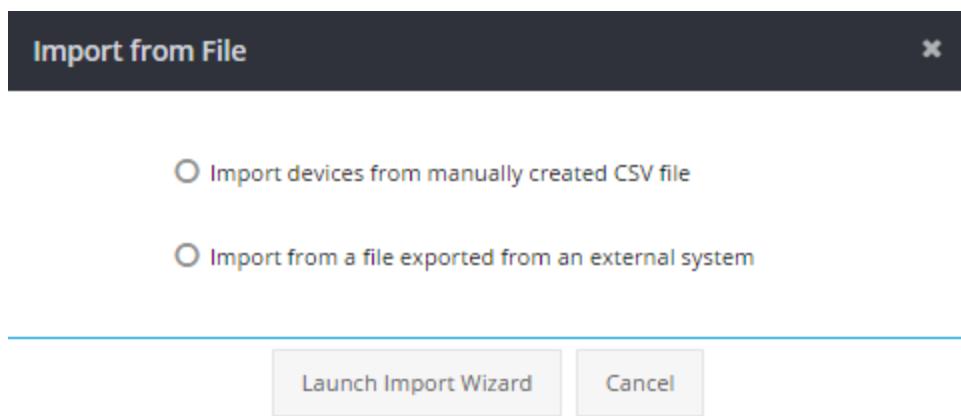
To add multiple devices using a CSV file, you can use Management Center's template CSV file, or you can create your own. You can import multiple devices of various types, including:

- 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 166 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**.

Management Center Configuration & Management

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**.

Tip: 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.

name	deploymentStatus	host	port	userNmae	password	enablePassw ord	collectPdmSt ats
Enter the device name. Each device name must be unique.	Specify the deployment status: DEPLOYED UNDEPLOYED	Enter the IP address.	Enter the port number.	Enter the administrator account for the device.	Enter the password for the device.	Enter the enable password to enter privileged mode on the device.	Specify whether to collect statistics from the device for reporting: TRUE FALSE

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.

Note: 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

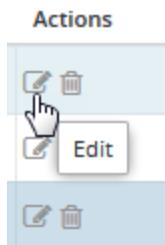
What do you want to do next?	Refer to this topic
Ensure that all devices belong to a hierarchy and group.	"Ensure Devices Belong to Device Groups" on page 169
View information about an imported device.	"Verify Device Details" on page 73
Edit device information.	"View and Edit Device Information" on the next page
Check device metrics.	"View System Metrics" on page 161

View and Edit Device Information

When you select a device and click **Edit**, you can view a variety of device information.

Edit a Device

1. Select the **Network** tab. (Optional) Browse to the hierarchy and folders/subfolders where the device you want to edit belongs.
2. Edit a device in one of the following ways:
 - Select the device and click **Edit**.
 - Click the device hyperlink in the **Name** column of the grid view.
 - Click the edit device icon in the **Actions** column.



Review and Edit Device Information

When you edit a device, the system displays the following tabs:

- **Status**
- **Statistics**
- **Settings**
- **Connection Parameters**
- **Backup**

- Policies
- Certificates
- License

Management Center displays the **Backup**, **Policies**, **Certificates**, and **License** tabs only when those features are supported by the device. For example, Management Center does not display the **Policies** tab for Reporter devices.

Status

View errors and warnings, system metrics, and health check information.

Statistics

Displays a dashboard of important device statistics. See "Monitor Device Health " on page 147.

Settings

- **Basic Info:** 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 160
- **Membership:** View and edit membership.
- **Attributes:** View or change the value on mandatory attributes. You cannot delete "Add Attributes" on page 584.

Connection Parameters

- The authentication type, [public key or credential](#).
- The IP address or hostname of the device
- The username and password you use to authenticate to the device

Management Center Configuration & Management

- The enable password for administrator actions.
- Reporter only—the role (_admin).
- [SSL context](#) setting.
 - Hostname verification and certificate trust validation for device connections is performed when the CCL for the working SSL context is defined.
 - The device-specific SSL context overrides the global context defined in the device-communication CLI command.
- [Host key validation](#) setting.

Backup

View system backup information; restore or delete a backup.

Policies

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.

Tip: The **Local**, **Central**, and **Forward** slots display CPL policy only. See "Create a CPL Policy Object" on page 295 or see "Create a CPL Policy Fragment" on page 344

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

Tip: You can also "Perform an Operation on a Managed Device" on page 77.

Certificates

Displays a list of the certificates installed on the device. Click a certificate to review more details.

License

Provides a list of all installed licenses and their current status.

Determine Your Next Step

What do you want to do next?	Refer to this topic
Ensure that all devices belong to a hierarchy and group.	"Ensure Devices Belong to Device Groups" on page 169
View information about the device.	"Verify Device Details" on the next page
Choose Operations for a Device or Device Group.	"Perform an Operation on a Managed Device" on page 77
Edit device or policy attributes.	"Edit Attributes" on page 587

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, select a device to view, and click **Edit**.
2. Click **Dashboard**. The web console displays information about errors, system metrics, health checks, and resources. To refresh the values, use your browser's refresh function.
3. If you want to launch the device console, select the **Operations** pull-down list (upper-right) and click **Launch Console**.

View Device Certificate Data

To view the certificate data for a device, you must first run the "Collect Device Certificates" on page 78 job. After you run the job, the results can be viewed in the following ways:

- The **Certificates** tab at the top of the **Network** page.
- The **Certificates** tab on the device details page.

Note: At this time, you can view certificate data only for ProxySG and SSL Visibility 4.x appliances.

Important Notes

- Management Center only provides data about certificates. It does not manage the certificates.
- Management Center does not do full certificate validation. That is the responsibility of the device.
- Management Center will parse user-supplied Certificate Revocation Lists (CRLs), but these are only applied to the certificates on that target device, not on all certificates in the device

inventory.

- Management Center does not do full certificate path validation. Do not rely on Management Center for 100% accurate path validation.
- The full PEM of a certificate is not stored. Management Center only stores specific pieces of metadata.
- In some cases, the PEM from an SSL Visibility appliance cannot be extracted, and Management Center is only able to get attributes. In those cases, the certificate details may not be as complete as that provided for other certificates and the proper path might not be known.
- Upgrading and importing certificates, and then downgrading, can lead to orphan data if a device is removed after downgrade.

View Certificate Data

1. Run the "Collect Device Certificates" on page 78 job.
2. Select the **Network** page and click the **Certificates** tab.
3. Hover over a device to review a brief summary.

Device/Group Name	Status	Expires
ProxySG - Advanced Reverse Proxy	20 Expired, 5 Expiring	<6 Months

VA

ProxySG

486 CA Certificates 20 Expired, 5 Expiring

0 External Certificates Green Checkmark

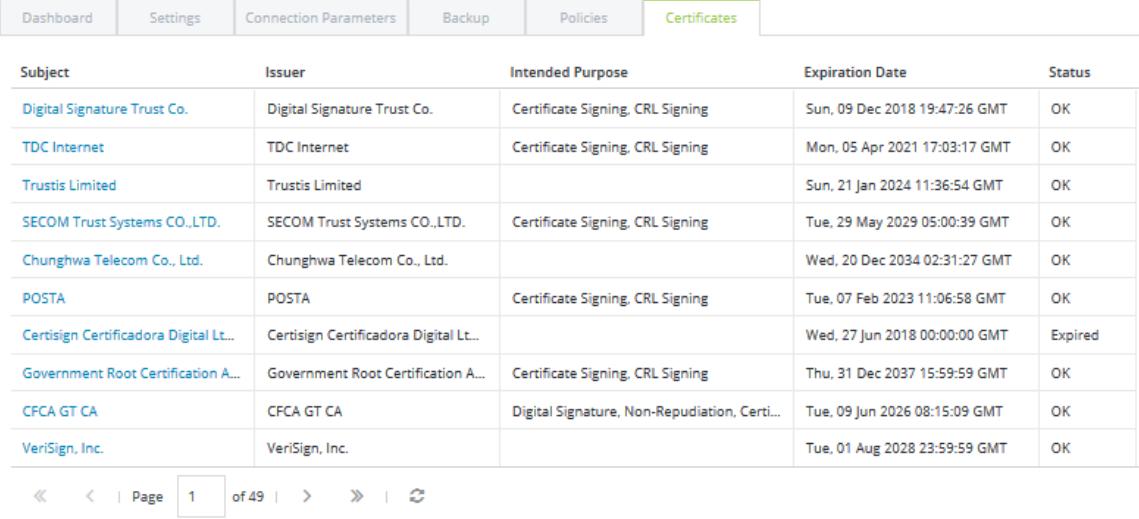
20 Expired Certificates Red Exclamation

5 Certificates expire within three months Yellow Warning

The summary indicates the number of expired and revoked certificates and also reminds you of the number expiring within the next three months.

View Individual Device Certificate Data

1. Run the "Collect Device Certificates" on page 78 job.
2. Select **Network > devicename > Edit**.
3. In the device details page, select the **Certificates** tab to view the certificate data.



The screenshot shows a table of certificates. The columns are: Subject, Issuer, Intended Purpose, Expiration Date, and Status. The table contains 10 rows of data. The status column for all entries is 'OK' except for one which is 'Expired'. The expiration dates range from 2018 to 2028. The issuers include Digital Signature Trust Co., TDC Internet, Trustis Limited, SECOM Trust Systems CO.,LTD., Chunghwa Telecom Co., Ltd., POSTA, Certisign Certificadora Digital Lt..., Government Root Certification A..., CFCA GT CA, and VeriSign, Inc.

Subject	Issuer	Intended Purpose	Expiration Date	Status
Digital Signature Trust Co.	Digital Signature Trust Co.	Certificate Signing, CRL Signing	Sun, 09 Dec 2018 19:47:26 GMT	OK
TDC Internet	TDC Internet	Certificate Signing, CRL Signing	Mon, 05 Apr 2021 17:03:17 GMT	OK
Trustis Limited	Trustis Limited		Sun, 21 Jan 2024 11:36:54 GMT	OK
SECOM Trust Systems CO.,LTD.	SECOM Trust Systems CO.,LTD.	Certificate Signing, CRL Signing	Tue, 29 May 2029 05:00:39 GMT	OK
Chunghwa Telecom Co., Ltd.	Chunghwa Telecom Co., Ltd.		Wed, 20 Dec 2034 02:31:27 GMT	OK
POSTA	POSTA	Certificate Signing, CRL Signing	Tue, 07 Feb 2023 11:06:58 GMT	OK
Certisign Certificadora Digital Lt...	Certisign Certificadora Digital Lt...		Wed, 27 Jun 2018 00:00:00 GMT	Expired
Government Root Certification A...	Government Root Certification A...	Certificate Signing, CRL Signing	Thu, 31 Dec 2037 15:59:59 GMT	OK
CFCA GT CA	CFCA GT CA	Digital Signature, Non-Repudiation, Certi...	Tue, 09 Jun 2026 08:15:09 GMT	OK
VeriSign, Inc.	VeriSign, Inc.		Tue, 01 Aug 2028 23:59:59 GMT	OK

« < | Page 1 of 49 | > » | ⌂

4. Navigate through the list of certificates using the page arrows beneath the certificate list.
5. Sort through the information using the table headers.

6. Select an individual certificate to drill down into its details.

The screenshot shows the 'Certificates' tab selected in the top navigation bar. Below it, a specific certificate for 'TDC Internet' is displayed. The certificate details are as follows:

Common Name:	TDC Internet
Organization:	TDC Internet
Location:	DK
Valid:	Apr 05, 2001 to Apr 05, 2021
Serial Number:	[REDACTED]
Signature Algorithm:	SHA1WITHRSA
Thumbprint:	[REDACTED]
Issuer:	TDC Internet
Self Signed:	Yes

Below this, under 'Certificate Purpose', it states: 'This certificate is intended for the following purpose(s):' followed by two options: 'Certificate Signing' and 'CRL Signing'.

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 147.

Note: 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](#)
 - [Open CLI Shell](#)
 - [Restart](#)
 - "Change Device Password" on page 107
 - [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](#)

Collect Device Certificates

The **Collect Certificates** job collects all certificate lists and associated certificates from the target device and extracts the metadata from them. After running the job, refer to "View Device Certificate Data" on page 73 to view the results.

Note: The **Certificates** tab does not display unless the **Collect Certificates** job has been run for that device.

Supported Devices

The **Collect Certificates** job supports the following devices:

- ProxySG appliance
- SSL Visibility 4.x appliance

Note: The **Collect Certificates** job takes six minutes or more on SSL Visibility appliances.

Collect Certificates

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Collect Certificates**.
3. **Targets:**

Select the devices or groups to collect certificates from.

Management Center Configuration & Management

- Select the **Devices** or **Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

4. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. **Name:**

- Verify or change the name and add an optional description.

7. Click **Save**.

8. Navigate to the device's detail page to view the job results. See "View Device Certificate Data" on page 73

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 make immediate configuration changes on the device. This topic applies to all managed devices.

Launch Device Console

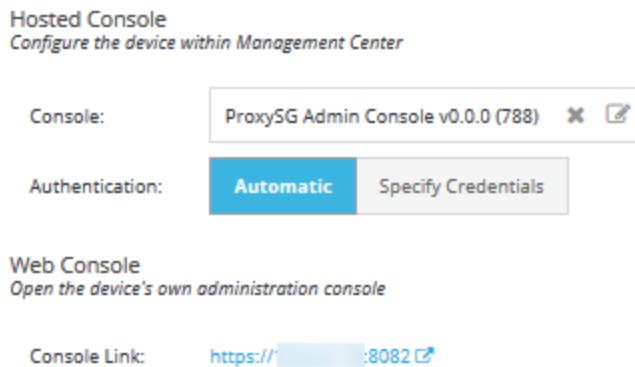
1. Select the **Network** tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. Do one of the following:
 - From the **Operations** drop-down list, click **Launch Console**.
 - or
 - Click the device link to edit the device and select **Operations > Launch Console**.
4. Log in to the device.

Launch ProxySG/ASG Admin Console

Management Center 2.4x and later support the new Admin Console available on ProxySG or Advanced Secure Gateway (ASG) appliances running SGOS 6.7.4 or later. To use the Admin Console, you must first install the package. For more information, see "Install the ProxySG Admin Console" on the facing page.

1. Select the **Network** tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. Do one of the following:

- From the **Operations** drop-down list, click **Launch Console**.
- or
- Click the device link to edit the device and select **Operations > Launch Console**.
4. Select an Admin Console package in the **Console** field. If you have more than one Admin Console version installed, the system displays the compatible versions so you can select the desired version to use.



5. Log into the device. Choose the authentication method—**Automatic** or Manual (**Specify Credentials**).

Note: To log into the ProxySG Admin Console automatically, provide users with the **Device Console (auto login)** permission.

6. Click **Configure** to display the Admin Console.

Install the ProxySG Admin Console

Management Center 2.4.x and later include support for the new ProxySG Admin Console. The improved Admin console does not require Java and has been redesigned to help you complete tasks more efficiently. It is supported on both the ProxySG and Advanced Secure Gateway (ASG) appliances.

To use the new Admin Console, you must first download the installation package from the Management Center or ProxySG/ASG appliance Software Download site on [MySymantec](#). The

packages are signed to ensure their integrity. Management Center validates the package signature when you install the package.

Note: If this is your first time using the Admin Console, refer to the SGOS Release Notes and Administration Guide for your version to learn about features, known issues, and bug fixes.

Admin Console Requirements

- Available only on ProxySG and ASG appliances running 6.7.4 and later.
- To login automatically to the Admin Console, users must have the **Device - Console (auto-login)** permission.
- To provide users with read-only or read-write privileges, assign the **Device - View** or **Device - Manage** permissions.

See "Grant Permissions" on page 572 for more information.

Admin Console Notes

If Public Key authentication is enabled, you will be prompted to enter the device's admin credentials when accessing advanced URLs with the Admin Console.

Step 1—Download the Admin Console Installation Package

1. Go to [MySymantec](#) and sign in with your credentials.
2. Select **My Products**.
3. Find the serial number for your product and click the download icon  to access the **Download Software tab**.
4. Locate the software version to download and expand it to see the files available for

download.

5. If you intend to install the installation package from a URL, copy the URL of the installation package. Otherwise, download the installation package.

Step 2—Install the Installation Package on Management Center

1. Select **Administration > Packages**.
2. Add the file using one of the following methods:
 - Browsing:
 - a. Click **Add Package**.
 - b. Click **Select File** and browse to the file(s).
 - c. Select the file.
 - d. Click **Open**.
 - e. Click **Upload**.
 - Dragging and dropping one or more files:
 - a. Click **Add Package**.
 - b. Drag and drop the files into the **Upload From Browser** window.
 - c. Click **Upload**.
 - Specifying a URL:

Note: At this time, Management Center does not challenge you when downloading from a secure web site.

- a. Click **Add Package**.
- b. In the **URL** field, specify the location of the package.

c. Click **Upload**.

- The system displays the status of the upload and adds the package if it successfully downloads.

Packages				
Package Name	Package Type	Supported Devices	Version	Size on Disk
ProxySG Admin Console	Device Console	Advanced Secure Gateway: 6.7.4+ ProxySG: 6.7.4+	0.0.0 (680)	17.55 MB

Step 3—Launch the Admin Console

To launch the Admin Console, see "Launch a Device Console" on page 81.

Access the CLI of a Managed Device

Management Center offers a central location from which you can open a CLI shell of a managed Symantec device so that you can make immediate configuration changes on the device.

Note: You can also "Access the Management Center CLI " on page 46.

Supported Devices

The following devices are supported:

Note: The CLI shell is not supported for use with Web Security Service, SSL Visibility 3.x, and PacketShaper.

- ProxySG and Advanced Secure Gateway (ASG)

Automatic authentication is supported for both credentials and public-key authentication. When using public-key authentication, the user account is "director" or "management-center," depending on the SGOS version.

- SSL Visibility 4.x and later

- Malware Analysis

Automatic authentication uses the "g2" username and will succeed only if the password is in sync with the user interface credentials.

- Content Analysis

- Reporter

- Security Analytics

Automatic login is not supported because Management Center does not store the credentials.

Authentication Methods and Requirements

You can authenticate to a device's CLI shell using the following methods:

- Automatic authentication

If Management Center stores the authentication credentials, you can click **Login Automatically**. The user must have the following permissions for the device to use this option: <Device, CLI Access (auto-login)>

If a user is granted permissions for automatic authentication, they can also do manual authentication.

- Manual authentication:

Manually enter your login credentials. The user must have the following permissions for the device to use this option: <Device, CLI Access>

Access a Device's CLI

Management Center Configuration & Management

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 **Open CLI Shell**.
 - or
 - Highlight the device, right-click and select **Open CLI Shell**.
 - or
 - Click the device. In the device details page, Click the **Operations** drop-down list and select **Open CLI Shell**.

A new browser window opens.

4. Examine the device's host key to ensure the connection has not been compromised.

Host Key 

Expected Fingerprint:	SHA256:eGShM9wk5R7L5SxSjTWP+reRoNgOxpnyZRw1+R5iiJU=
Device Fingerprint:	SHA256:eGShM9wk5R7L5SxSjTWP+reRoNgOxpnyZRw1+R5iiJU=

Management Center has confirmed the authenticity of the device connection.

Authentication

Enter your credentials for 10.169.2.228 -
Blue Coat SG300 Series:

Username:

Or, log in automatically using the credentials
stored in Management Center

Password:

Login Automatically

Connect

If Management Center has stored the host key information and can verify it, the system displays a green check mark and this text: **Management Center has confirmed the authenticity of the device connection.**

Note: Currently, Management Center only stores the host key information for the ProxySG and ASG appliances.

If Management Center does not store the host key information, it displays the information, along with this message: **Management Center has no recorded host key for this device and so cannot verify the secure connection to the device. Before continuing, confirm that the device fingerprint matches the expected fingerprint.**

5. Log in to the device.

Device authentication requires specific user permissions. See "Authentication Methods and Requirements" on page 86.

Set Boot Image

Create a job to specify the default system image. The job installs the system image and waits for the device to reboot so that it can verify the correct image is installed before reporting success or failure.

Note: If the specified image is already set as the default image or is running, the device will not reboot.

Supported Devices

This job is supported only for the following devices:

- Advanced Secure Gateway
- Content Analysis 2.x and later

- ProxySG
- SSL Visibility 4.x and later

Create Boot Image Job

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Set Boot Image**.
3. **Configuration:**
 - Select the device type for which you are going to set the boot image. The system displays compatible devices in the **Targets** section.
4. **Targets:**
 - Select the **Devices** or **Groups** tab.
 - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
 - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
 - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
 - All selected targets appear in **Selected Targets**.
5. You can select a device group of mixed devices; the system extracts the devices that match your selection (supported device type and version).
6. **Image:**
 - Select the system image to boot.
 - The system displays all images stored on the selected target devices.
 - If a device does not have the selected image, a warning is displayed; the job will still run successfully, skipping those devices.
 - If a device already has the selected image installed, installation is skipped.
7. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

7. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

8. **Name:**

- Verify or change the name and add an optional description.

9. Click **Save**.

Upgrade System Images on Managed Devices

You can install system images to the following devices:

- ProxySG appliance
- Advanced Secure Gateway
- Content Analysis

Note: If you want to retrieve the image from Management Center using the Content Analysis CLI, see "Install Management Center Certificates on Content Analysis to Establish SSL Trust" on page 854.

- Malware Analysis
- SSL Visibility

Restrictions

- Downgrading a Content Analysis 2.x appliance, and retaining your configuration 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.

Refer to the CA and SSL Visibility product documentation and release notes for information about these restrictions.

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 797 for more information.
2. Select **Jobs > Add > New Job**.
3. On the **Add New Job** page, select **Install System Image**.
4. **Configuration:**
 - **System Image:** Select the system image. 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.
 - **Image device type:** This field auto populates depending on your choice above.
 - **Delivery method:**
 - **Upload image to targets**

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

If the target devices are connected to Management Center using SSH public key connections, Management Center will not be able to push the system image because the system does not store the device credentials. If you must push the image to the target device, you must use the [Device Credentials authentication method](#). If device credentials cannot be used, enable the **Download Image from Management Center for targets with Public Key authentication** check box to allow the target device to pull the image from Management Center.

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

Note: 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.

Select **download over secure connection** to have the device retrieve the image from the Management Center file server. This operation requires that Management Center knows the device credentials. During the download operation, Management Center, if necessary, installs its certificate chain on the target device.

Note: ASG does not support image installation using the **download over secure connection** option. Install ASG images using HTTP (described below) or **Upload Image to Targets** delivery methods. For more information, refer to the ASG product limitations.

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
```

Note: If you enable HTTP after using HTTPS, you must delete the HTTPS cookie from your browser to be able to use the HTTP connection for the UI.

5. Targets:

- Select the **Devices** or **Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

6. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

7. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the next page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

8. Name:

- Verify or change the name and add an optional description.

9. Click **Save**.

Troubleshooting

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

- Verify HTTP/HTTPS connectivity between Management Center and the target device(s).
- If Management Center is configured with a server certificate issued by a Certificate Authority, ensure that the certificate chain is added to the "management-center" CA Certificate List.
- Verify that the image being installed is associated with the correct device type.
- Check Management Center and target device logs for errors.

Restart a Device

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

Note: You can also schedule a restart by creating a job. See "Schedule Device Restart " on page 612.

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.

Compare Device Configurations

The **Jobs > Compare Config** job compares the configuration settings of managed devices to those on a "golden" device. The report displays the configuration options that are not identical. The job results are saved to **Jobs > Archived Files**.

Supported Devices

The **Compare Config** job supports the following devices:

- ProxySG appliance
- Advanced Secure Gateway
- Content Analysis
- SSL Visibility 4.x
- Malware Analysis

Compare Device Configurations

1. Select **Jobs > Add > New Job** and click **Compare Config**.
2. **Configuration:**

- Select the source device or source file to be used as the "golden device" for comparison.

Source File: Use the **Save Config** job to save device configurations as a JSON file to be used as the source file for the comparison. See "Save Device Configurations" on page 614 for more information.

Note: If you have saved a configuration file and the system does not show it in the file list, download the file from the file archive and upload it to Management Center (see "Upload Files to Management Center" on page 797).

- Determine whether to compare devices with different software versions.

Note: When selecting this option, you must carefully review the job results because they will likely include false positives. This is because the configuration structure can differ between device versions.

- Enter the JSON paths to include or exclude, or select individual configuration sections. Use hard returns to enter multiple JSON paths.

If you are not familiar with the JSON paths available in your device configuration, select all of the sections. Then, run the job and view the saved configuration file to determine if additional filtering is required. JSON paths are entered using standard JSON path expressions. For example, enter `$.Policy` to specify the Policy node at the root level.

The JSON paths you enter override in the **Paths to Include** section overwrite any of the selected categories. For example, if you enter `$.Auth` and have selected **Tenants**, **Policy Slots**, and **PKI** in the **Sections to Compare**, only the **Auth** configuration will be saved. All categories are ignored.

If you enter one or more JSON paths in the **Paths to Exclude** section, the checkboxes in **Sections to Compare** are used, with the exception of any specified in the **Paths to Exclude**.

3. Targets:

Select the devices or groups to compare to the source device. The selected devices must be running the same system image as the source device.

- Select the **Devices or Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

4. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the next page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. Name:

- Verify or change the name and add an optional description.

7. Click **Save**.

View Job Results

When you run the job, the Job Progress window displays the status of the job. If there are configuration differences, the **Status** shows **Completed with warnings**. To view details about the differences:

1. Select **Jobs > Archived Files**.
2. Select the job and click **Download**.
3. Open the zip file downloaded by your browser.
4. Open the HTML file and review the configuration differences—highlighted in the file.

10.169.48.50 - Blue Coat SG-VA Series		10.169.48.51 - Blue Coat SG-VA Series		
1	{	1	{	
2	"Policy" : {	2	"Policy" : {	
3	"proxy_default" : "0",	3	"proxy_default" : "0",	
4	"mac_key" : **** Not viewable ****,	4	"mac_key" : **** Not viewable ****,	
5	"upgraded_order" : "1",	5	"upgraded_order" : "1",	
6	"initialized_private_network" : "1",	6	"initialized_private_network" : "1",	
7	"restrict_ddos" : "1",	7	"restrict_ddos" : "1",	
8	"coverage_enabled" : "0",	8	"coverage_enabled" : "1",	
9	"restrict_dotx" : "0",	9	"restrict_dotx" : "0",	
10	"maximum_trace_bytes" : "1000000"	10	"maximum_trace_bytes" : "1000000"	
11	},	11	},	
12	"Dotx" : {	12	"Dotx" : {	
	skipping 17 matching lines		skipping 17 matching lines	
30	"16" : "0",	30	"16" : "0",	
31	"17" : "0",	31	"17" : "0",	
32	"18" : "0",	32	"18" : "0",	
33	"19" : "0",	33	"19" : "0",	
34	"0" : "178717781",	34	"0" : "15448744272018285548",	
35	"1" : "0",	35	"1" : "0",	
36	"2" : "0",	36	"2" : "0",	

Viewing Notes

- Identical sections are omitted for the sake of brevity.
- Additions, omissions, and changes are highlighted in green, yellow, and red.
- Arrays only include items that differ.

Remove Unused Tenant Policy

You can delete unused policy from a tenant slot. Management Center considers policy in a tenant slot to be unused if policy is installed on the appliance but does not exist in the tenant slot in Management Center, regardless of whether or not the policy was created or deployed through Management Center. Consider the following examples:

- If you create tenant policy in Management Center, deploy it to an appliance, and then remove it from Management Center, it is considered to be unused.
- If you create tenant policy on the appliance without importing it to Management Center, it is considered to be unused.

Tip: See also "Schedule Removal of Unused Tenant Policy" on page 435.

1. On the **Network** tab, select a ProxySG appliance.
2. From the **Operations** drop-down list, select **Remove Unused Policies**.

3. On the Remove Unused Policy: Devices dialog, select additional ProxySG appliances if required. Otherwise, click **Next**.
4. On the Policies to Remove dialog, all unused tenant policies are selected by default. Clear the policies you do not want to remove. Leave selected the policies you want to remove.
If there are no unused policies, any tenant policy on the appliance also exists in the same tenant slots in Management Center.
5. Click **Next**.
6. The Schedule tab shows job options. For details on running or scheduling jobs, see "Job Scheduling Options" on page 637.
7. Click **Finish** when the job is complete.

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).

A screenshot of a search input field. The field contains the text "10.0.0.1". To the right of the input field is a magnifying glass icon, which serves as the search button.

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.

Configure Hierarchy for Devices and Device Groups

In Management Center, a hierarchy (**Administration > Manage Hierarchies**) is a logical organization that helps you manage your devices. The hierarchy is the highest level in the device structure in Management Center and each device group must reside within one or more of these hierarchies. Management Center organizes its many managed devices into hierarchies with parent and child configurations.

Because you can manage up to 500 devices, creating hierarchies is critical in managing device health, status, deploying policy and handling large jobs. 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.

Create hierarchies to represent geographical regions, organizational or departmental structure, deployment type, or anything else appropriate for your network. For example, a company that has to manage many ProxySG appliances might create the following hierarchies:

Lab A ProxySGs: **SG-LabA**

All ProxySGs on campus: **SG-HQ**

All ProxySGs in the state: **SG-Cal**

Hierarchy Properties

Hierarchies have the following properties:

- Any hierarchies that you create are at the *same level* as the predefined **Location** and **Organization** hierarchies. Once a device group has been created within a hierarchy, it cannot be moved to another hierarchy.
- A device may be associated with only one device group within a hierarchy. A device may be assigned to groups in different hierarchies.

Hierarchies—Inheritance When Used in Policy and Scripts

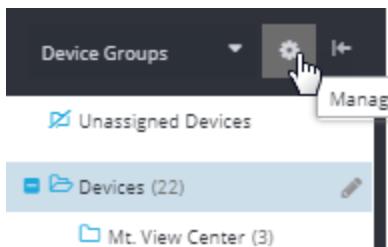
The hierarchical structure of Management Center enables you to more easily manage policy across a large number of devices. When used with policy or scripts, hierarchies allow you to establish a precedence for device [variable substitution](#). The precedence determines which inherited device attributes are used when assigning policy. When a device is a member of several hierarchies, the ranked order of the hierarchy dictates the attribute values that are assigned. Using this 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.

Only hierarchies that have been specifically marked for use in policy are evaluated when resolving device substitution variables. To enable policy use, edit the hierarchy and select **Use this hierarchy for policy assignment, script execution, and substitution variable inheritance**. When a device is a member of several hierarchies, the attribute that is used during policy evaluation depends on the precedence of the hierarchies. See the following sections for additional information.

Note: The concept of attribute inheritance applies to group membership, and does not alter attribute settings configured on individual appliances. Attributes assigned at the device level are not changed when resolving device substitution variables. Devices only inherit device attributes if a specific value has not yet been assigned to the attribute on the device.

Add a Hierarchy

Select **Administration > Manage Hierarchies > Add Hierarchy**. Or click the gear icon  in the left pane of the **Network** page, then **Add Hierarchy**.



In the dialog, configure the hierarchy properties.

Management Center Configuration & Management

- **Hierarchy Name:** Enter a unique name.
- **Comments:** Enter useful comments to differentiate this hierarchy from others.
- **Root Folder Name:** The hierarchy name you entered automatically populates the field. Accept the name if you do not want to create a root folder within the hierarchy. To create a new root folder, enter a name for it in the **Root Folder Name** field. Click **Save**.
- **Policy, scripts:** Select this option when you want to use the hierarchy for policy assignment, script execution, and substitution variable inheritance. When this option is selected, inheritable values or variables are evaluated based on the hierarchy precedence specified in the **Manage Hierarchies** page. If this option is not selected, any specified values are used only for organizational purposes.

Tip: The root folder is the parent folder for all subfolders. For example, in the hypothetical *Beach Names* hierarchy, Beach Names is the parent folder for the subfolders (West Coast Beaches, East Coast Beaches and Gulf Coast Beaches).

After creating a hierarchy, add a device group to the hierarchy. See "Add a Device Group " on page 166.

Manage Hierarchies

Select **Administration > Manage Hierarchies > Add Hierarchy**. Or click the gear icon  in the left pane of the **Network** page.

Manage Hierarchies

Manage Hierarchies							
		Used to assign policy		Description	Root Folder	Device Groups	Devices
Order	Name						
1	Device Groups	✓			Devices	2	25
2	Organization				Company	7	0
3	Location	✓			World	14	7
4	Headquarters				Headquarters	0	0
5	DirectorGroups				Custom Groups	8	9

- To edit a hierarchy, select the hierarchy and click **Edit**.
- To duplicate a hierarchy, select the hierarchy and click **Duplicate**.
- To delete a hierarchy, select the hierarchy and click **Delete**.
- To change the order of precedence, select the hierarchy and click **Move Up** or **Move Down**. The upper-most hierarchy attribute settings are those that will be used for policy evaluation. In the preceding graphic, if a device is a member of a group in both the **Location** and **Device Group** hierarchies, and the two groups have differing values for the same attribute, the attribute value specified in the **Device Group** hierarchy is applied in policy. See "Hierarchy Device Attribute Example" below for more information.

Note: You can delete any hierarchy except for the **Device Groups** hierarchy.

Tip: 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, click **Unassigned Devices** to see the device.

Hierarchy Device Attribute Example

Example Corporation has the following device groups: **Main1** and **DC1**.

Device Group	Hierarchy	Attribute Name/Value
Main1	Main	Campus/California
DC1	DC	Campus/Northridge

As you can see, Example's administrator has [created an inheritable attribute](#) called **Campus** and set the value differently for the two groups. The two groups each contain many devices, but they both include the ProxySG appliance, 198.51.100.14, albeit in different hierarchies.

Example's administrator has created CPL that includes the following substitution variable:

```
$(device.attributes.campus)
```

Management Center Configuration & Management

This CPL sets the value of the campus attribute. The value set during policy evaluation is determined by the order of the hierarchies at the time of policy evaluation. In this example, **Main** has precedence over **DC** because it is higher in the list.

Manage Hierarchies

Manage Hierarchies						
Order	Name	Used to assign policy	Description	Root Folder	Device Groups	Devices
1	Device Groups	✓		Devices	2	26
2	Organization			Company	7	0
3	Location	✓		World	15	9
4	Headquarters			Headquarters	0	0
5	DirectorGroups			Custom Groups	8	9
6	Main	✓		Main		
7	DC	✓		DC		

Practically, this means that if **Main1** is assigned as a target and the policy is installed, the device 198.51.100.14 will inherit the **Campus** attribute value **California** (the value set in the **Main** hierarchy). However, if the admin subsequently moves **DC** above **Main** and installs policy again, 198.51.100.14 would inherit the **Campus** attribute value **Northridge**.

Change Device Password

Use these instructions to change the device password for the admin account, or other account, that was used to register the device with Management Center.

Device Notes

ProxySG and Advanced Secure Gateway (ASG)

- Only the password for the predefined admin account can be changed.
- You can change the Enable password.
- When challenged for the existing password, use the password for the admin account, *not* the Enable password.

Content Analysis (CA) 2.x and later	<ul style="list-style-type: none">■ You cannot change the password for CA appliances running releases prior to 2.x■ You can change the password for other accounts, besides admin.■ You cannot change the Enable password.
SSL Visibility (SSLV)	<ul style="list-style-type: none">■ Only the password can be changed.■ You can change the password for other accounts, besides admin.■ You cannot change the Enable password.

Tip: You can also use the REST API to change a device password. See "Management Center REST API" on page 870 for more information.

Change Password

1. Select **Network** and the device you want to change the password for. Then select the **Operations** drop-down list and click **Change Password**.
2. Configure the job options:
 - **Current Password**
 - ProxySG/ASG: Enter the current account password. For SG/ASG, use the password for the admin account, *not* the Enable password.
 - CA/SSLV: Enter the current password for the account you are changing.
 - **Password Type** - Select **Device** or **Enable**. You cannot change the Enable password on SSLV and CA devices.
 - **New Password** - Enter the new password for the account.
 - **Retype New Password** - Confirm the new password for the account.
3. Click **Save**.

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 161.

Device Sync Details

Different settings are 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

- 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.

Caution: When **Retain segment definitions** is used, all segments must have a ruleset assigned to them. If a disabled segment does not have a ruleset assigned, the transfer will fail. This is by design and enforced by the SSLV device.

Support for Content Analysis (CA)

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

Synchronization areas:

Note: Refer to the [Content Analysis 2.3.x Administration and Reference Guide](#) for more information about these settings.

- **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:
 - Alert Settings
 - Alert Templates
 - SMTP Settings
 - Consent Banner
 - Custom Logo
 - NTP Settings
 - Timezone Configuration
 - HTTP Settings
 - SNMP Settings
 - Predictive Analysis Settings
 - Global Anti-Virus Policy

- Kaspersky Policy
 - Sophos Policy
- **Sandbox Settings:** Includes sandbox service and file-scanning settings.
 - **Firewall:** Includes firewall task settings for the IntelliVM analysis environment.
 - **Patterns:** Includes pattern groups created by users.
 - **Yara Rules:** Includes Yara rules defined on the appliance.
 - **File Hashes:** Synchronizes the whitelist or blacklist file hashes with those on the source device. This operation is not a merge; any existing whitelist or blacklist file hashes on the target devices are destroyed during synchronization.
 - **Scanning Profiles:** Synchronizes base images and scanning profiles for on-box sandboxing. Synchronizing these eliminates the need to create individual scanning profiles on every CA device.

Note: If the base OS image is not on the target, it is transferred before synchronizing the profile.

Note: The **Sandbox Settings**, **Firewall**, **Patterns**, **Yara Rules**, **File Hashes**, and **Scanning Profiles** options apply only to CA 2.x appliances. If you select one of these options, the system does not display any 1.x CA device targets.

Support for Malware Analysis Appliance (MA)

Tip: 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

Synchronize Devices

Follow this basic procedure.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Synchronize Devices**
3. **Configuration:**
 - Select a **Source Device**(*) from the list of available devices. After selecting a source device, click **OK**.
 - Select the check boxes to define **What to synchronize**(*). Available choices are specific to the device and are *not* platform specific.
4. **Targets:**
 - Select the **Devices** or **Groups** tab.
 - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.

- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

5. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. **Name:**

- Verify or change the name and add an optional description.

8. Click **Save**.

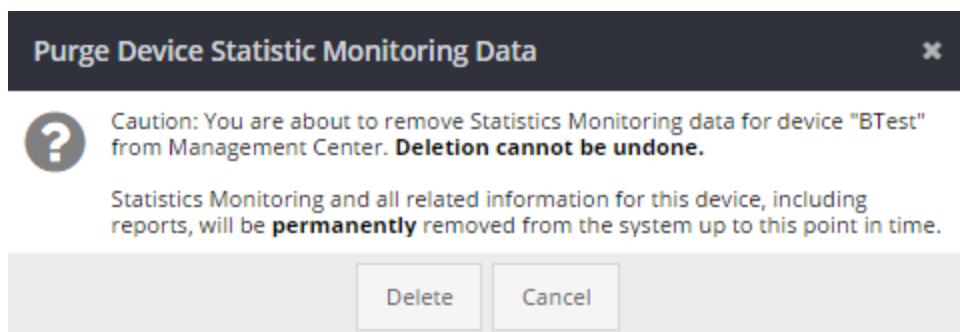
Purge Statistics

To delete the backlog of statistics stored from monitoring a ProxySG, you can purge the data from Management Center storage.

Note: 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 perform more advanced disk maintenance, see # service.

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** menu, select **Purge Stats Monitoring**.

4. Confirm the deletion.



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								
Type	Mode	Name ↑	Device Type	OS Version	IP Address	CPU	Memory	Status
		192.168.1.100...	Malware Analysis	4.2.1.20141110-BETA04				OK
		192.168.1.101...	ProxySG	SGOS 6.6.3.1 Proxy Edition				OK
		192.168.1.102...	ASG	ASG 6.6.3.1			n/a	Errors
		192.168.1.103...	ProxySG	SGOS 6.6.3.0 Proxy Edition				Warnings

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

Allowed Operations for Read-Only Mode

Operation	Allowed?
Edit Metadata	Yes
Edit Attributes	Yes
RMA	Yes
Purge Stats Monitoring	Yes
Import from file	Yes
Assign Group Membership	Yes
Use as a policy target	Yes
Install Policy	No
Remove unused policy	No
Execute script	No

Operation	Allowed?
Backup Device	Yes
Export Backup	Yes
Restore Backup	No
Launch Console	Yes
Activate Device	Yes
Deactivate Device	Yes
Restart Device	Yes
Device sync as a source	Yes
Device sync as a Target	No

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 Existing device from the Deployment status menu.**

1 Device Management Modes

What aspects of this device should be managed by Management Center?

Deployment status:	Existing device	
Edit mode:	Read/Write	Read Only
Monitor mode:	Monitor health	Do not monitor
<input checked="" type="checkbox"/> Collect statistics for this device		

Note: 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 Read-Only Mode

1. Select the **Network** tab.
2. Locate the device, select it, and click **Edit**.
3. In the **Settings** tab, select **Read Only**.
4. Click **Save**.

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.

Note: 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 102.
3. (Recommended) Verify that the device is the one you want to delete. See "Verify Device Details" on page 73.
4. Select the device, and then click **Delete**. The device and all related information, including reports is permanently removed from the system.

Caution: 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.

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 "Enable Device Health and Statistics Monitoring" on page 155.

Note: 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 660.
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.

Note: 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.

RMA Device ×

RMA device: [REDACTED] - Blue Coat SG300 Series

Serial Number

Serial Number detected on device: [REDACTED]

Provide previous Serial Number: *

Statistics Monitoring

Do you want to migrate the Statistics Monitoring data, and associate it with the new serial number, to retain the existing statistics?

migrate Statistics Monitoring data

ignore Statistics Monitoring data (lose old data)

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**.

View Security Analytics API Key

The Security Analytics API key is used for web services APIs. It is not visible on the web UI by default.

For more information about this procedure, refer to the [Security Analytics documentation](#).

Retrieve the API key

- Navigate to the Security Analytics appliance.
- Log in to the Security Analytics appliance with the account that you wish to use for Management Center authentication.
- Select *Account Name* > **Account Settings** and click **Reset API Key** to view and copy the API key.
- In the **Account Settings** dialog, click **Reset API Key** to view and copy the API key.
- After you close the **Account Settings** dialog, the API key will not be available again. You must click **Reset API Key** to generate a new key.
- When you click **Reset API Key**, the previous API key is deleted.
- A new user account does not have an API key until the user logs in to the web UI, opens **Account Settings**, and clicks **Reset API Key**.

Reference: Device Communication

This topic describes Management Center to device communication.

ProxySG Appliance SSH Ciphers

Management Center uses the following ciphers for SSH communication with the ProxySG appliance:

- aes256-ctr
- aes192-ctr
- aes128-ctr

If you cannot add a ProxySG appliance because it is in FIPS mode and the ciphers used are not on Management Center, use one of preceding ciphers on the ProxySG appliance.

All Other Appliances

Management Center uses HTTPS to communicate with all devices except the ProxySG. Management Center restricts communication to the TLSv1.1 and TLSv1.2 protocols and a variety of ciphers that use:

Management Center Configuration & Management

- ECDHE/DHE key exchange
- RSA/DSA certificate authentication
- 128 – 256 bit AES stream cipher with optional CBC/GCM modes
- SHA – SHA384 message authentication

Supported Key Exchange in Management Center Operations that use SSH/SCP

Management Center supports the following key exchange algorithms for SSH/SCP connections:

- DHGex
- DHG
- Curve25519

If a user attempts to export a backup to a server using SCP and the target server does not support the at least one of the preceding key exchange algorithms, the export may fail with the message `A connection could not be established or The secure handshake failed during key exchange.` This applies to any operation using SSH/SCP, for example, importing backups.

Receive Alert Error Notifications

This page describes the options on the [Administration > Settings > Alerts page](#). Management Center generates two different types of alerts:

- Alerts for Management Center itself.
- Alerts for errors detected by Management Center on devices it is monitoring.

These alerts cause SNMP events to be raised if [SNMP alerting](#) is enabled on Management Center.

Management Center Alerts

The following alerts are generated for events that occur on Management Center itself (not to be confused with [alerts that occur on managed devices](#)):

Description	Message Example or Description
Internal critical errors.	<p>Subscription URLs are not installed.</p> <p>Unable to complete the subscription download process on Management Center. Currently, only the Web Application Firewall (WAF) component uses subscriptions.</p>
Database disk quota warning.	Statistics Monitoring DB exceeded allowed disk quota. Collector to reject upload requests.
Errors with auditing user actions.	Unable to write audit record, user: <username>, event: <action>.
License errors due to duplicate serial or server avoidance.	<p>License error <message_string>.</p> <p>If the system detects that a VA is being used in a way that precludes Management Center from validating the license. This is case is called "server avoidance" and results in an alert.</p> <p>Note: Server avoidance alerts only occur with VAs that are required to have connectivity to the Symantec license service. Hardware and special offline VA licenses are not affected.</p>
License expiration warnings.	<p>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.</p>
	 <p>The web console banner displays an alert for each licensed component.</p>
	<p>Once a 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 134 for more information.</p>
	<p>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 <code>(config)# licensing load</code> or see <code>#licensing</code> in the Configuration Management Guide for more.</p>

Description	Message Example or Description
Migration errors during an upgrade.	<p>Migration step: <<i>step_name</i>> 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.</p> <p>A migration step is when the system has to update data as part of the upgrade.</p>
Version repository errors.	<p>If there is an internal error or problem starting Management Center version repository. Management Center uses this service to store the following:</p> <ul style="list-style-type: none"> ■ Device backups taken by Management Center for devices ■ Device scripts ■ Policy objects ■ Unable to initialize the <<i>repository_name</i>> repository.

Alerts for Managed Devices

These are errors that Management Center detects on a managed device. These alerts are triggered from events such as the loss of connectivity or a device taking too long to respond. The associated settings are on the **Administration > Settings > Alerts** page.

To enable the alerts, you must select the global option called **Raise alerts on device errors**. After enabling that option, you can enable or disable individual alerts or change the alert thresholds and severity.

To configure the alert, set a threshold that must be exceeded to trigger the alert and then set the severity. The severity level is what triggers alert notification. The severity can be set to INFO, WARNING or ERROR.

- If the value is set to INFO, the alert will only be recorded on the Alerts page in Management Center. *No external notification is sent*. To configure external notification, you must set the severity to WARNING or ERROR.
- If the value is WARNING or ERROR, an alert notification is sent.

Tip: See "Configure Alerts for Device Errors" on page 133 for more information.

Device Alert Events

The following events can result in alerts for managed devices (if configured):

Description	Message Example or Description
Hardware monitor warnings or critical errors.	<p><<i>monitor_name</i>> has exceeded <<i>level_name</i>> level of <#>%, current usage is <#>%.</p> <p>If one of the Hardware Monitor Setting (Administration > Settings > Hardware Monitor Settings) values is exceeded, an alert is generated. You can disable these using the Monitor Enabled setting.</p> <p>Also:</p> <ul style="list-style-type: none"> ■ Memory Usage — When the memory utilization of the device exceeds the configured threshold. A distribution metric is used to prevent a short term spike from causing an alert. ■ CPU Usage — When the CPU utilization of the device exceeds the configured threshold. A distribution metric is used to prevent a short term spike from causing an alert.
Device errors.	<ul style="list-style-type: none"> ■ Device Health Response Time — On average, the time it takes for a device to reply with its health status exceeds the configured time. ■ Device Details Response Time — On average, the time it takes for a device to reply with its details (OS, name, etc.) exceeds the configured time. ■ Device Connection Failure — The number of consecutive times a device has a connection failure, meaning we could not establish a connection or it failed to respond at all. ■ Error Health Check — The number of consecutive times a device reports a health check error. For example, a ProxySG appliance's DNS lookup is failing. ■ Warning Health Check — The number of consecutive times a device reports a health check warning.

Description	Message Example or Description
Device license errors.	<ul style="list-style-type: none"> ■ 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. License component <<i>component_name</i>>, for device <<i>device_name</i>> has, or will, expire on <<i>date</i>>. ■ If a device license expires, the warning alert closes to open an error alert. State changed from NEW to CLOSED. System closed alert because license expired. ■ If a device license, in the warning state, is renewed, the warning alert closes because of subscription renewal. State changed from NEW to CLOSED. System closed alert because license was renewed. ■ If a device license, in the error state, is renewed, the error alert closes because of subscription renewal. State changed from NEW to CLOSED. System closed alert because license was renewed.

Note: You can disable all of the Hardware Monitor Settings by deselecting the **Monitor Enabled** setting . (**Administration > Settings > Hardware Monitor Settings**)

Next Steps — Configure SNMP and SMTP Notification

After configuring your alerts, you will not receive alert notification unless you configure the SNMP (**System Settings > SNMP Alerts**) and SMTP (**System Settings > SMTP Alerts**) communication settings. You must provide information for the SNMP destination and the SMTP mail server. You must also set the **What to Send** option to **ERROR** to receive alert notifications for alerts not controlled by the **Administration > Settings > Alerts** page. These include internal alerts within Management Center (HW failure, memory issues, and so on). See "Configure SNMP Alerts" on page 131 and "Configure SMTP Alerts" on the facing page for more information.

Configure SMTP Alerts

Configure the mail server for sending device health monitoring notifications from Management Center and specify which administrators receive the alerts. These settings are for sending the alerts received from managed devices, not from Management Center itself.

Note: These settings are different from those in the SMTP CLI command. The CLI SMTP settings are for configuring SMTP settings for Management Center core health monitoring notification.

Note: The message supports basic HTML formatting, which might not be supported by all email clients.

1. Select **Administration > Settings**.
2. Click **SMTP Alerts** on the left. SMTP fields display on the right.
3. Specify SMTP settings.

Setting	Description	Input Value/Format
What to send*	Specify OFF to turn off e-mail notification or ERROR when errors occur with mail delivery. Note: If you select OFF, device alerts are still sent if SMTP alerting is enabled on the Administration > Settings > Alerts page.	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. Enter the username and passphrase, if applicable.

5. Specify the variables to use in the subject line and message body. You can use the following:

- \${severity}
- \${priority}
- \${category}
- \${state}
- \${message}
- \${sourceType}

Shows the source of the alert, typically DEVICE but can be other sources. If the source is DEVICE, the following are available:

- \${device.name}
- \${device.model}
- \${device.host}
- \${device.name}
- \${device.type}
- \${device.osVersion}
- \${device.serialNumber}

6. 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.

Note: Click **Cancel** to remove your current changes and revert to the default or last saved settings.

7. Click **Activate** 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

If configured, 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. By default, no SNMP traps are sent.

Tip: For information on SNMP best practices, see "Management Center: SNMP Monitoring Best Practices " on page 778.

To enable SNMP traps, see the following:

- "Configure Alerts for Device Errors" on page 133

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).

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

This section describes how to configure SNMP settings for Management Center. For best practice information, refer to the [Management Center 2.1 SNMP Monitoring Best Practices](#).

Note: If you want to enter a password for the SNMP traps, see "Configure the SNMP Agent Password" on page 777.

Management Center Configuration & Management

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

Setting	Description	Input Value/Format
What to send*	Specify OFF to turn off SNMP notifications or ERROR when errors occur with the SNMP traps.	OFF ERROR
SNMP Destination IP*	Specify an IP address for the listener.	Example: 192.0.2.0
SNMP Destination port*	Specify the port for the listener.	Example: 155
SNMP Version*	Specify the protocol version for the SNMP listener.	2 3
Community	A password that allows access to a device's statistics (transmitted in plaintext).	Enter the password. See "Configure the SNMP Agent Password" on page 777.
Engine ID	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.	Click generate to generate the engine ID.
Security	Use name used to access the management module. Applies to SNMPv3 only.	Enter the username.
Auth Protocol	The authentication protocol algorithm to use. SHA is the default. Applies to SNMPv3 only.	SHA MD5
Auth Passphrase	Passphrase to use for authentication. Applies to SNMPv3 only.	Enter the passphrase.

Setting	Description	Input Value/Format
Priv Protocol	The protocol to use for SNMP message privacy. AES is the default. Applies to SNMPv3 only.	AES DES
Priv Passphrase	Passphrase to use when encrypting messages. Applies to SNMPv3 only.	Enter the passphrase.

- Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

Configure Alerts for Device Errors

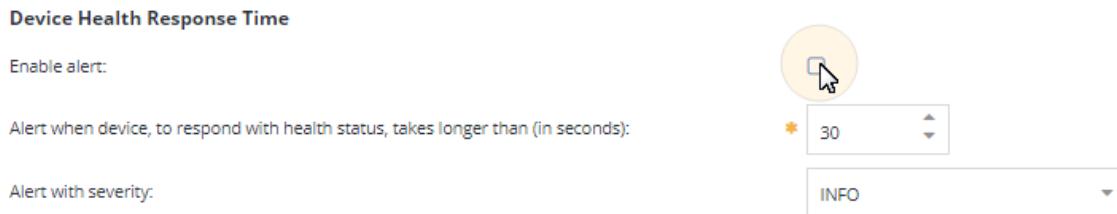
Use the settings on the **Administration > Settings > Alerts** page to enable alerts, configure alerting thresholds, and specify alert severity.

About Alerting

- An alert is raised according to the severity you configure (INFO to 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.
- SNMP or SMTP messaging can be enabled for each alert.

Enable Alerting

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



4. Examine the threshold settings for the alert and change them if desired.
5. Specify the severity to trigger the alert: **INFO**, **WARNING**, or **ERROR**.
6. Optional—Indicate whether to send [email notification](#) for the alert.
7. Optional—Enable [SNMP trap](#) notification.
8. Click **Save**.
9. Click **Activate** to restart the service.

[View Alerts](#)

To view and manage your alerts, see "Manage Alerts" below.

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.

Note: This is different from the message viewer. To view messages in the Recent Messages pane, see "Read Messages and Alerts" on page 864.

Related Tasks

- "Create Alerts" on page 142
- "Edit Alerts" on page 144
- "Configure Alerts for Device Errors" on the previous page
- "Receive Alert Error Notifications" on page 124

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).

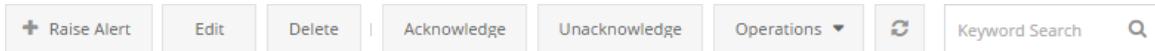


- **Navigation** options at the bottom allow you to go to specific pages.



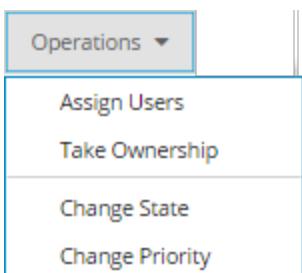
« < | Page **1** of 1 | > » | Page Size **50** ▾

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



+ Raise Alert Edit Delete | Acknowledge Unacknowledge Operations ▾ Keyword Search 

- 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.



Sort Alerts

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

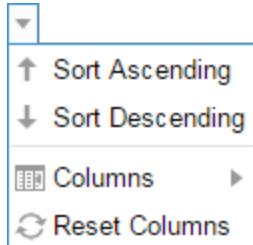
Management Center Configuration & Management

different columns.

*Indicates columns that are NOT shown by default

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

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.

Tip: 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](#).

Note: 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.

The screenshot shows a configuration panel with the following fields:

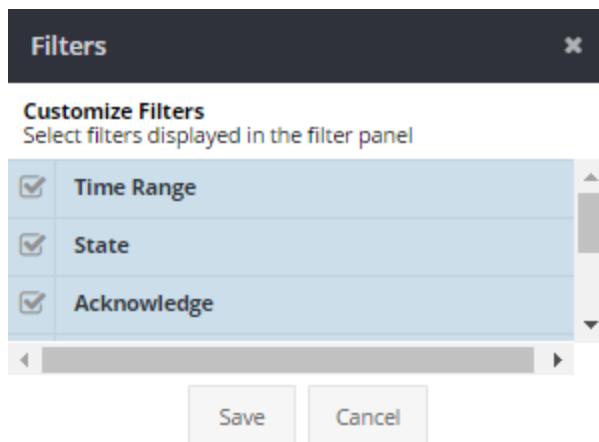
- Buttons:** Apply (green), Clear, and a gear icon.
- Time Range:** A dropdown menu.
- State:** A list of checkboxes for New, Pending, Assigned, In Progress, Resolved, and Closed.
- Acknowledge:** A list of checkboxes for Acknowledge and Unacknowledge.
- Category:** A list of checkboxes for Policy, Configuration, License, Operational, Security, Other, and System.
- Priority:** A dropdown menu.
- Owner:** A dropdown menu.

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.

Hour Options	Day Options
Last 1 Hr	Last 24 Hrs
Last 12 Hrs	Last 3 Days
Last 24 Hrs	Last 7 Days

State

Select the alert current status(es).

Option	Description
New	New or unworked issues.
Pending	Already known issue, but resolution hasn't started.
Assigned	Assigned to a specific user.
In Progress	A resolution has been started.
Resolved	The issue has been resolved.

Management Center Configuration & Management

Option	Description
Closed	The issue has been closed. This can be used whether or not the issue has been resolved.

Acknowledge

Select the receipt status(es).

Option	Description
Acknowledge	Alert received by owner.
Unacknowledge	Alert not received by owner.

Category

Select the element(s) affected.

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

Priority

Select the importance level of resolution.

Priority Level
Low
Medium
High
Urgent

Owner

Select the current owner.

Note: 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 (x) within the search box.

Navigation

Navigate between pages and set navigation options.

« < | Page of 1 | > » | Page Size ▾

Management Center Configuration & Management

Option	Icon	Description
Beginning	<<	Go to the first page.
Back	<	Go back a page.
Page Number	Page <input type="text" value="1"/> of <input type="text" value="1"/>	Current page number and total page count. Type a number to go to a specific page.
Forward	>	Go forward a page.
End	>>	Go to the last page.
Refresh	⟳	Refresh the list.
Page Size	Page Size <input style="width: 40px;" type="text" value="50"/> ▾	Number of alerts displayed per page.

Create Alerts

To create an alert, go to the **Alerts** page using one of the following methods:

- Select **Administration > Alerts**.
- Click the **Alert Notification**  icon. This shows the number of open (or unresolved) alerts.

Create an Alert

1. Click **Raise Alert** to create a new alert.



Alert Message

Received:	
Message:	*
1024 of 1024 characters left	
Severity:	Info
Description:	
4096 of 4096 characters left	
Notifications:	<input type="checkbox"/> Send eMail <input type="checkbox"/> Send SNMP Trap

2. Enter the message you want to associate with the alert.

3. Assign a severity.

Option	Icon	Severity Level	Definition
Info*		Low	Little or no impact.
Warning		Medium	Potential to cause errors.
Error		High	Errors found.
Fatal		Critical	System failure.

4. Assign a priority.

5. Assign a state.

6. Set the 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 524.

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

7. Assign a category, which describes the element affected by the alert.

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

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

Tip: 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.

9. Specify alert notification settings. The alert can trigger an email or SNMP trap. The notifications use the information specified in the [SMTP](#) and [SNMP](#) configuration settings.
10. Click **Save**.

Edit Alerts

To edit an alert, go to the **Alerts** page using one of the following methods:

- Select **Administration > Alerts**.
- Click the **Alert Notification**  icon. This shows the number of open (or unresolved) alerts.

Edit Alerts

1. 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.

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

Edit alert information in the **Details** tab. The system displays a summary of the current saved status of the alert. 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.

2. Edit any of the desired information in the **Alert Message**, **Response**, or **Source** panels. To change information with fixed values, click the down arrow to view the list of available states. For example, clicking the down arrow for **Severity** enables you to choose from **Info**, **Warning**, **Error**, **Fatal**.

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

3. When finished with your changes, click **Save Alert**.

Other Alert Management Actions

- 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 776 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.

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

Note: 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.

Alert Change Log

A history of the changes made to the alert are logged in the **Journal** tab beneath the **Notes** field. All notes are collapsed for easy viewing. Click the down arrow to open a note. Actions you can take include:

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

- **Clear** any information typed.

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.

If Management Center is configured to use a server certificate issued by a Certificate Authority, the certificate chain (intermediate/top CA) needs to be added to the **management-center** CA Certificate List (CCL). For Statistics Monitoring, Management Center will install this chain of trust to manage each device in order for it to establish a secure channel with Management Center.

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 77.

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 32 for more information on status colors in various areas of the web console.

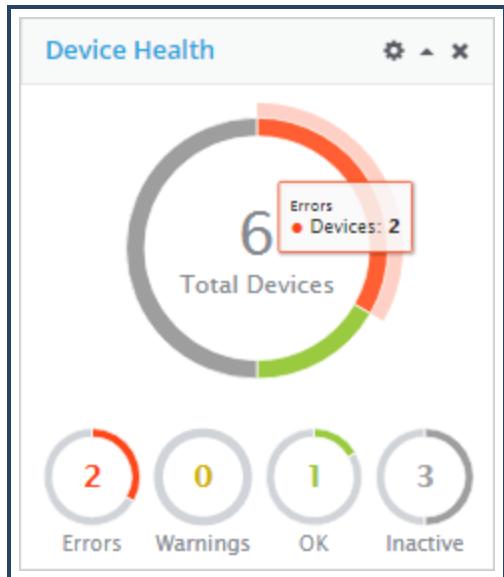
Tip: For more information on monitoring health status on the ProxySG appliance, refer to the *SGOS Administration Guide*.

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.

Management Center Configuration & Management

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



Tip: If you have removed a widget from the Dashboard, you can display it again. See "Change the Dashboard Layout or Refresh Rate" on page 765 for instructions.

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.

Top Problem Devices	
Health	Name ↑
	- Blue Coat SG300 Series
	- Blue Coat SG300 Series

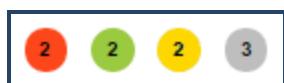
For example, if you [edit](#) the first SG300 Series device, the **Dashboard** tab displays the health status as red with the specific errors and warnings for each device value.



The screenshot shows a banner titled "Errors and Warnings" with a red notification icon containing the number "1". Below the title, there is a message: "Management Center's key is not trusted by the device." This indicates a critical error.

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. See also "Web Console Overview" on page 29.

View Device Health Status

1. Select **Network** and a device or group you want to view. By default the **Health** page is the default view. From here, you can review the information in the **Status** column to view the device health status. If you are viewing group details, the system displays the aggregate health by status.
2. To review all devices by their licensing status, click **Licensing**.
3. To view certificate information for the devices, click **Certificates**.
4. To receive more details, edit the device whose health you want to view. See "View and Edit Device Information" on page 69.
5. Review the errors and warnings, system metrics, and health checks for the selected device. Each device type provides unique health details.

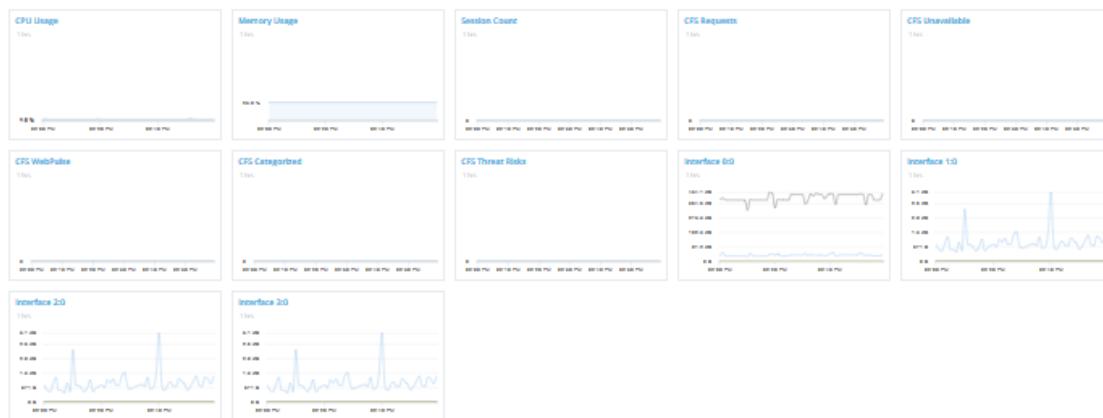
Note: Note: As of Management Center 1.11.1, SSL Visibility appliances running version 4.0 or later support health reporting for **License**, **Load**, **Network**, and **System** attributes with the Up/Down column. Earlier versions of SSL Visibility do not support this functionality.

View Device Statistics

Management Center provides dynamically generated device statistics for each monitored device.

1. Select the **Network** tab.
2. Edit the device whose health you want to view and click **Statistics**.

The system displays a variety of important device statistics. For example:



When **Auto Refresh** is enabled the statistics refresh every 60 seconds. If Auto Refresh is disabled, you can manually refresh the statistics by clicking the refresh icon.



Device Statistics Notes

- 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 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 " on page 61 for more information.

Change Device Health and Statistics Monitoring State

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.

Caution: 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" on page 745 for more information.

Tip: This topic describes how to create a job to change the device monitoring state. This can also be accomplished on individual devices. See "Enable Device Health and Statistics Monitoring" on page 155.

Change Device Monitoring Status

Tip: Deactivating a device is NOT the same as deleting a device. See "Stop Managing a Device" on page 120.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Change Monitoring State**.
3. **Configuration:**
 - **Change Health Monitoring state:** Select to activate or deactivate health monitoring. If you try to activate the device when the connection parameters are not specified, you receive an error. To specify connections parameters, see "View and Edit Device Information" on page 69.

Note: Deactivating a device disables all statistics monitoring.

Change Statistics Monitoring state: Select to change device data collection. You can disable statistics monitoring without deactivating the device. However, Management

Center can only collect statistics from activated devices.

Note: The device status can take up to 30 seconds to change.

4. Targets:

- Select the **Devices or Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

5. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the next page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date

- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. Name:

- Verify or change the name and add an optional description.

8. Click **Save**.

Enable Device Health and Statistics Monitoring

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.

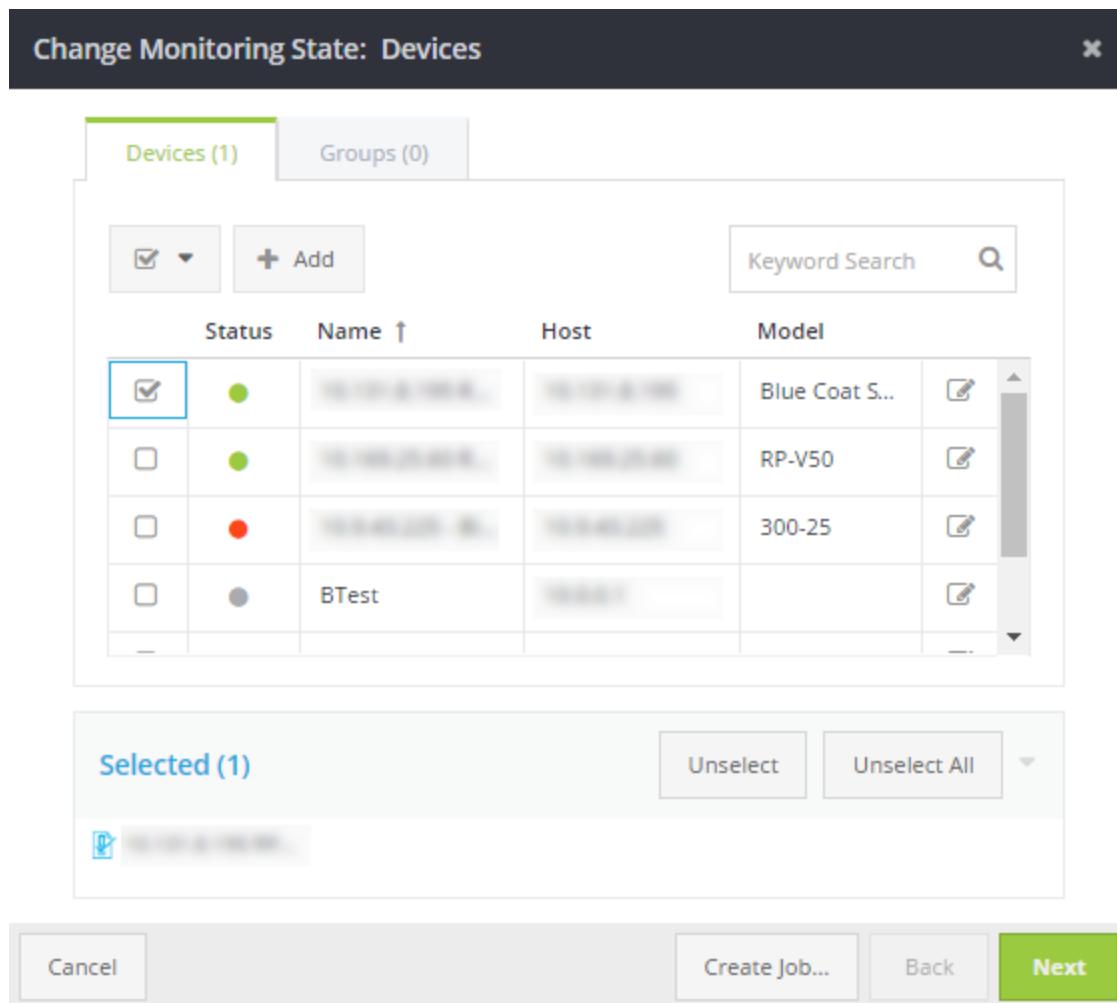
Caution: Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. See "Statistics Monitoring Over HTTPS" on page 745 for more information.

Tip: Any of the **Change Monitoring Status** actions can be saved to a job and scheduled. See "Change Device Health and Statistics Monitoring State" on page 151 for more information.

Change Health Monitoring Status

Tip: Deactivating a device is NOT the same as deleting a device. See "Stop Managing a Device" on page 120.

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 575.
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:

- To activate a deactivated device, select **Activate Device**.
- To deactivate an activated device, select **Deactivate Device**.

Note: Deactivating a device disables all statistics monitoring.

7. Click **Run Now**. The system displays the **Activate Devices - Job Results** window.

Activate Devices - Job Results 100%

Filter by: Complete: 1 Error: 0 Running: 0

Target	Duration	Status	Actions
RP-V50	0.2 seconds	<input checked="" type="checkbox"/> Complete	<input type="button" value=""/>

« < | Page 1 of 1 | > » | Displaying 1 - 1 of 1

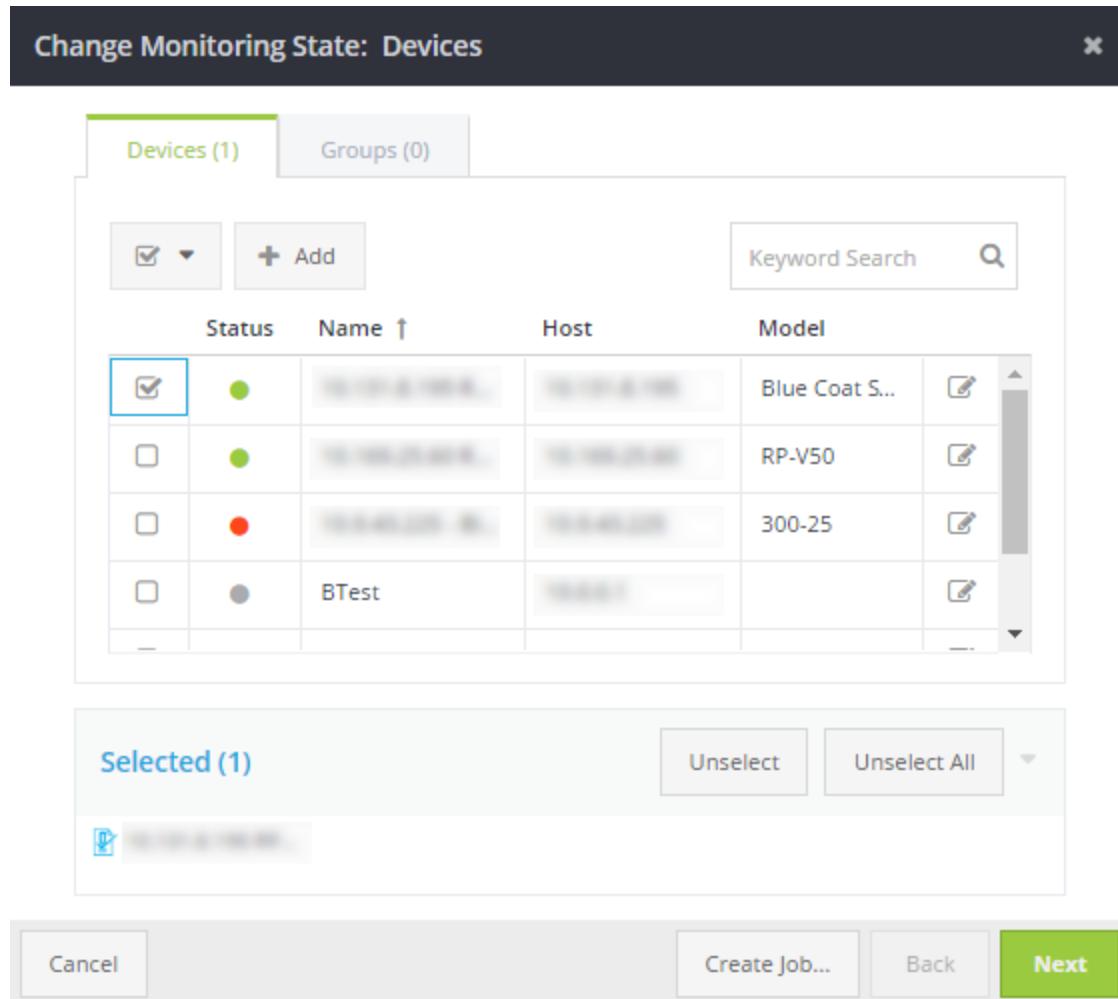
Note: The device status can take up to 30 seconds to change.

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 575.
3. Select the device, and click the **Operations** drop-down list.
4. Select **Change Monitoring Status...**

Management Center Configuration & Management



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**.

Note: 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.

Activate Devices - Job Results  100%

Filter by: Complete: 1 Error: 0 Running: 0 

Target	Duration	Status	Actions
RP-V50	0.2 seconds	 Complete	

« < | Page 1 of 1 | > » |  Displaying 1 - 1 of 1



Note: The device status can take up to 30 seconds to change.

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**:



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 32.

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 121.
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.

Note: 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 795 An example of a ProxySG appliance is displayed in the table shown below.

Metric Description	Status	Current Value	Warning Threshold	Critical Threshold
CPU Utilization	OK	3%	80%	95%
Memory Utilization	OK	25%	90%	95%
Disk 1 Status	OK	present		
Disk 2 Status	OK	present		

Management Center Configuration & Management

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 147.

Name	Info	State	UP/DOWN
- General (4)			
License		OK	Up
Load		OK	Up
Network		OK	Up
System		OK	Up

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 183. You must select a backup from the list to **View**, **Restore**, or **Delete** a backup. See "Monitor Device Health " on page 147. An example of a ProxySG appliance backup information is displayed in the table shown below.

Name	Description	Date/Time ↓	Device Type	OS Version	Exported Date	Restored Date	Pinned
Device Name	SG in Dallas	7/3/15 8:05 PM GMT	ProxySG	SGOS 6.5.5.410			↳
Device Name	SG in Tuscon	6/3/15 7:58 PM GMT	ProxySG	SGOS 6.5.5.410	7/11/15 1:58 AM GMT	7/12/15 3:30 PM GMT	
Device Name	Joe's SG	5/3/15 8:01 PM GMT	ProxySG	SGOS 6.5.5.410	5/23/15 6:01 AM GMT	5/27/15 4:12 PM GMT	↳
Device Name	Matt's SG	5/3/15 8:03 PM GMT	ProxySG	SGOS 6.5.5.410			

Determine Your Next Step

What do you want to do next?	Refer to this topic
Export device backups to an external server.	"Export Device Backups" on page 191
Verify device details in the Overview tab.	Verify Device Details
View device backup in a text editor.	"Monitor Device Health " on page 147

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.

Note: 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.

Add Device Group Attributes

Device Group attributes are **Primary Contact** or **Location** or are custom attributes that you create.

1. Select the **Administration > Attributes** section.
2. From the **Manage Attributes** list, you can select the following:
 - **Device**
 - **Device Group**
 - **Policy**
 - **Device Script**
3. Click **Device Group**.
4. Click **Add Attribute**. An asterisk denotes fields that are mandatory.

Property	Description or Purpose
Display Name (*)	Name that displays throughout Management Center.
Name (*)	This name contains underscores if spaces are used in the Display Name.
Type (*)	Boolean, String, Decimal, Date, Pick List Note: Depending the Type that you choose the remaining properties will differ.
Format (*)	Alpha, alphanumeric, Email, Phone, Text, URL, World Phone
Min Length (*)	Set a numeric value as the Minimum Length of this attribute (starting with 0). It must be a smaller numeric value than the Maximum Length.
Max Length (*)	Set a numeric value as the Maximum Length of this attribute (1024 character limit). It must be a larger numeric value than the Minimum Length.
Default Value	The Default Value is required when you create or edit a device group.

Property	Description or Purpose
Device Type	Restricts the device attribute to the specified device type. The default is All Device Types .
	<p>Note: The Device Type property applies only to device attributes.</p> <p>If you add a value to an attribute on a device and subsequently change the device type, the value will be deleted from unsupported devices. The system warns you of this before you apply your changes.</p>
Mandatory	All attributes that are checked as mandatory will be mandatory when you add or edit a device. For example, if you define the Location attribute as mandatory, you will be required to enter a location.
Inheritable	Checking this box denotes that the device can inherit the attributes assigned the Device Group.
Description	Give a useful description of this attribute to distinguish it from the others when viewing all of the attributes in a list.

- When you are done editing the attribute properties, click **Finish**. Your new device group attribute is saved in the Device Group Attributes list.

To use attributes that can be inherited from a group, see "Enable Attribute Group Inheritance" below.

Enable Attribute Group Inheritance

To use attributes that can be inherited from a group, do the following:

- Define the attribute as a *device* attribute. Mark the attribute as inheritable.
- Edit the group that you want to assign the value to. Locate the attribute from step 1.
- Set the desired value. Inherited variables are only supported on the default hierarchy (Device Groups). User-defined hierarchies are not supported.
- Create a script with variable substitution.
- Reference the substitution variable in the script as \${device.attributes.*myattr*} where *myattr* is the name of the attribute you defined.
- When the script runs, the system looks for *myattr* on the device.

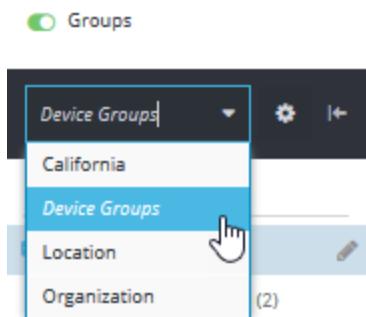
If the value is not set, it looks up the group the device is associated with in the default hierarchy. It then walks the group structure looking for that value. If it finds the value, it will be replaced; otherwise, it is ignored. Group inheritance within hierarchies is described in "Configure Hierarchy for Devices and Device Groups" on page 103.

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.

Note: You can also add a [cluster](#), which represents a group of services bundled in a chassis or in AWS or Kubernetes auto-scaling groups.

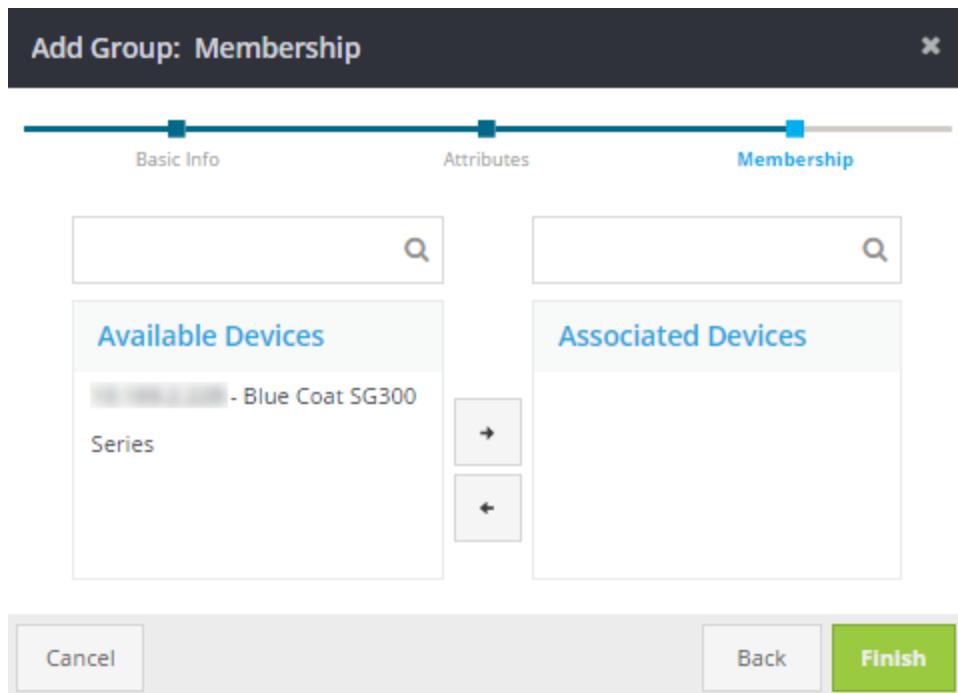
1. Select the **Network** tab. In the left pane, select the [hierarchy](#) in which you want to create the device group.



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.
4. Select a parent group from the **Parent Group** drop-down list. 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 756.

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 window.**



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. See also "Ensure Devices Belong to Device Groups" on page 169 or "Configure Hierarchy for Devices and Device Groups" on page 103.

Tip: You can define attributes for a particular a device, device groups policy and script objects. See "Manage Attributes" on page 583.

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 575.
 - **Membership** - Add or remove devices.
5. Click **Save**.

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 the previous page.

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.

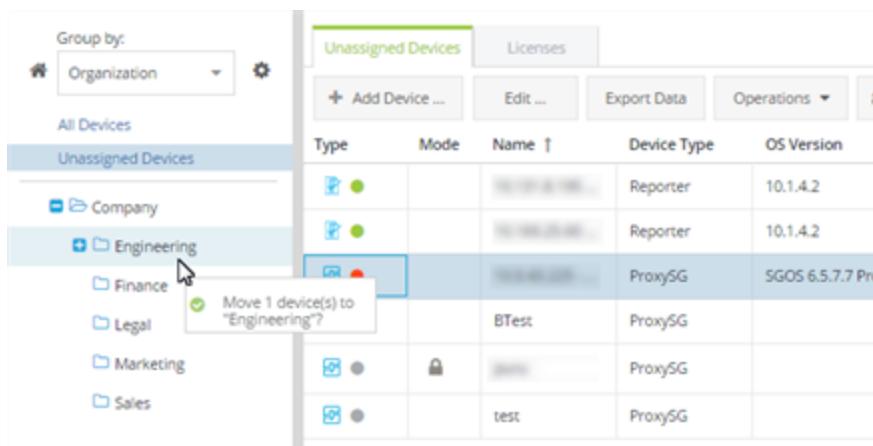
Note: A device group can be inside another device group, but a device group cannot be in multiple hierarchies.

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

Note: 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.



Add a Group to Represent Chassis or Cloud Services (Device Cluster)

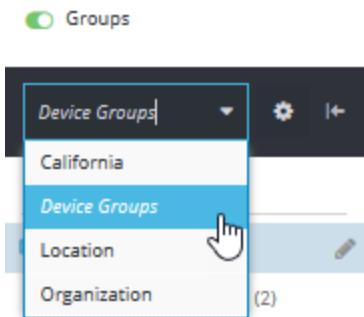
A device *cluster* is a special type of group that represents a group of services bundled in a chassis or in some virtualization auto-scaling environment such as AWS. In addition to organizing devices, a cluster can store meta data about how a device operates within that group. When AWS autoscaling or other software is managing the devices in the cluster, that software will communicate cluster membership information directly to Management Center—users will not be able to change cluster membership.

All operations that can be performed on a group also apply to clusters, with the following restrictions:

- A device can only be assigned to one cluster.
- A cluster must stand alone. It cannot be inside another cluster. One or more groups can be put inside a cluster, however.

Procedure—Add Device Cluster

1. Select the **Network** tab. In the left pane, select the [hierarchy](#) in which you want to create the device cluster.



2. (If applicable) Browse to the folder in which you want to create the device cluster. Select **Add Cluster**.

Note: This system does not display the **Add Cluster** option unless the **Folders** option is enabled.

3. In the **Add Cluster: Basic Info** dialog, enter a name and a description.
4. Select a parent group from the **Parent Group** drop-down list. Click **Next**.
5. In the **Add Cluster: 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 756.
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 Cluster wizard displays the **Add Cluster: Membership** window.
8. Select devices from the **Available Devices** list and add them to the **Associated Devices** list.
9. Click **Finish**. The new device cluster is displayed under the network tab. See also "Ensure Devices Belong to Device Groups" on page 169 or "Configure Hierarchy for Devices and Device Groups" on page 103.

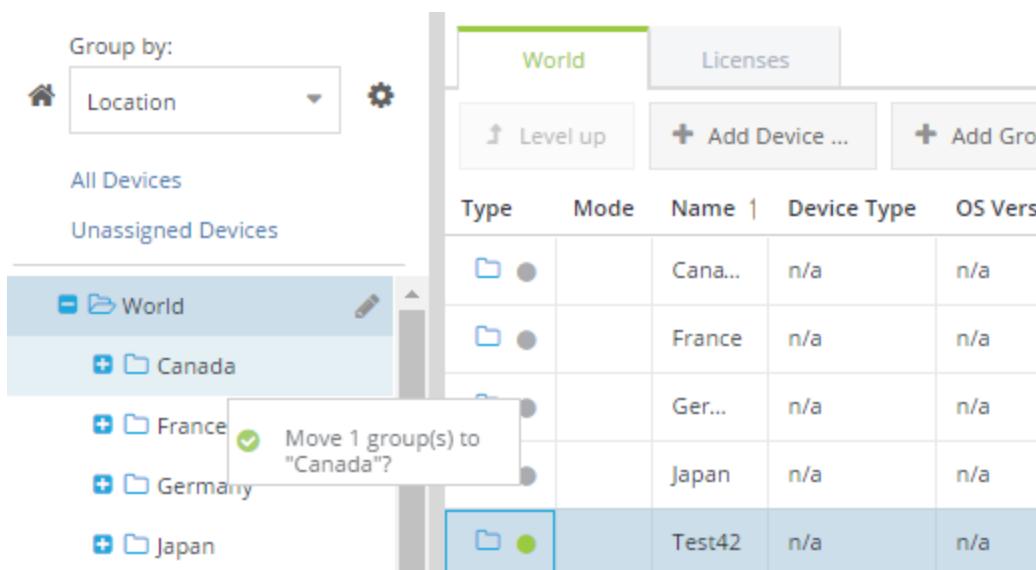
Tip: You can define attributes for a particular device, device groups, clusters, and policy and script objects. See "Manage Attributes" on page 583.

Drag and Drop Device Groups

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

1. Click the **Network** tab. Select a device group. While holding the mouse, drag the device group into another device group or hierarchy.

Note: Device groups cannot be unassigned and will be ignored if you drop them outside of the Device Group.



2. When you drop the group, confirm the move by clicking **OK**.

Note: While you are dragging the selected device group, the message that hovers over the pointer changes according to where Management

Center perceives that you are dropping the device group. See "Move Items" on page 40.

Back Up Device Configuration Now

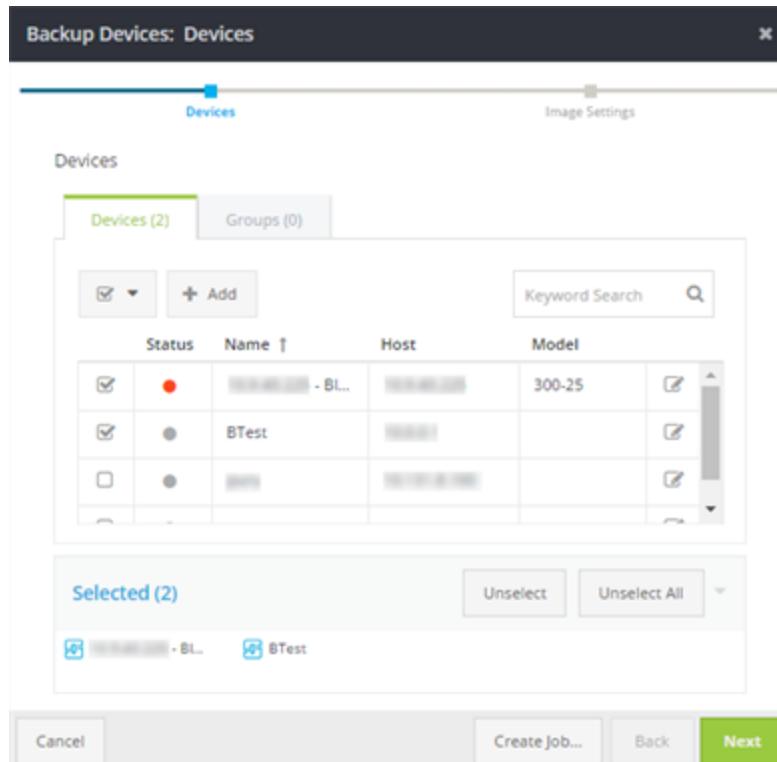
Management Center allows you to initiate and automate the configuration backup of supported devices. You can select one or more devices or device groups to back up immediately or schedule a job for the backup.

Note: 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.

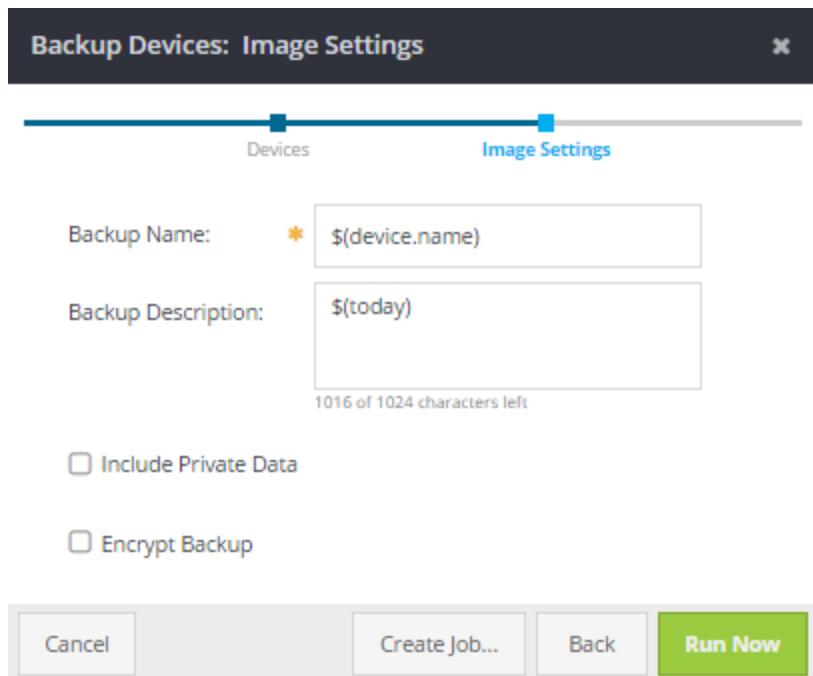
Note: To schedule device backup, see " Schedule Device Back Up" on page 185.

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.**

Management Center Configuration & Management



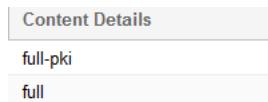
3. Click **Next**. The system displays the **Backup Devices: Image Settings** screen.
4. Enter the **Backup Name** and **Backup Description**. Optionally, you can use variables, as shown in the following graphic. (See "Use Device Information for Backup Job Image Metadata" on page 179.)



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:



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...** See "Schedule Device Back Up" on page 185, for more information.

Next Steps

Task	Topic
List the configuration backups for a device and view the content of a backup file	"View Device Backups" on page 181
Restore a device configuration	"Restore Device Backups" on page 183
Export a device backup	"Export Device Backups" on page 191
Import a device backup	"Import Device Backups" on page 189

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).

Note: 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 166.

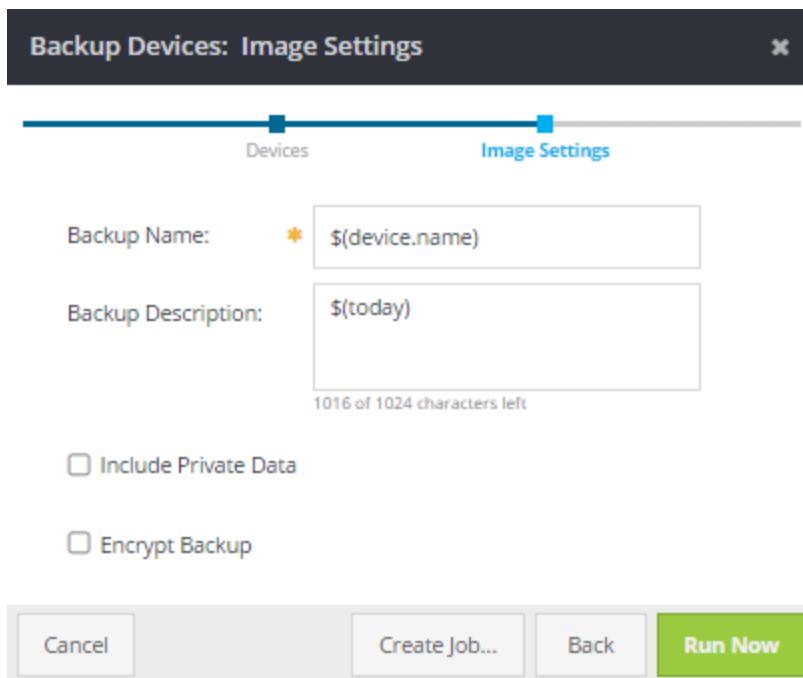
2. Create a **Backup Device** job. Select the device group you created in step 1, and schedule the job to run on a **Periodic** basis, every 7 days starting on a weekend day. See "Schedule Device Back Up" on page 185.
3. Verify the backups are being created for each device in the group. See "View Device Backups" on page 181,
4. Restore a backup when necessary. See "Restore Device Backups" on page 183.

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.

Note: 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.**



Although the backup name is shown as mandatory, use "Use Substitution Variables in Policies and Scripts" on page 312 to replace the words 'Manual Backup'. In the example shown, the device name variable will be replaced when the job is run.

Tip: Use \${today} in the **Description** field of the backup to display the date that the backup is run. If you run the backup now, today's date displays in the backup description.

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 tab of the device.**

Name	Description
10.168.61.103 - Blue Coat SGVA Ser...	Wed Apr 29 03:11:12 UTC 2015
Manual Backup (4/28/15)	VA Backup of workhorse ProxySG
Manual Backup (4/28/15)	VA Backup of workhorse ProxySG

View Device Backups

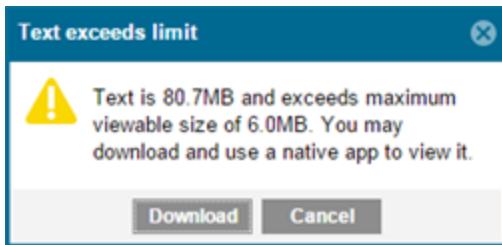
For any device whose configuration you have backed up, you can view a list of backup files as well as view the content of the backup files. Once the list is displayed, you can delete or restore the backups.

Note: 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, then select the device and click the device name hyperlink or click **Edit**.

Note: To configure the maximum number of backups stored per device, see "Set the Number of Backup Slots" on page 195.

3. In the device editor, select the **Backup** tab. 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 the next page for more information.

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.

Note: 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.

Restore Backup Immediately

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 **Edit**, then the **Backup** tab in the editor.
4. In the list of backups, choose the backup version you want to restore.

Note: 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" on page 189.

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. To restore the configuration immediately, click **Restore**. The system displays the running/completed job and more details about the job
 7. (Optional) To view the contents of the backup (configuration), click **View Contents**.
 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**.

Schedule Device Backup Restore

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 **Edit**, then the **Backup** tab in the editor.
4. In the list of backups, choose the backup version you want to restore.
5. Click **Restore**, then **Create Job**.
6. **Backup:**
 - Verify the details of the backup. To view the contents of the backup (configuration), click **View Contents**.
7. **Job Results:**
 - Optional—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).
8. **Schedule:**

Define a schedule for the job. See "Job Scheduling Options" on page 637 for more information.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

9. **Name:**

- Verify or change the name and add an optional description.

10. Click **Save**

Schedule Device Back Up

Management Center allows you to initiate and automate the configuration backup of supported devices. This job backs up the configuration of the selected device(s) on a defined schedule; any supported type of device can be backed up.

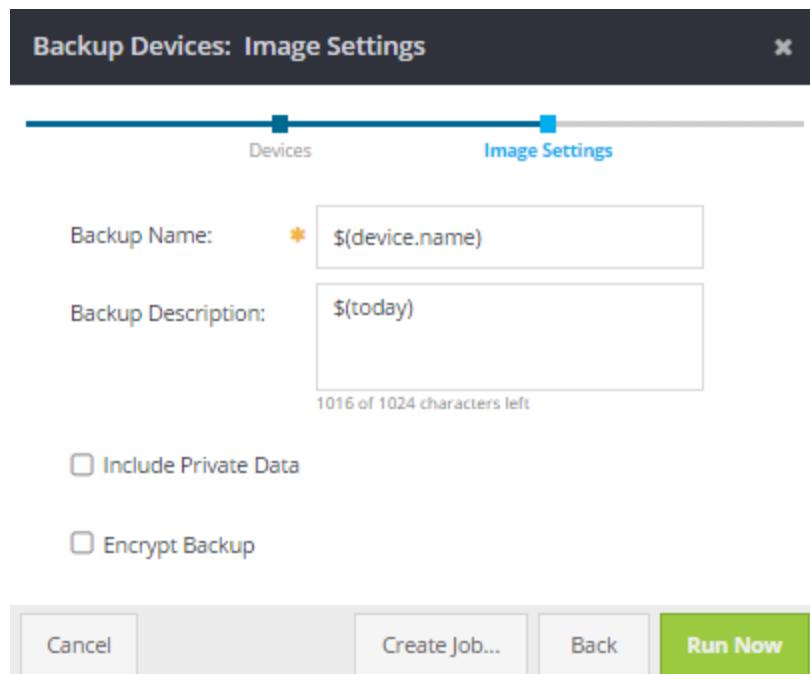
Note: Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

Tip: See also "Back Up Device Configuration Now" on page 174.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Backup Device**.

3. Configuration:

- 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 179.)



- Include Private Data:** Select to include private key data in the backup.

Note: 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:

Management Center Configuration & Management

Content Details
full-pki
full

- **Encrypt Backup:** Secures the backup with the data protection key. 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.

4. Targets:

- Select the **Devices** or **Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

5. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).

6. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. Name:

- Verify or change the name and add an optional description.

8. Click **Save**.

Next Steps

Task	Topic
List the configuration backups for a device and view the content of a backup file	"View Device Backups" on page 181
Restore a device configuration	"Restore Device Backups" on page 183
Export a device backup	"Export Device Backups" on page 191
Import a device backup	"Import Device Backups" below

Import Device Backups

From the Management Center **Network** tab, you can import device backups that you have previously exported. You may want to do this so you can restore an exported backup that has been pruned from Management Center.

Note: Backups created while a device is in FIPS mode cannot be imported to a device that is not in FIPS mode. Conversely, standard backups (non-FIPS mode) cannot be imported to a device in FIPS mode.

Note: SNMP trap settings are not backed up or restored.

Supported Devices

Management Center supports configuration backup/restore/import/export of the following device types:

- ProxySG
- Content Analysis
- Malware Analysis
- SSL Visibility
- Content Analysis 2.1

1. Click the **Network** tab. Select a device from a device group.
2. From the **Operations** drop-down list, click **Import Backups**. The web console displays the Import Backups dialog.
3. From the Import dialog, select one of following:
 - **Import from local file:** If the file is stored on a local system, browse to the backup file.
 - **Import from server:** If the file is stored on a web, FTP, or SCP server, define the URL path to the file and server credentials.
 - **Download URL(*)** - Enter the URL using HTTP, HTTPS, FTP, or SCP.
 - **Username** - Enter the server username.
 - **Password** - Enter the password for this user.
4. **Replacement Strategy(*)**: Select **All** or **As Required**.
 - **All:** Replaces all of the existing backups with the backups that you are importing.
 - **As Required:** Takes into account how many slots that you have provisioned for device backups in **Administration > Settings > General**. If the maximum number of device backup slots is 10, and you have eight backups that are pinned (locked) and you are importing three backups, then Management Center will attempt to satisfy the requirement to replace three backups. As a result, only two backups will be imported because only two backup slots are available.
5. You can prune (delete) backups when exporting to a server, and you can do the reverse when importing backups by overwriting pinned backups. Select the **Replace Pinned Backups** check box. (You can pin backups from the Backup tab. See "View Device Backups " on page 181.)
6. Click **Import**.

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.

Note: 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.

Note: 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 at least one of those key exchange algorithms, the export may fail with the message A connection could not be established or The secure handshake failed during key exchange. This also applies to other Management Center operations that use SSH/SCP.

Enter a unique name and a description for the Export. Click **Next**.

1. Navigate to the New Job: Export Backup page using one of the following methods:
 - Select **Jobs > Add > New Job**. On the **Add New Job** page, select **Export Backups**.
 - Select **Network** and a device or a device group whose configuration backup you want to export. Then select the **Operations** drop-down list and 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.
2. Configure the job options:

- **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.
- **Backups to Include:**
 - **Not Yet Exported:** Include backups that have never been exported.
 - **Previously Exported:** Include backups that were previously exported.
 - **Prune Backups:** 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 195.)
- **Prune Pinned** - Select this option to remove backups, even if they have been pinned (locked).

3. Targets:

- Select the **Devices or Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

4. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

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 637.
7. **Name:**

- Verify or change the name and add an optional description.
8. Click **Save**.

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**.

Note: 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 191.

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

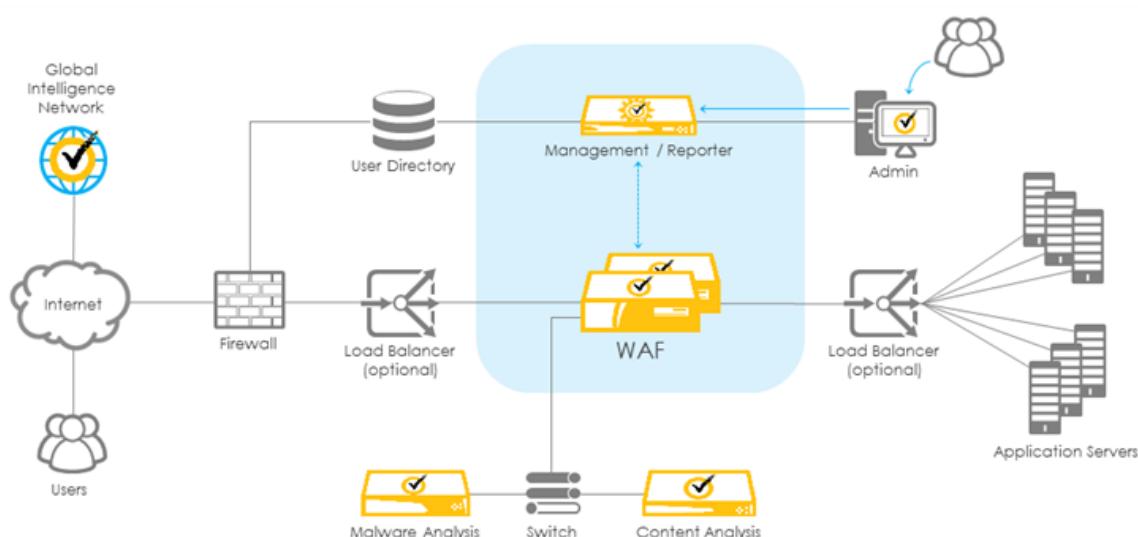
- TACACS settings

Management Center Configuration & Management

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 a Web Application Firewall subscription. The WAF subscription is included with Management Center but must be purchased for each of your ProxySG appliances—it is purchased on a per ProxySG appliance basis. The WAF subscription includes the multi-tenant license that is also required for WAF functionality.

If you have purchased one or more subscriptions, they are automatically downloaded to Management Center. To manage your subscriptions, see the subscriptions information in the *Management Center Configuration WebGuide*. To find the appropriate guide for your Management Center version, go [here](#) and select your version.

Note: To use WAF features, you must ensure that Management Center can connect to <https://subscription.es.bluecoat.com> to download the WAF subscription bundle. If the WAF 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. See "Required Ports, Protocols, and Services" on page 43 for a complete list of required ports and URLs. The WAF subscription cannot be loaded when Management Center is in offline mode.

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](#).

The *Tenant Determination File* 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](#).

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.

Note: 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.
10. Verify your compliance with [PCI DSS Requirement 6.6](#)

About WAF Policy

As described in "Use WAF Policy To Protect Servers From Attacks" on page 199, 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

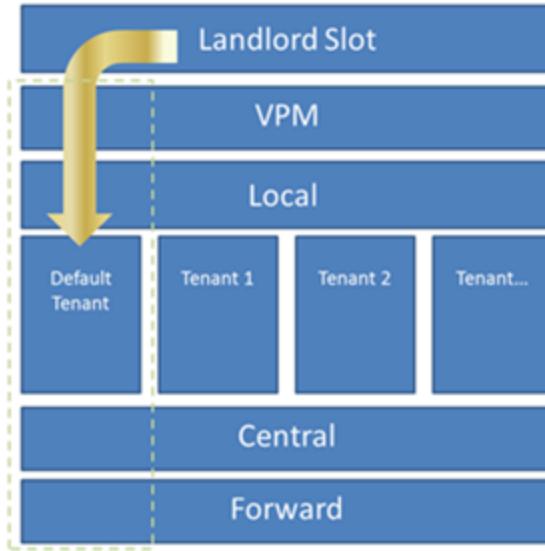
For new WAF deployments, you begin by associating a WAF application with the *default tenant*. The default tenant contains the policy rules applied to all requests that do not match a specific tenant. This ensures that all requests have a base level of WAF protection, and simplifies the deployment process.

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.

Note: 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.

Condition	Available Qualifiers	Example
Client Address	matches	Client Address matches 10.167.3.25
Client Effective Address	matches	Client Effective Address matches 10.167.0.87
Proxy Address	matches	Proxy Address matches 10.140.2.104
Proxy Port	=	Proxy Port = 8080
Port	=	Port = 80

Condition	Available Qualifiers	Example
URL	equals contains matches regex	URL equals http://www.example.com/test
URL Domain	contains	URL Domain contains example.com
URL Extension	equals is not present	URL Extension equals .net
URL Host	equals contains matches regex	URL Host equals http://www.example.com
URL Path	equals contains matches regex	URL Path equals /example
URL Query	equals contains matches regex	URL Query contains ?name=

Tenant Determination CPL Example

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

```
<tenant>

url.path.substring="/Webapp/portal" tenant(webapp_portal)

url="http://domain.com/mail" tenant(domain_mail)

tenant(default)
```

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.

Note: 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:

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.

Note: The Management Center WAF interface leverages option #2 to control tenancy determination via the Tenant Determination object. See "About WAF Policy" on page 202 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.

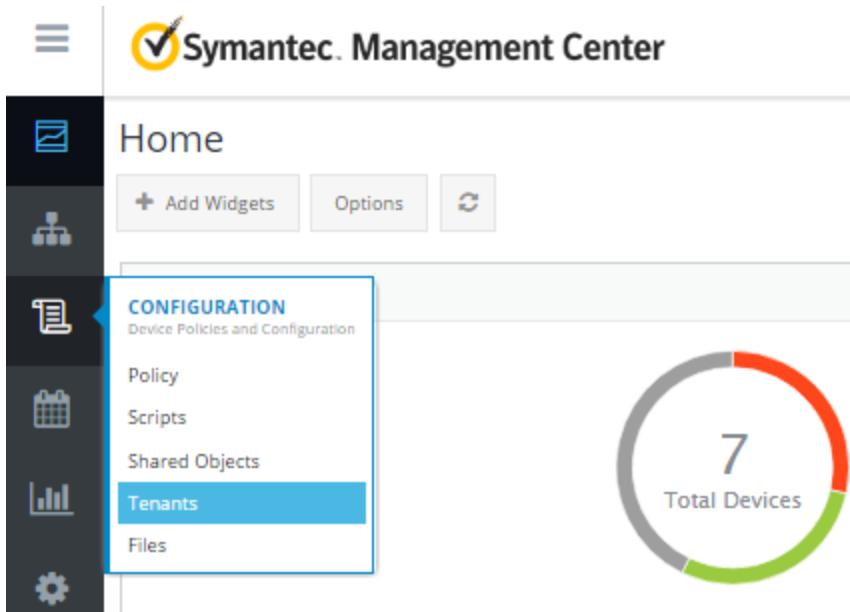
Obtain the tenant identifiers before you write multi-tenant policy in Management Center. For more information on multi-tenant policy, refer to the [Multi-Tenant Policy Deployment Guide](#).

WAF Policy Use

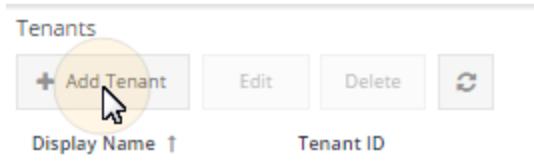
Selecting a tenant is step 2 in "Use WAF Policy To Protect Servers From Attacks" on page 199. A base-level of WAF policy should be installed to the default tenant before any additional tenants are created. This ensures that all requests are processed by the WAF.

Add a Tenant

1. Select Configuration > Tenants.



2. Click Add Tenant.



The web console displays the Add Tenant dialog.

Add Tenant

Display Name: * Outlook_Lab3

Tenant ID: * OutLa3

Description: Test environment
1008 of 1024 characters left

Save Cancel

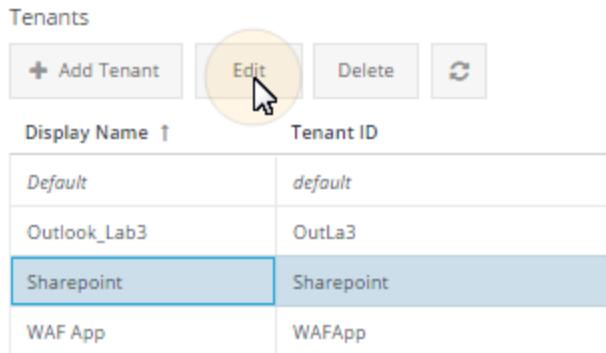
3. Enter a **Display Name**.
4. Enter the **Tenant ID**. This controls the name of the tenant slot where policy will be installed. This ID is also used in the tenant determination CPL using the `tenant()` property.
5. (Optional) Enter a **Description** (up to 1024 characters).
6. Click **Save**.

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.

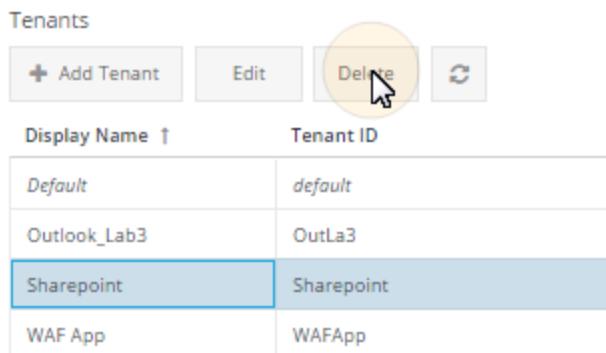


Tenants	
Display Name ↑	Tenant ID
Default	default
Outlook_Lab3	OutLa3
Sharepoint	Sharepoint
WAF App	WAFAApp

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	
Display Name ↑	Tenant ID
Default	default
Outlook_Lab3	OutLa3
Sharepoint	Sharepoint
WAF App	WAFAApp

4. Select **Yes** to delete the selected tenants.

Caution: 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

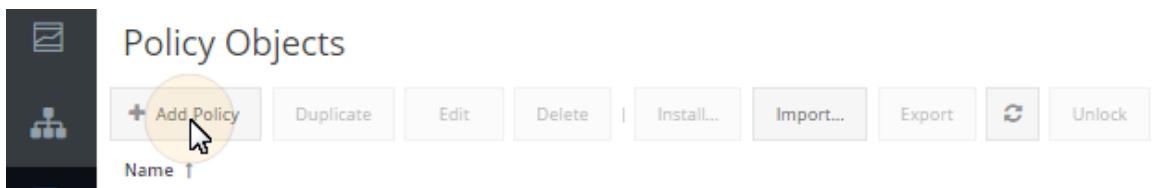
A Tenant Determination file includes policy conditions that control which tenant policy slot is evaluated for an HTTP request. When policy matches a request, the tenant is identified and all policy associated with the tenant ID is applied to the request. On the ProxySG appliance, this file is called the "Landlord Policy." See "About WAF Policy" on page 202 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 199.

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.

Create New Policy: Basic Information

Basic Information Attributes

Policy name: * Landlord

Policy type: * Tenant Determination File

Reference ID: Landlord

Description:

1024 of 1024 characters left

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.

Note: 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 215 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.

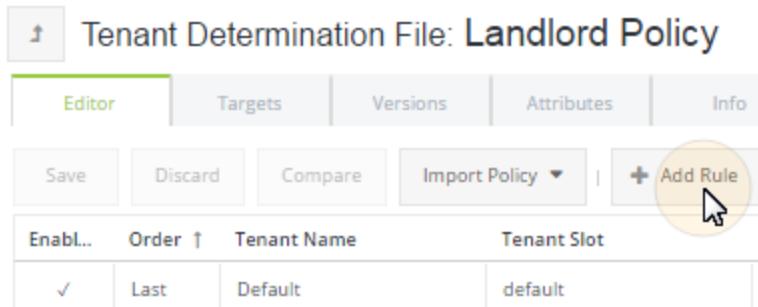
Tenant determination rules specify the properties used to identify a tenant. You specify these properties using a simple, natural language interface that generates equivalent CPL rules.

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

The screenshot shows a user interface for managing policy objects. At the top, there is a toolbar with several buttons: 'Add Policy', 'Duplicate', 'Edit' (which is highlighted with a yellow circle and a cursor icon), 'Delete', 'Install...', 'Import...', 'Export', and 'Unlock'. Below the toolbar, there is a table with a single row. The first column contains the text 'Name ↑'. The second column contains the value 'abc'. The third column contains the text 'Acceptable Use'. The fourth column contains the text 'A Landlord Policy', which is highlighted with a blue bar at the bottom. The entire row is also highlighted with a blue bar.

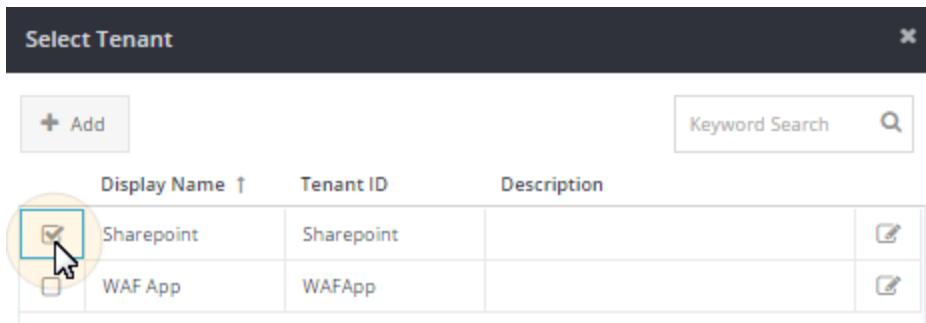
The selected file displays in the **Editor** tab.

3. **Click Add Rule.**



The system displays the Add Rule dialog.

- 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 426.

- Click **OK** to exit the Select Tenant dialog.
- In the **Determination Rules** field, use the natural language fields to create the tenant's determination rules:
 - Select **All** or **Any** of the following rules.
 - 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:

Determination Rule
The selected tenant's policy will apply when the following condition is met

Any	of the following rules:				
Port	=	80	-	+	Folder
Client Address	matches	198.51.100.0/24	-	+	Folder
Client Address	matches	203.0.113.25	-	+	Folder

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

Determination Rule

The selected tenant's policy will apply when the following condition is met

All of the following rules:

URL Domain	contains	.com	-	+	o
URL Domain	contains	casino	-	+	o
URL Domain	contains	finance	-	+	o

Any of the following rules:

Port	=	80	-	+	o
Port	=	443	-	+	o

Configure WAF Security Rules

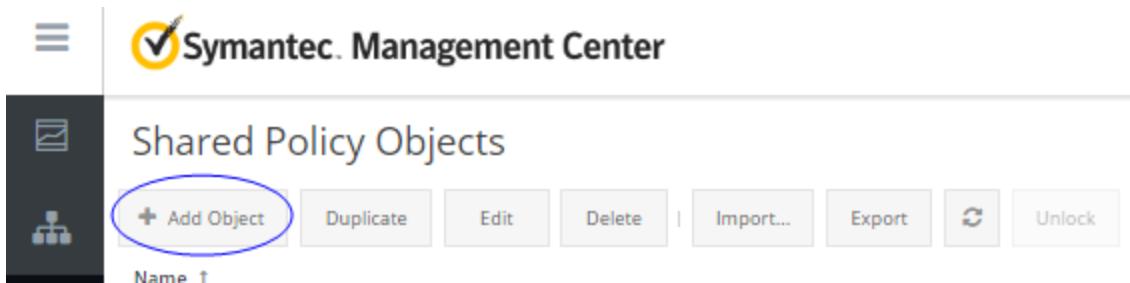
A *WAF security profile* is a shared object (a policy element that can be referenced by multiple policy objects) that defines the Web Application Firewall settings for the associated WAF application object. You associate the WAF security profile with a WAF application object to define the security rules 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 199.

Step 1 — Create a WAF Security Profile

1. Select Configuration > Shared Objects > Add Object.



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

Basic Information

Object name: * WAF Security Policy

Object type: * WAF Security Profile

Reference ID: WAF_Security_Policy

Description:

1024 of 1024 characters left

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.

Note: 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

Add Object Duplicate Delete Import... Export Unlock

Name ↑

blacklisted_categories

category_whitelist

DLP - Outbound

High Secure

The selected file displays in the Editor tab.

Shared Objects > Basic-Security

WAF Security Profile: Basic-Security

Editor Versions Attributes Info

Save Discard Compare Import

Request Validation

Request Normalization

Blacklist

Analytics Filter

Security Engines

XML Validation

Request Security

Response Security

Optimizations

Logging

Cross-Site Request Forgery

Exemptions

Path Normalization

Header Normalization

Parameter Normalization

Cookie Normalization

Multiple Encoding: Monitor

The action taken when unanticipated levels of nested encoding are detected

Invalid Encoding: Monitor

The action taken when an invalid encoding sequence is detected

3. Review the following settings and adjust to create the desired security settings:

Request Validation	Controls general HTTP request properties such as size restrictions, WAF validation properties, allowed methods, and allowed file types.
---------------------------	---

The default settings are adequate for most environments. To ensure Management Center is efficiently managing traffic, consider the following:

- In the **Protocol Compliance** settings, the action is triggered when the size of one or more parts of the request exceeds the specified limit. If the action is set to Ignore, the query string, headers, and body are scanned up to the specified count or size, and any excess is ignored. For example, if you set the Body: Max size to 10 KB, set the action to Ignore, and the appliance receives a request with a body size of 15 KB, then the first 10 KB of the request are scanned. The remaining 5 KB are not scanned, blocked, or monitored.

Note: If you have enabled this setting and specified the `http.request.data=` condition in policy, WAF engines use the greater of the two values for scanning. For more information, see the `http.request.body.inspection_size()` property in the [Content Policy Language Reference](#).

- In the **WAF Properties** settings:
 - The **Null Byte Detection**, if enabled, might cause false positives. If this setting does cause multiple false positives, Symantec recommends disabling this setting.
 - The **Parameter Pollution Separator** setting should not be enabled unless a protected backend, such as ASP.NET/IIS, is concatenating like-named query arguments.
- In the **Restricted File Upload Types**, enable as many file types as possible without backend functionality being degraded. As a minimum, Symantec recommends restricting uploads of EXE and HTML files. To restrict

file types:

1. Select **Block uploads based on the apparent data type**
2. Select the file types to restrict
3. Click **Save**.

For further information, see the following CPL gestures in the [Content Policy Language Reference](#):

- `http.request.body.inspection_size()`
- `http.request.detection.other.invalid_json()`
- `http.request.body.data_type()`
- `http.request.detection.other.null_byte()`
- `http.request.detection.invalid_form_data()`
- `http.request.detection.other.multiple_header()`
- `http.request.detection.other.parameter_pollution()`
- `http.request.detection.other.parameter_pollution_separator()`

Request Normalization	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 <code>http.request.normalization.default()</code> in the <u>Content Policy Language Reference</u> .
------------------------------	---

Blacklist

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.

To ensure Management Center is efficiently managing traffic, consider the following:

- Configure the **Use effective date** setting to efficiently handle newly published rules. By configuring this setting in this way, pre-existing rules continue to block attacks, and new rules monitor traffic to verify that the new rules are not creating false positives. To configure this setting to allow existing rules to block traffic and new rules to monitor it:

1. Select **Use effective date**.
2. In the **Effective Date** field, select a date before the effective date of the new rules; for example, if new rules had an effective date of October 31, 2018, then you could select October 30, 2018.

Note: When selecting an effective date, consider which rules you want to have blocking traffic and which you want monitoring traffic. The further in the past you select for your effective date, the more rules that will have a Monitor verdict.

3. In the **Verdict before** field, select **Block**.
4. In the **Verdict after** field, select **Monitor**.
5. Click **Save**.

- Set actions for individual rules; for example, if a single rule returns excessive false positives, set the action for that rule to Ignore. To set an action for an individual rule:

Note: Actions that are set for individual rules are exemptions to the global effective date rule; therefore, the action set for the individual rule overrides the action of the global rule.

1. In the table of rules, locate the individual rule.
2. Click the plus symbol to expand the rule.
3. Select the radio button for the appropriate action.
4. Click **Save**.

For further information, see the `define application_protection_set` gesture in the [*Content Policy Language Reference*](#).

Analytics Filter

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.

To ensure Management Center is efficiently managing traffic, consider the following:

- Configure the **Use effective date** setting to efficiently handle newly published rules. By configuring this setting in this way, pre-existing rules continue to block attacks, and new rules monitor traffic to verify that the new rules are not creating false positives. To configure this setting to allow existing rules to block traffic and new rules to monitor it:
 1. Select **Use effective date**.
 2. In the **Effective Date** field, select a date before the effective date of the new rules; for example, if new rules had an effective date of October 31, 2018, then you could select October 30, 2018.

Note: When selecting an effective date, consider which rules you want to have blocking traffic and which you want monitoring traffic. The further in the past you select for your effective date, the more rules that will have a Monitor verdict.

3. In the **Verdict before** field, select **Block**.
4. In the **Verdict after** field, select **Monitor**.
5. Click **Save**.

- Set actions for individual rules; for example, if a single rule returns excessive false positives, set the action for that rule to Ignore. To set an action for an individual rule:

Note: Actions that are set for individual rules are exemptions to the global effective date rule; therefore, the action set for the individual rule overrides the action of the global rule.

1. In the table of rules, locate the individual rule.
2. Click the plus symbol to expand the rule.
3. Select the radio button for the appropriate action.
4. Click **Save**.

For further information, see the `define application_protection_set` gesture in the [Content Policy Language Reference](#).

Security Engines	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 .
-------------------------	--

To ensure Management Center is efficiently managing traffic, consider the following:

- Customize the security engines to inspect particular parts of an HTTP request. By default, the security engines inspect all parts. Disabling the settings for some parts might reduce false positives.
- For the **Command Injection** and **Code injection** settings, disable the settings for technologies that are not relevant to your installation. Disabling these settings can decrease false positives.

For further information, see the `define application_protection_set` gesture in the [Content Policy Language Reference](#).

XML Validation

These options ensure the XML is valid and check for potentially malicious constructs.

To ensure Management Center is efficiently managing traffic, consider the following:

- The **XML External Entity (XXE)** setting inspects requests for XML External Entity injection attacks, which may allow external malicious content to be processed by an XML parser.
- The **XInclude Reference** setting inspects requests for Xinclude elements that might reference malicious content.
- The **Invalid XML** setting inspects requests for XML documents that are not well formed.
- The **Expand CDATA Sections** setting enables parsing of CDATA sections. As CDATA sections are not expanded nor interpreted by the XML parser, these sections can be used to evade detection of malicious content. Enable parsing of CDATA sections to detect potentially malicious content.

For further information, see the following CPL gestures in the [Content Policy Language Reference](#):

- `http.request.detection.xml.xxe()`
- `http.request.detection.xml.xincluder()`
- `http.request.detection.xml.invalid()`
- `http.request.detection.xml.cdata()`

Request Security

These options ensure that requests are safe by checking for common attacks like HTML tag injection, buffer overflow, header injection, and request smuggling.

The **Buffer Overflows** settings protect your servers from buffer overflow attacks by setting a global length limit for various parts of the request. By default, the **Buffer Overflows** setting is disabled as it can trigger false positives in some environments.

The **Aggressive Header Injection Blocking** setting blocks header injection attacks, in addition to the protection your ProxySG appliance already provide by default; however, this setting might produce excessive false positives in some environments.

For the **Block Insecure SSL Ciphers** setting, if one or more of these ciphers have been enabled on the ProxySG appliance, then you can disable them here. For example, if one tenant has legacy applications that still require an insecure cipher and all other tenants should not use this cipher, then disable this cipher in all other tenants. To disable ciphers, select **Block Insecure SSL Ciphers** and select the ciphers you want to block.

Response Security

These options make server responses more secure by obfuscating the back-end technology and directing browsers to implement additional client-side security.

To ensure Management Center is efficiently managing traffic, consider the following:

- The **Force "secure" and "HttpOnly" Cookie Flags** setting modifies Set-Cookie response headers to include the Secure and HttpOnly flags. The secure flag prevents browsers from sending cookies using cleartext and the HttpOnly flag helps prevent Cross-Site Scripting (XSS) attacks.
- The **Rewrite the "Server" Response Header to "unknown"** and **Web Application Fingerprinting Protection** settings hide information about the backend from potential malicious parties.
- The **HTTP Public Key Pinning** setting instructs the browser to recognize certain public keys for a set period of time for the site. Generally, this setting is not recommended due to the complexity and risk enabling it poses. Support for this setting has been deprecated or removed in some popular browsers.
- For the **HTTP Strict Transport Security** setting, if your site fully supports HTTPS, enable this setting for enhanced security. When initially enabling this setting, validate that the setting is functioning properly by selecting a low value for the **Age**. When you've validated it, Symantec recommends that you select an **Age** of at least 10368000 seconds (120 days) and ideally 31536000 (one year).
- The **X-XSS-Protection** setting inserts an X-XSS-Protection header into the response. It instructs browsers to not render a page if the appliance detects certain types of XSS attacks in the response.
- The **X-Content-Type-Options** setting inserts an X-Content-Type-Options header into the response. It helps prevent attacks that leverage inconsistencies between the Content-Type response header and the actual content type of the body that the browser's MIME sniffing determines.
- The **Clickjacking: X-Frames-Options** setting inserts an X-Frames-Options header into the response. It helps prevent clickjacking attacks by ensuring that your site's content can only be embedded in a frame of the same origin of your site.
- The **Enable Response Error Code Cloaking** setting hides common

error codes. Error codes that the server returns can contain information that might be useful to malicious parties. Enable this feature, and select error codes you want to hide and that won't impair functionality by them being hidden.

Optimizations

Disable WAF controls for POST requests consisting of binary data; bypass WAF scanning for cache hits.

To ensure Management Center is efficiently managing traffic, consider the following:

- The **POST Body Processing Control** settings are not required to be enabled for most environments. If these settings are disabled and you receive false positives pertaining to the POST body, then you might need to enable these settings.
- For the **Cache Control** setting, Symantec recommends enabling the **Bypass WAF Scanning for Cache Hits** setting. In most environments, this setting significantly improves performance.

For further information, see the `http.request.detection.bypass_cache_hit()` gesture in the [Content Policy Language Reference](#).

Logging

These options control when 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.

Warning: Sensitive data, such as personally-identifiable information, might be logged unless masking is performed.

For information on log details and masking, see the following CPL gestures in the [Content Policy Language Reference](#):

- `http.request.log_details[header,body]()`
 - `http.request.log.mask_by_name[regex_pattern]()`
 - `http.request.log.mask_by_value[regex_pattern]()`
-

Cross-Site Request Forgery 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.

By default, the **Enable CSRF Protection** setting is not enabled. Enable this setting only for applications that do not have protection, such as anti-CSRF tokens, from CSRF attacks. If the application does not have CSRF protection and you enable this setting, limit the scope of this setting. This setting modifies HTTP transactions and might disrupt user traffic, if applied too broadly.

For further information, see the following CPL gestures in the [Content Policy Language Reference](#):

- `http.csrf.authentication_link()`
- `http.csrf.detection()`
- `http.csrf.token.insert()`

Exemptions Define exemptions to your WAF policy to handle false positives. To create exemptions, see "Manage WAF Security Policy" on page 237.

PCI DSS Compliance Displays the status of PCI DSS Compliance for the WAF security profile or WAF application. The possible compliance states are as follows:

- Compliant
All PCI DSS requirements are met.
- Partial Compliance
One or more PCI DSS requirements are met, but not all.
- Non-Compliant
No PCI DSS requirements are met.

See "Verify WAF Policy Compliance With PCI DSS Requirement 6.6" on page 241, for more information.

Note: Many of the options include a Block/Monitor/Ignor 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 237.

Configure WAF Application Objects

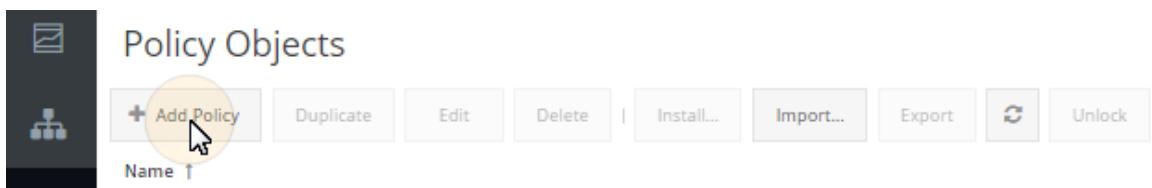
A *WAF application object* represents a web application (or group of applications) and its associated WAF security settings. The WAF application object is associated with a specific tenant and WAF Security Policy. You install this policy on ProxySG appliances to configure WAF settings.

WAF Policy Use

Configuring a WAF application object is step 6 in "Use WAF Policy To Protect Servers From Attacks" on page 199.

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.

Create New Policy: Basic Information

Basic Information

Policy name:	*	WAF_App_Policy
Policy type:	*	WAF Application
Reference ID:	WAF_App_Policy	
Tenant:	*	Default X EDIT
Description:	General WAF application using WAF_App_Policy and the default tenant slot to handle all traffic initially. 919 of 1024 characters left	

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.

Note: 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.

Note: 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.

Select Tenant				
		Add	Keyword Search	
	Display Name ↑	Tenant ID	Description	
<input checked="" type="checkbox"/>	Default	default	The tenant whose policy is used whe...	
<input type="checkbox"/>	Sharepoint	Sharepoint		

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.

1 Tenant Selection

The Tenant Determination File (Landlord) controls how requests are routed to specific tenants

Tenant:	Default	
---------	---------	---

Step 2 - Specify WAF Application

Settings

The WAF Application Settings panel enables you to set policy generation controls.

The screenshot shows the 'WAF Application Settings' panel. At the top, it says 'Policy generation controls for this WAF Application'. Below this, there are two main sections: 'WAF Security Profile:' and 'Profile Override:'. Under 'WAF Security Profile:', there are two radio buttons: 'Always use the latest version' (selected) and 'Use specific version:' followed by a dropdown menu set to '1.0'. Under 'Profile Override:', there is a checkbox 'Disable entire Security Profile' which is unchecked. Below these, there is a section for 'Block/Monitor Override:' with a checkbox 'Change all WAF controls to:' followed by a dropdown menu set to 'Monitor'. At the bottom, there is a note: 'Overrides all WAF actions in the associated Security Profile'. Under 'User Notification Page:', there are two radio buttons: 'Use default ProxySG exception page (invalid request)' (selected) and 'Use a specific page:' followed by a dropdown menu labeled 'Select or enter page name'. A note below says: 'Custom exceptions pages need to be prefixed with "user_defined"(ie "user_defined.my_exception")'.

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.**

The screenshot shows the 'Select Policy' dialog. At the top, it has a title bar with 'Select Policy' and a close button. Below the title bar, there is a search bar with 'Keyword Search' and a magnifying glass icon. On the left, there is a button with '+ Add'. The main area is a table with columns 'Name ↑' and 'Description'. There are two rows:

Name ↑	Description
<input checked="" type="checkbox"/> High Secure	<input type="button" value="Edit"/>
<input type="checkbox"/> WAF_Security_Pro...	<input type="button" value="Edit"/>

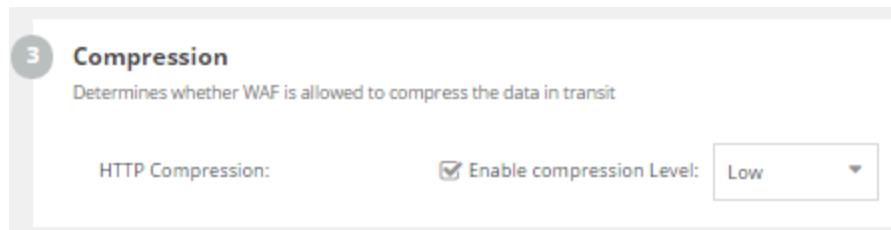
- c. Click **OK** to close the Select Policy dialog.
 - d. Specify the WAF Security Profile version to use. Select **Always Use the Latest Version** or specify a specific version in the **Use Specific Version:** field.
2. (Optional) To override all WAF Security Profile settings, select **Disable entire Security Profile**.
3. (Optional) To globally change all Block/Monitor verdicts, select **Change all WAF controls to: Monitor** or **Block**.

Note: 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.

4 Allow Rules

In a Default Deny configuration, "Allow Rules" control what traffic can pass through the ProxySG

Allow traffic based on:

Tenant Determination Allow all traffic processed by the configured tenant:
 CPL Fragment [Default](#) [Show Rules](#)

Warning! An "allow" rule must be specified when using the default tenant.
Please select an appropriate CPL fragment or create a custom rule. [More Info](#)

Note: 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.

5 CPL Fragments

Add Content Policy Language (CPL) fragments that are deployed with this WAF Application

+ Add CPL Fragment	Edit	Delete	Move Up	Move Down	
Order	CPL Fragment Name	Version			

1. Click **Add CPL Fragment**. The web console displays the **Add CPL Fragment** dialog.

Add CPL Fragment

CPL Fragment Name: *

Always use the latest version

Use specific version: [text input field]

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

	Name ↑	Description	
<input type="checkbox"/>	DLP - Outbound		
<input type="checkbox"/>	Forwarding Policy		
<input type="checkbox"/>	Test23		
<input checked="" type="checkbox"/>	WAF Policy1		

- b. Select the CPL Fragment. See [Create a CPL Fragment](#) 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 199.

Analyze and Refine WAF Policy Workflow

Step	Overview	References
1	<p>Check access logs to determine which rules or engines you must update to address false positives, false negatives, and other wanted behavior.</p> <p>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.</p>	<p>"View a Reporter Report" on page 674</p> <p>"Reference: Report Descriptions" on page 691</p> <p>"Search for Specific Report Data (Search and Forensic Report)" on page 702</p>
2	Optional-Perform a policy trace.	<p>"Launch a Device Console" on page 81</p> <p>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.</p>

Step	Overview	References
3	Based on your analysis of the access logs, create policy exemptions to eliminate false positives and other unwanted behavior.	"Manage WAF Security Policy" below
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:	Repeat the previous steps as needed.
	<ul style="list-style-type: none"> <li data-bbox="339 625 980 819">■ 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. <li data-bbox="339 851 980 963">■ Continue to test and refine policy, move to production, and then update policy actions to block. <li data-bbox="339 994 980 1115">■ Continue to test and refine policy, move to production, and gradually update each engine or policy's actions to block. 	Configure Monitor/Block actions: "Manage WAF Security Policy" below

Manage WAF Security Policy

As described in "Analyze and Refine WAF Policy (Mitigate False Positives)" on the previous page, 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 199.

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.**

The screenshot shows a list of shared policy objects. At the top, there are buttons for 'Add Object', 'Duplicate', 'Edit' (which is highlighted with a yellow circle and a mouse cursor), 'Delete', 'Import...', 'Export', and 'Unlock'. Below these are four rows of policy objects: 'blacklisted_categories', 'category_whitelist', 'DLP - Outbound', and 'High Secure'. The 'High Secure' row is highlighted with a blue background.

3. **Click Exemptions > Add Exemption.**

The screenshot shows the 'WAF_Security_Profile' editor interface. On the left, a sidebar lists various policy components: Request Validation, Request Normalization, Blacklist, Analytics Filter, Security Engines, XML Validation, Request Security, Response Security, and Exemptions (which is highlighted with a blue border). On the right, under the 'Exemptions' section, there is a button labeled '+ Add Exemption' with a yellow circle and a mouse cursor over it. Below this button is a list item 'URL'.

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.

Note: 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 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**.

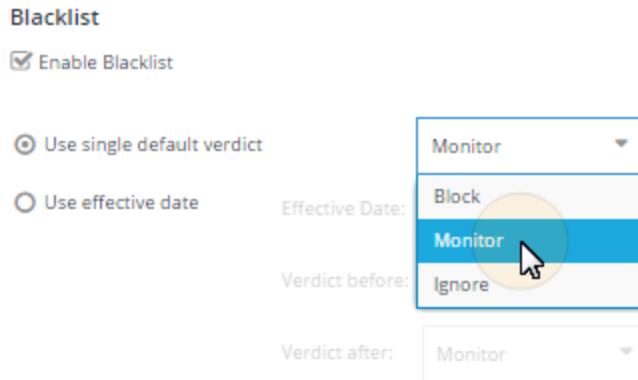
Options that support the Block/Monitor/Ignore action include an action drop-down menu. To set, select the appropriate action and click **Save**.

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.

<input type="checkbox"/> Rule Id	Description	Activation Date	Attack Category	Vulnerability...	Ignore	Monit...	Block	Default
<input checked="" type="checkbox"/> 2000 - Global: "/..": (7 rules)								
<input type="checkbox"/> 2000-0	Global: "/..":	2015-07-10	Directory Traversal		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> 2000-1	Global: "/..":	2015-07-10	Directory Traversal		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> 2000-2	Global: "/..":	2015-07-10	Directory Traversal		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Use Effective Date to Manage New Rule Updates

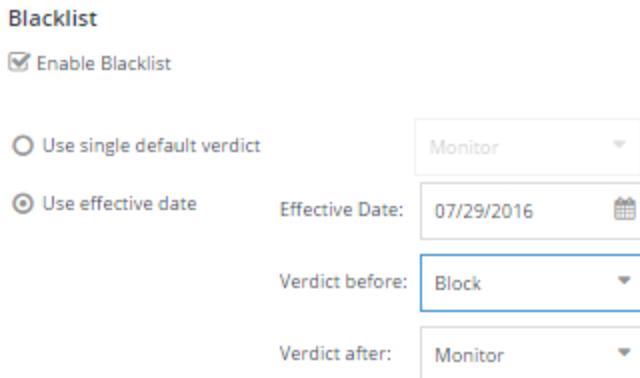
When Application Protection Subscription (APS) updates are published, the updated Blacklist and Analytics engine content is immediately available. Because the updated engine rules can potentially change the behavior of the existing WAF security policy, Management Center enables you to use this activation 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.



Verify WAF Policy Compliance With PCI DSS Requirement 6.6

Note: This is an optional step in configuring your Web Application Firewall.

The Payment Card Industry Data Security Standard (PCI DSS) specifies a set of data security requirements for web sites, including one (Requirement 6.6) that can be satisfied by enabling specific Web Application Firewall options to comply with the standard.

Management Center provides a visual indicator of the level of PCI DSS Compliance for WAF Applications and WAF security profiles and allows you to modify the current settings, if needed.

- Compliant

All PCI DSS requirements are met.

- Partial Compliance

One or more PCI DSS requirements are met, but not all.

- Non-Compliant

No PCI DSS requirements are met.

WAF Application

The example below shows the location of the PCI DSS compliance status indicator in the WAF application.

The screenshot shows the 'WAF Application Settings' page. At the top, it says 'Policy generation controls for this WAF Application'. Below that, there's a 'WAF Security Profile' dropdown set to 'WAF Test'. Underneath, there are two radio button options: 'Always use the latest version' (selected) and 'Use specific version: 1.0'. There are also 'Profile Override' and 'Block/Monitor Override' sections. A large yellow oval highlights the 'PCI DSS Compliance' section. This section shows a radio button for 'Partial Compliance' (selected), a link to 'View Security Profile > PCI DSS Compliance', and a note stating 'This WAF Application is in partial compliance with PCI DSS Standards.'

In this case, the WAF application is in partial compliance because its associated WAF security profile has one or more, but not all, options in compliance. To bring the WAF application into compliance, click the link to open the associated WAF security profile.

WAF Security Profile

Payment Card Industry Data Security Standard – Requirement 6.6 Compliance Report	
Status: ● Partial Compliance	
Protection Against	Compliance
<input type="checkbox"/> Command Injection	✗ Non-compliant
<input type="checkbox"/> Code Injection	✗ Non-compliant
<input type="checkbox"/> SQL Injection	✗ Non-compliant
<input type="checkbox"/> LDAP Injection	✗ Non-compliant
<input type="checkbox"/> XPath Injection	✗ Non-compliant
<input type="checkbox"/> XML External Entity (XXE) Injection	✗ Non-compliant
<input type="checkbox"/> Cross-Site Scripting	✗ Non-compliant
<input type="checkbox"/> Directory Traversal	✗ Non-compliant
<input type="checkbox"/> Buffer Overflows	✗ Non-compliant
<input type="checkbox"/> Cross-Site Request Forgery	✗ Non-compliant
<input type="checkbox"/> Upload File with Dangerous Type	✗ Non-compliant
<input type="checkbox"/> File Inclusion	✗ Non-compliant
<input type="checkbox"/> HTTP Response Splitting	✗ Non-compliant
<input type="checkbox"/> Information Leakage	✗ Non-compliant
<input type="checkbox"/> Vulnerability Scanners	✓ Compliant

As you can see in the preceding example, this WAF security profile is in partial compliance because one of its options, **Vulnerability Scanners**, is in compliance. To bring the WAF security profile into compliance, all non-compliant options must be modified.

To change a setting, click the + to the left of the option. The system displays the remediation required to achieve compliance and a link to the setting. In the following example, the remediation is "**Linux, Windows, or OSX command injection must be on block if enabled.**"

PCI DSS Compliance Report
Payment Card Industry Data Security Standard – Requirement 6.6 Compliance Report

Status: ! **Partial Compliance**

Refresh Last compliance check: 1/30/2019, 9:35:57 AM

Protection Against	Compliance
Command Injection <small>Linux, Windows or OSX command injection must be on block if enabled</small> Go to Command Injection	✖ Non-compliant
Code Injection	✖ Non-compliant

When you click the link, the system displays the command injection section in the WAF security profile so you can make the necessary change. After making a change, navigate back to the **PCI DSS Compliance Report** and click **Refresh** to update the status.

Non-Compliance

Normally, a WAF Application is non-compliant because the associated WAF security profile is not in compliance. However, even if the WAF security profile is fully compliant, a WAF application can be shown as non-compliant in the following cases:

- You have disabled the security profile by selecting the **Disable entire Security Profile** option.
- You have changed all WAF controls to Monitor using the **Block/Monitor Override** option.

Either of these actions cause the WAF application to be non-compliant.

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 devices. 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.

"Schedule the Execution of a Configuration Script " on page 281

- 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" on page 468

Create and Distribute Configurations Using Scripts

Create commonly used device configurations in a script. After you create the script, you choose to execute the script on a device immediately, or you can create a job. Scripts are collection of CLI commands that are executed in the order shown within the script itself. Scripts are NOT in any type of scripting language. Scripts can be executed on the following devices:

- Blue Coat ProxySG appliance
- Advanced Secure Gateway
- Content Analysis appliance
- SSL Visibility 4.x appliance
- Reporter 10.3 and later

Note: To successfully execute a script on a Content Analysis, Reporter 10.3, or SSLV 4.x appliance, you must specify the device's enable password in the device's connection settings (**Network > devicename > Edit > Connection Parameters**). See "Add a Device" on page 660 for more information.

Add a Script

1. Select **Configuration > Scripts**. Click **Add Script**. An asterisk denotes fields that are mandatory.
 - **Name***—The name displays in the **Script Object** list.
 - **Type***—Scripts can be imported from devices and then executed on supported, managed devices.
 - **Description**—Although entering a description is optional, the description helps

differentiate versions of the same script. For more information about the script, see "View Script Information" on page 262

2. Ensure **Replace substitution variables** is selected. See "Use Substitution Variables in Policies and Scripts" on page 312.
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. Optional tasks:
 - "Add a Script Operation (Includes, If Statements, and Error Handling)" on page 267
 - "Apply Logical Expressions to Scripts and Policy" on page 268
 - "Optimize a Script for Use on Other Devices" on page 264
6. Click **Save**.

Next Steps

After you create script object, you can refine it or leave it as an empty object while you perform other tasks (for example, edit script details) or you execute the script now. Refer to the following table to determine the next step to take.

What do you want to accomplish?	Go to
Create a job to execute a script on a schedule	"Schedule the Execution of a Configuration Script" on page 281
Execute the script now	"Execute Scripts" on page 251
Compare script versions	"Compare Versions of the Script" on the facing page
Import a script from a managed device	"Import Script from a Device" on page 259
Restore previous version of a script	"Restore a Version of Script" on page 261
Customize object filters	"Customize Object Filters" on page 249
View script information	"View Script Information" on page 262
Manage attributes	"Manage Attributes" on page 583
Filter by attributes and keyword search	"Filter by Attributes and Keyword Search" on page 256

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 256.
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.

Tip: See "Restore a Version of Script " on page 261.

Customize Object Filters

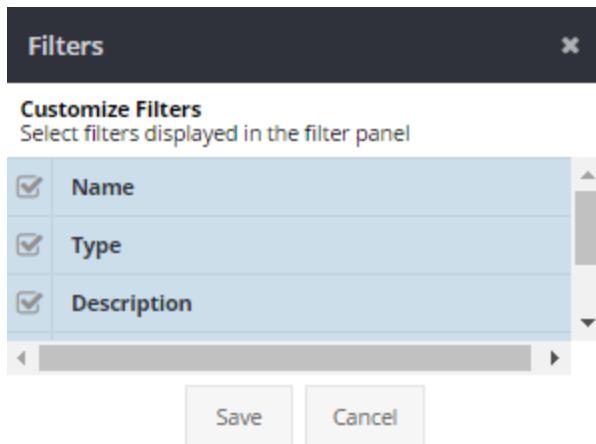
Filters control the specific objects that are searchable.

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.

Tip: To substitute variables in policies, policy fragments or scripts, see "Use Substitution Variables in Policies and Scripts" on page 312.

3. The **Filter** panel also includes mandatory attributes. See "Manage Attributes" on page 583.
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 "Create and Distribute Configurations Using Scripts" on page 246. 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:

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

Tip: See also "Schedule the Execution of a Configuration Script " on page 281.

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**.
5. OR
6. 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**.

Note: 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**.

From a Job Operation

See "Schedule the Execution of a Configuration Script " on page 281.

(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.

Add Error Handling for Scripts

You can specify the behavior Management Center should take when encountering errors or warnings while running a script. Any response line starting with a "%" is an error, and any response line starting with "Warning" is a warning. Management Center provides two levels of script error handling: one at the job level and another within the script itself.

- When multiple scripts are specified in a job, you can [specify the error handling](#) if a warning or error in a script is encountered.
- You can add comments within a script to specify the behavior when a warning or error is encountered.

The following table describes these error-handling comments.

Operation	Text Comment	Description
Stop on Error	stop-on-error	When this directive is encountered, Management Center runs the script line-by-line and will abort script execution if an error occurs. Inline commands are treated as one command to the EOF instruction.
Continue on Error	continue-on-error	When this directive is encountered, Management Center ignores all subsequent errors until another directive is reached (if there is one).
Stop on Warning	stop-on-warning	When this directive is encountered, Management Center runs line-by-line and reports a failure if warnings are encountered.

Operation	Text Comment	Description
Continue on Warning	continue-on-warning	When this directive is encountered, Management Center ignores all subsequent warnings.
Execute as Batch	begin-batch end-batch	Instructs Management Center to submit everything between these comments as a single "command." You must have a begin-batch and an end-batch. An end-batch without a begin-batch results in an error before script execution.
Refresh Session	refresh-session	<p>Instructs Management Center to return the device CLI to its default starting position. This is useful for situations in which the script operation encounters an error, such as a missing policy object, that would cause a script error when the next command is run.</p> <p>Using Refresh Session, you can reset the CLI to its starting position and execute a new set of commands.</p> <p>For ProxySG and ASG, the starting position is #(config), while SSL Visibility and Content Analysis use the enable mode.</p> <p>Any directives encountered before Refresh Session are enforced. For example, if Continue on Error is encountered before Refresh Session, it will still be enforced after Refresh Session is executed.</p>

Insert Script Error Handling

You can add script error handling in the following ways:

- Using the [Operations](#) menu.
- Inserting them manually in the script.

Manually insert the directives using standard comment format. For example:

```
! - MC stop-on-error
Script section
! - MC stop-on-warning
```

You can insert multiple error-handling directives in your script. For example:

```
ssl
!- MC: continue-on-error
!- Creating will fail if it already exists, but we're OK with it already existing
create keyring show-director newkeyring
delete keylist newkeylist
```

```
create keylist newkeylist
delete certificate newkeyring

ssl
edit keylist "notfound"
clear
exit

!- MC: refresh-session
ssl
edit keylist "found"
clear
exit

!- MC: stop-on-error

!- MC: begin-batch
create certificate newkeyring
US
CA
Los Angeles
Company Inc
Development
example.com
admin@example.com
Company Inc
sha256
!- MC: end-batch

edit keylist newkeylist
add newkeyring
exit
exit
```

In the preceding example, the administrator has inserted a "Continue on Error" directive before creating a keyring. This is because it is OK if the keyring already exists. The admin has inserted "Refresh Session" to make sure the device goes back to its starting place to ensure the following script commands execute successfully. The admin has then inserted a "Stop on Error" directive so script execution will fail if an error occurs after this point. The final directive is to execute commands as a batch (a single command).

Job and Script-Level Error Handling Interaction

The error handling inserted into scripts works in conjunction with the error handling specified for the entire script in the job settings. For example, if a script contains a directive for

Management Center Configuration & Management

"Continue on Error", Management Center ignores all errors encountered after that directive and the script continues to run—even if the job setting specifies "Stop on Error." The same is true for warnings.

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.

Tip: You are not limited to the displayed **Filter** fields. See "Customize Object Filters" on page 249.

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

Caution: Additional fields are created when you create a new attribute. See "Manage Attributes" on page 583.

- **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**. ~or~
 - 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).

Tip: 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.

Caution: You cannot search on special characters, such as ^%|~.

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.

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

/IPv6 "0:0:0:0:0:1"

Tip: 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.

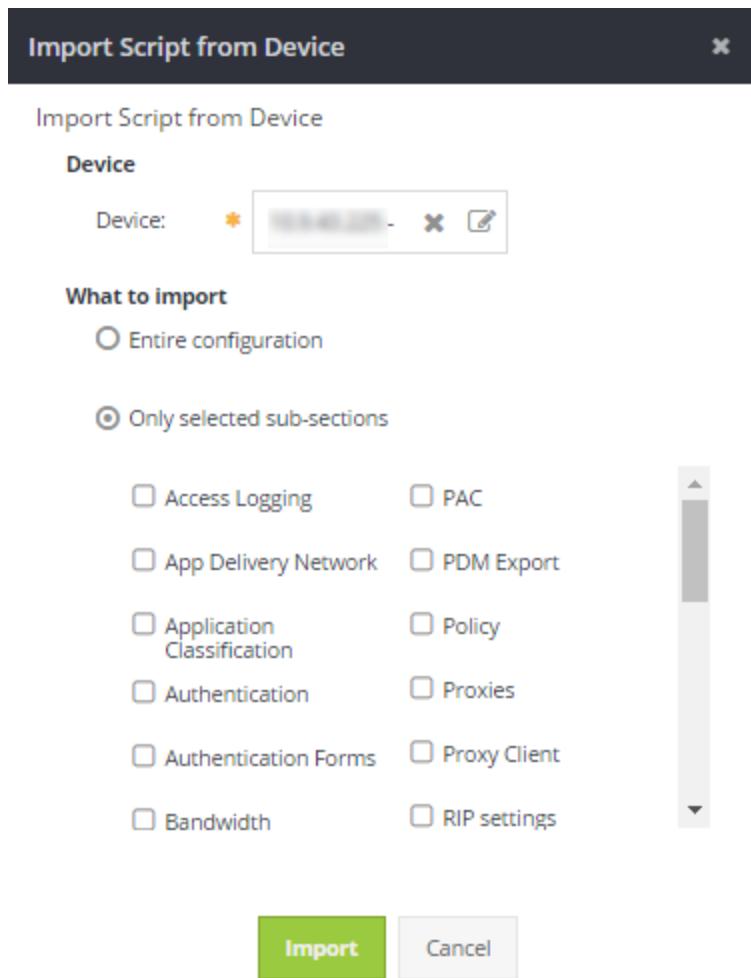
How do you clear the search results?

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 subsections.**



6. Click **Import**.

The comment you enter is saved as script metadata.

Determine Your Next Step

What do you want to accomplish?	Refer to this topic
View existing script information.	"View Script Information" on page 262
Restore a version of the script.	"Restore a Version of Script " on the next page
Execute the script, as is, to devices.	"Execute Scripts" on page 251

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 256.
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**.

Note: 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.

Tip: 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 583.

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. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

Optimize a Script for Use on Other Devices

To help ensure that a script runs without errors when used on multiple devices, you can add local variables or optimize the script. You can add local variables to any device scripts but the optimization tools are only supported for use with ProxySG or Advanced Secure Gateway (ASG) devices. Access the optimization tools by selecting **Configuration > Scripts > ScriptName > Tools**.

Add Local Variables to a Script

Management Center allows you to insert local variables into your script. You can use these local variables to create script templates, for example.

Define the Local Variable

To create a local variable, define the variable:

- Set a local variable to some value:

```
 ${@set-local LocalVariableName = value}
```

- Set a local variable based on the value of another variable. Note that the nested variable is not nested in {}:

```
 ${@set-local LocalVariableName = $variable}
```

For example:

```
 ${@set-local deviceLocation = $rack}
```

Reference the Variable

After defining the local variable, you can reference it in the following ways:

```
 ${@get-local LocalVariableName}
```

or

```
 ${locals.LocalVariableName}
```

Clean Up and Remove Problematic Script Entries

Note: Currently, these tools can only be used with ProxySG and Advanced Secure Gateway (ASG) appliances.

Management Center provides the following script optimization tools:

- **Make scripts portable**

Troubleshoot and optimize the script so that it runs without errors. This process has the following options:

- **Replace appliance-name with parameters**

Replaces appliance-name XXXX with appliance-name \${locals.applianceName} and adds a \${@set-local applianceName} to the top of the script.

- **Replace username and passwords in Active Directory (AD) authentication**

This process finds any security windows-domains and replaces the hard-coded username and password with variables. It also adds a conditional \${if locals.adUseExistingAccount} to surround the inline domain-details and an \${else} join \${end} so you can decide whether to use the existing account or a different account (based on the local variable adUseExistingAccount).

It also replaces <password> with \${locals.kerberosPassword} if there is a defined Kerberos-user.

- **Remove any inline policy**

This process removes all inline policy; policy should be contained in policy objects, not as inline policy.

- **Remove "create" operations for default settings**

This process removes any lines starting with the following attributes:

- "adn-compress disable"
- "attribute adn-byte-cache disable"
- "attribute use-adn disable"
- "enforce-signed disable"
- "create format \"dns\""
- "create format \"clientagent_v1\""
- "create log \"dns\""
- "create log \"client-agent\""

It also removes:

- All commands from create https-console "HTTPS-Console" to the exit.
- The default interface 0:0 and ip-default-gateways statements.

- **Remove inline policy**

This process removes all inline policy; policy should be contained in policy objects, not as inline policy.

- **Correct PEM encoded certificates**

This process corrects any PEM certificates that have incorrect formatting due to line breaks or other issues.

When you run one or more of these processes, the system does not automatically save the changes. This allows you to compare the new script version with the original version to ensure the changes are acceptable. Select **Compare** to view the changes. For more information, see "Compare Versions of the Script" on page 248.

Add a Script Operation (Includes, If Statements, and Error Handling)

You can add the following script insertions:

- **Insert Include**
- **Insert If**
- **Insert Error Handling**

Add a Script Operation

1. Select **Configuration > Scripts**, highlight the row the script is on and click **Edit**.
2. Place your cursor where you want to insert the operation.
3. Click **Operations** and select the desired operation.
4. Modify the inserted operation as needed. See sections below for more information.
5. Click **Save**.

Insert Include

This feature allows you to:

- Include one script inside another. For example:

```
 ${include:IncludeKeys}
```

- Specify a specific version of the included script. For example:

```
 ${include:IncludeKeys[1.2]}
```

The script type is considered when including scripts. ProxySG scripts can run only on ProxySG appliances, but ASG scripts can be run on both appliances. Therefore, you cannot include an ASG script in an SG script, though the converse is allowed.

Note: Cyclical script references are not allowed. If detected, the system generates errors.

Insert If

See "Apply Logical Expressions to Scripts and Policy" below.

Insert Error Handling

See "Add Error Handling for Scripts" on page 252.

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 apply unique \${if ...} and \${else logic to loop script processing to test for a specific value.

Add an If Expression to an Existing Script

1. Select the script and click **Edit**.
2. Click **Operations** and select **Insert If**.
3. Modify the inserted \${if condition} as needed.
4. Click **Save**.

Supported Expressions

`${if variable}`

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

Tip: 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.

Caution: 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 312.

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  
   add server 203.0.113.5  
 ${end}  
  
 ${if group='Data Center 3'}  
   dns-forwarding  
   edit primary  
   add server 203.0.113.6  
 ${end}  
  
 ${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.

Note: 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" on page 246).
2. Include substitution variables in the CPL or script. See "Supported Variables" on the next 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 275 below for details.

Examples

Substitute the device's serial number.

`${device.serialNumber}`

Substitute the value of the device's Rack attribute.

`${device.attributes.Rack}`

Caution: 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.

Variable	Description
`\${device.memberOf}`	List of the groups to which a device is assigned
`\${device.uuid}`	Internal ID of device
`\${device.modelNumber}`	Device model number
`\${device.description}`	Text in the Description field in device properties in Management Center
`\${device.name}`	Text in the Device Name field in device properties in Management Center
`\${device.serialNumber}`	Device's serial number
`\${device.osVersion}`	Operating system version running on the device
`\${device.type}`	The device type, for example, ProxySG.
`\${device.attributes.name}` where <i>name</i> is the attribute name	System or user-defined device attribute value, including any values inherited from the device group

Device Connection - \${device.connection.field}

The following variables are available for policies and scripts. A variable might not be applicable to every device.

Variable	Description
`\${device.connection.host}`	Host IP address

<code> \${device.connection.port}</code>	Port number
<code> \${device.connection.connectionType}</code>	Designates the way the connection is established and optionally how authentication is performed. For example, SSH_PUBLIC_KEY
<code> \${device.connection.network}</code>	PRODUCTION or PREPRODUCTION
<code> \${device.connection.username}</code>	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).

Variable	Description
<code> \${policy.author}</code>	Last user who edited and saved the policy
<code> \${policy.description}</code>	Text in the Description field in policy properties
<code> \${policy.name}</code>	Text in the Name field in policy properties
<code> \${policy.referenceId}</code>	Text in the Reference Id field in policy properties
<code> \${policy.revision}</code>	Policy's current Version number
<code> \${policy.revisionDescription}</code>	Comments entered for the last revision
<code> \${policy.attributes.name}</code>	User-defined policy attribute value

where `name` is the attribute name

Policy Fragment- `${fragment.field}`

The following variables are available for policy fragments.

Variable	Description
<code> \${fragment.author}</code>	Last user who edited and saved the policy fragment
<code> \${fragment.description}</code>	Text in the Description field in policy fragment properties
<code> \${fragment.name}</code>	Text in the Name field in policy fragment properties
<code> \${fragment.referenceId}</code>	Text in the Reference Id field in policy fragment properties

<code> \${fragment.revision} </code>	Policy fragment's current Version number
<code> \${fragment.revisionDescription} </code>	Comments entered for the last revision
<code> \${fragment.attributes.name} </code>	User-defined policy fragment attribute value
where <code>name</code> is the attribute name	

Script - `${script.field}`

The following variables are available for scripts only (not policies).

Variable	Description
<code> \${script.author} </code>	Last user who edited and saved the script
<code> \${script.description} </code>	Text in the Description field in script properties
<code> \${script.versionDate} </code>	Date of last update
<code> \${script.name} </code>	Text in the Name field in script properties
<code> \${script.type} </code>	Selected Type in script properties
<code> \${script.revision} </code>	Script's current Version number
<code> \${script.revisionDescription} </code>	Comments entered for the last revision
<code> \${script.attributes.name} </code>	User-defined script attribute value
where <code>name</code> 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.
```

Preview a Script With Variables Replaced

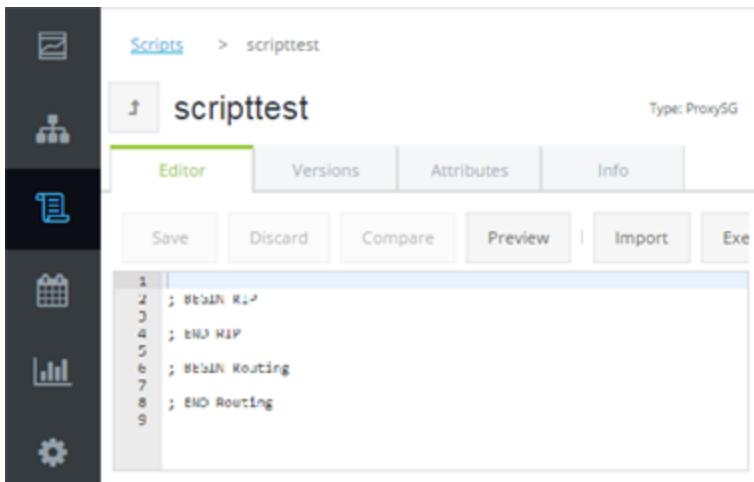
Management Center enables you to check the variable replacement in a script before you execute it. Previewing a script avoids inadvertently changing a device configuration.

Note: Devices that are in your network deployment should not be used to test configurations.

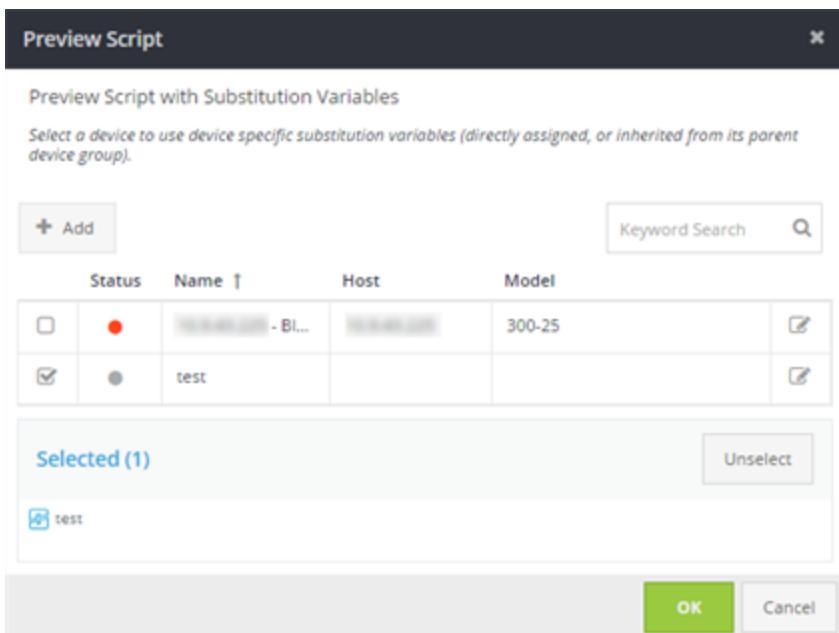
For scripts that use commands not in configure mode, you must exit configure mode before executing the script. Most commands are executed in configure mode. Licensing commands are the exception, and cannot execute in configure mode.

Management Center Configuration & Management

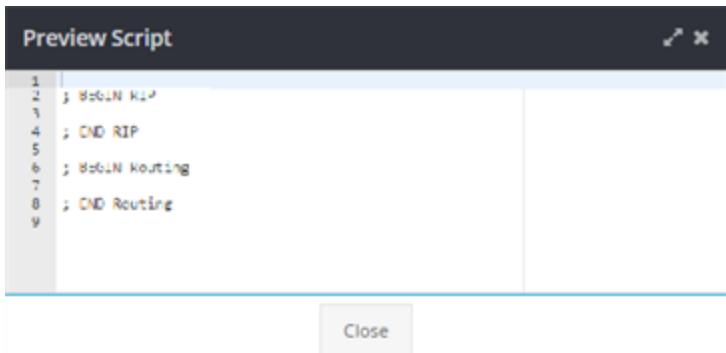
1. Select **Configuration > Scripts**.
2. **Open a script object.**



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**.

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.

Management Center Configuration & Management

Add Attribute

Display Name:	<input type="text" value="Purpose"/>
Name:	<input type="text" value="Purpose"/>
Type:	<input type="text" value="String"/> <input type="button" value="▼"/>
Format:	<input type="text" value="Text"/> <input type="button" value="▼"/>
Min Length:	<input type="text" value="0"/> <input type="button" value="▲"/> <input type="button" value="▼"/>
Max Length:	<input type="text" value="50"/> <input type="button" value="▲"/> <input type="button" value="▼"/>
Default Value:	<input type="text"/>
<input type="checkbox"/> Mandatory	
<input checked="" type="checkbox"/> Displayed as a default column	
Description:	<input type="text"/> 1024 of 1024 characters left
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

The new attribute's name is **Purpose** because we want to logically arrange the scripts by their purpose.

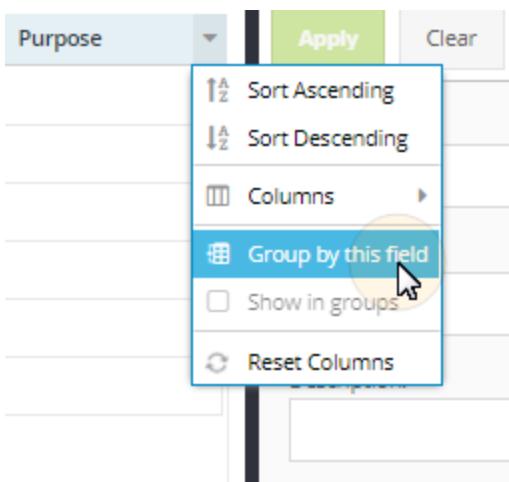
Note: Ensure that **Displayed as a default column** is checked so this attribute will automatically display on the script list grid.

3. Click **Save**.
4. Select **Configuration > Scripts**. You will see the **Purpose** header on the grid.

Name	Type	Description	Ver..	Author	Purpose
script001	ProxySG		1.11	admin	
script002	ProxySG		1.0	admin	
script003	ProxySG		1.2	Admin23	
Test Script 001	ProxySG	Test description	1.0	Ron Grimes	
Test Script 002	Advanced Secure..	Test description	1.0	Ron Grimes	
Test Script 003	ProxySG	Test description	1.0	Ron Grimes	

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.

scriptjob

- Editor
- Versions
- Attributes**
- Info

Attributes					
Date:	12/15/2016				
Purpose:	Test				

- 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.

<input checked="" type="checkbox"/> Purpose: Iteration 1	Local_DB	ProxySG		1.4	admin	Iteration 1
<input checked="" type="checkbox"/> Purpose: Iteration 2	scripttest	ProxySG		1.3	Admin23	Iteration 2
<input checked="" type="checkbox"/> Purpose: Test	scriptjob	ProxySG		1.12	admin	Test
	scriptjob2	ProxySG		1.1	admin	Test

You can also setup the attribute to be a picklist if you want to have predefined values.

Schedule the Execution of a Configuration Script

A script is a set of configuration commands, stored in a single text file. When you want to execute the same script on multiple devices, you can create the script once in Management Center and then execute it on all devices on which you want to put that configuration. To accomplish this goal, you create and test the script on a single device, and then create a job to execute the script on selected targets.

Before You Begin

- (Optional) Create a device group for the devices the configuration script will be executed on. See "Add a Device Group" on page 166.
- Create a script object. See "Create and Distribute Configurations Using Scripts" on

page 246.

3. (Optional) Import all or part of a configuration from one of your devices. See "Import Script from a Device" on page 259.
4. Test the script by executing it on one device. See "Create and Distribute Configurations Using Scripts" on page 246.

Schedule Script Execution

When you have completed the tasks in "Before You Begin" on the previous page, you are ready to create a job to execute the script on multiple devices.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Execute Script**.
3. **Configuration:**
 - Click **Add** to select one or more scripts to execute.
 - **Runs on** displays the compatible devices the script can run on.

Note: ProxySG scripts can run on Advanced Secure Gateway (ASG) appliances, but ASG scripts will not run on ProxySG appliances. Therefore, if you include one ASG script and one ProxySG script, the system displays only ASG targets.
4. **Targets:**
 - If you select **Continue on Fail**, the job will continue to run even if that script execution fails.
 - **Continue on Warning** is selected by default.

Management Center Configuration & Management

- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

5. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. **Name:**

- Verify or change the name and add an optional description.

8. Click **Save**

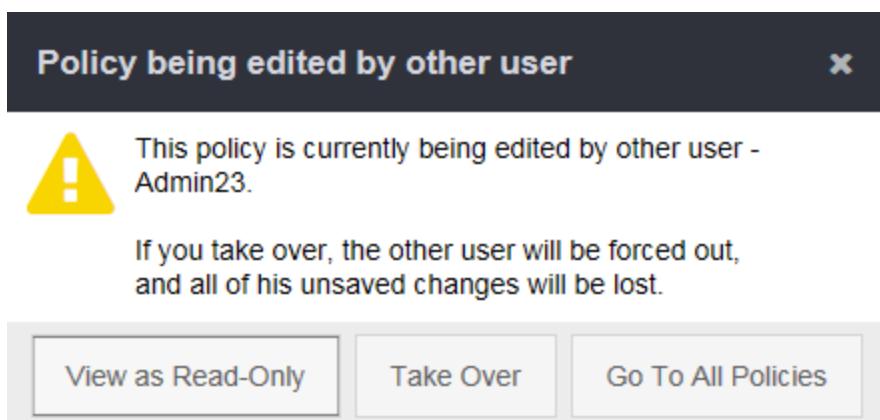
After Management Center runs the script execution job, confirm that the script was executed on the target devices.

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.

Note: 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 344.

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 292.
- Create policy without assigning it to devices immediately. See "Create a CPL Policy Object" on page 295
- Find and edit sections of the policy. See "Find a Policy Section" on page 309 and "Edit a Policy Section" on page 299
- Modify and test policy and group related rules together. See "Refine Existing CPL Policy" on page 302.
- Correct and modify the behavior of existing policy by re-ordering policy sections. See "Change the Order in which Policy Rules are Evaluated" on page 311
- Create versions of policy, and restore previous versions when needed. See "Restore a Version of Policy" on page 493
- [View](#) or [compare](#) policy versions.
- Enable substitution variables to be used, for any variable, so that you don't have to modify each attribute in each policy if a configuration has changed. See "Use Substitution Variables in Policies and Scripts" on page 312
- Create policy attributes and apply them to policy objects. See "Add Attributes" on page 584.
- 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 455.

- Import existing policy from a managed device. See "Import Policy or Shared Objects" on page 457
- Check the [consistency](#) of installed policy.
- View the [deployed policy](#) on a device.
- View existing policy information. See "View Existing Policy Information" on page 472.
- Deploy [universal CPL policy](#).

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 [legacy](#) or [web-based](#) VPM. See "Add a VPM Policy Object" on page 323.
- Select a reference device to edit VPM policy. See "Select Reference Device for VPM Policy" on page 325.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy" on page 493.
- [View](#) the CPL or XML source.
- [View](#) or [compare](#) policy versions.
- Create or "Edit Attributes" on page 587 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 455.
- Import existing policy from a managed device. See "Import Policy or Shared Objects" on page 457.
- Check the [consistency](#) of installed policy.
- View the [deployed policy](#) on a device.

- View existing policy information. See "View Existing Policy Information" on page 472.
- [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.

For more information about how UPE integrates with WSS, refer to the [Universal Policy Enforcement WebGuide](#).

- [Deploy](#) universal policy.
- [Create](#) a universal policy object.
- Import existing policy from a managed device. See "Import Policy or Shared Objects" on page 457.
- [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 325.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy" on page 493.
- [View](#) the CPL or XML source.
- [View](#) or [compare](#) policy versions.
- Create or "Edit Attributes" on page 587 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 455.
- Check the [consistency](#) of installed policy.
- View the [deployed policy](#) on a device.
- View existing policy information. See "View Existing Policy Information" on page 472.

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 210 and "Use WAF Policy To Protect Servers From Attacks" on page 199.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy " on page 493.
- Create policy attributes and apply them to policy objects. See "Add Attributes" on page 584
- 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 455.
- Check the [consistency](#) of installed policy.
- View the [deployed policy](#) on a device.
- View existing policy information. See "View Existing Policy Information" on page 472.

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 215 and "Use WAF Policy To Protect Servers From Attacks" on page 199.
- Create versions of policy, backup and restore previous versions when needed. See "Restore a Version of Policy" on page 493.
- Create policy attributes and apply them to policy objects. See "Add Attributes" on page 584.
- Deploy multiple policies to a group of devices by using Management Center's job feature. See "Install Multiple Policies" on page 455.
- View existing policy information. See "View Existing Policy Information" on page 472.

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 408.

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 IP Address List" on page 417.

Create Local Content Filter Databases

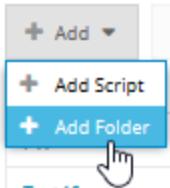
You can create a local content filter database in Management Center that all of your ProxySG or Advanced Secure Gateway appliances can use in policy. This database is hosted on Management Center. See "Create a Local Content Filter Database" on page 388 for details.

Organize Policy in Folders

To make it easier to find your policy, you can logically organize your policy objects, scripts, shared objects, and files using folders. This feature is supported on all pages in the **Configuration** section, except for **Tenants**.

1. Go to the policy page you'd like to add a folder to.
2. Click **Add > Add Folder**.

Note: This system does not display the **Add Folder** option unless the **Folders** option is enabled.



3. Provide a name and optional description and click **Save**.

The system displays the folder in the left pane. If you don't see the folder list, toggle the **Folders** option.

Policy Objects



4. Drag and drop the job(s) you'd like to move to the folder.
5. Optional—if you want to make the folder a sub-folder of another folder, drag and drop it to the top-level folder.

Use Content Policy Language (CPL) to Create Policy

Caution: 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 594.
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.

Tip: 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 299.

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 488 and "Compare the Device Policy Version with Current Policy Version" on page 491.
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 472.

Working with CPL Policy Fragments

A fragment is 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 into 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 344 and "Include a Shared Policy Object in CPL or VPM Policy" on page 355.

Caution: If you do NOT enable variable substitution in the CPL, variable substitution is not enabled for CPL Fragments as well.

Determine Your Next Step

What do you want to accomplish?	Refer to this topic
Enable variable substitution for CPL Policy and CPL Policy Fragments.	"Use Substitution Variables in Policies and Scripts" on page 312
Add new attributes that can be made available to the CPL Policy.	"Add Attributes" on page 584
Add or edit sections of a CPL Policy.	"Add or Edit CPL Policy Sections" on page 298
Import a policy from a device to Management Center.	"Import Policy or Shared Objects" on page 457
Modify/test policy and group related rules together.	"Refine Existing CPL Policy" on page 302

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*.

Note: 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.

Note: 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 472.
8. To enable variable substitution, select the check box **Replace substitution variables**. See "Use Substitution Variables in Policies and Scripts" on page 312 Click **Next**.

Caution: 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 344.

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 480
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.

What do you want to accomplish?	Refer to
Refine an existing CPL policy.	"Refine Existing CPL Policy" on page 302
Enable variable substitution for CPL Policy and CPL Policy Fragments.	"Use Substitution Variables in Policies and Scripts" on page 312
Validate existing policy.	Preview Policy Before Installing It
Import an external CPL policy.	"Import External Policy " on page 465
Create a new CPL policy section.	"Add or Edit CPL Policy Sections" on page 298

Management Center Configuration & Management

What do you want to accomplish?	Refer to
Manage your CPL policies.	"Manage CPL Policies" on page 304

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.

Note: These features are only available if the Modular Layout is selected .

Add a Section Based on an Existing Policy Section

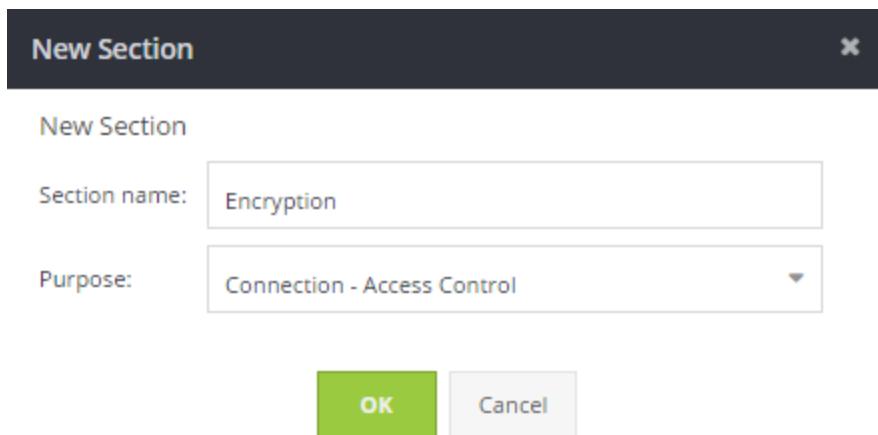
While composing the CPL or after importing policy from a device, you might find some policy rules that should be extracted from their respective sections and put into a new section. You can select some or all of the text in a section and convert the selection to a new section. When you convert a selection, 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.
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.

Note: 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 find 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.

Note: If you do not name the section, and only give it a purpose, the section appears as Untitled.

Management Center Configuration & Management

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

Caution: 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.

Note: 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 306 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 256.
Once you have found the policy object, you can determine the policy section to edit; see "Find a Policy Section" on page 309.
2. (Optional) Make sure that the policy you are editing is the one you want. See "View Existing Policy Information" on page 472.
3. (If applicable) Edit the CPL directly in the Policy Editor. See "Use Content Policy Language (CPL) to Create Policy" on page 292.
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 311.
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 483.
6. (If applicable) Add sections to contain policy for other purposes. See "Add or Edit CPL Policy Sections" on page 298.
7. (If applicable) Edit a section's name or purpose. See "Edit a Policy Section" on page 299.
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 292 in the Policy Editor.
 - "Import Policy or Shared Objects" on page 457.
 - "Add Attributes" on page 584
 - "Install Policy" on page 451 to devices or device groups.
 - "Install Multiple Policies" on page 455 to devices or device groups.
 - "Compare the Device Policy Version with Current Policy Version" on page 491.
2. To add custom metadata to policies, see "Add Attributes" on page 584.
3. "View Existing Policy Information" on page 472 to see the revisions and policy information.

Management Center Configuration & Management

4. "Compare Different Versions of the Same Policy" on page 488 to find the edited version of a policy that you want to use.

Work with CPL Policy Sections

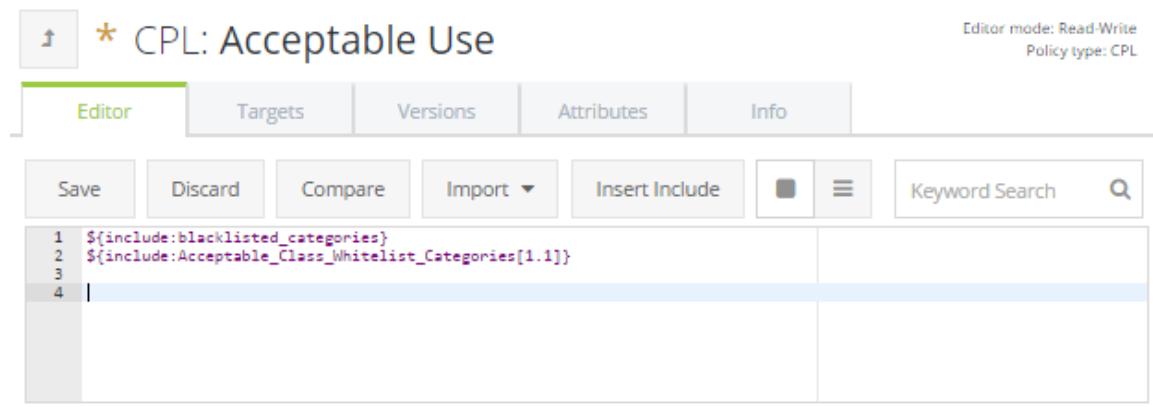
Layout Modes

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.

Note: 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.

[Policies](#) > [Acceptable Use](#)



The screenshot shows the 'CPL: Acceptable Use' editor interface. At the top, there's a breadcrumb navigation: Policies > Acceptable Use. To the right, it says 'Editor mode: Read-Write' and 'Policy type: CPL'. Below the header is a toolbar with tabs: Editor (which is selected and highlighted in green), Targets, Versions, Attributes, and Info. The toolbar also includes buttons for Save, Discard, Compare, Import, Insert Include, Keyword Search, and a magnifying glass icon. The main area is a code editor showing the following CPL code:

```

1 ${include:blacklisted_categories}
2 ${include:Acceptable_Class_Whitelist_Categories[1.1]}
3
4 |

```

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.

Management Center Configuration & Management

Policies > ASUP

* CPL: ASUP

Editor mode: Read-Write
Policy type: CPL

News Whitelist (Custom Solution)

default

override

mandatory

Shopping Whitelist (Custom Solution)

default

Please paste or enter policy here

override

mandatory

Quick Navigation

News Whitelist (Custom Solution)

default

override

mandatory

Shopping Whitelist (Custom Solution)

default

override

mandatory

Navigate sections

Note: 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.

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 311 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:



- 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.

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 256.
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   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 306 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:

```
; Deny EXE downloads
```

```
url.extension=.exe DENY
```

Another policy section has the purpose **Access Control**. It contains the following CPL:

```
; 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	How policy is evaluated	Resulting behavior
1. Threat protection - Inbound Policy	The Access Control section overrides the Threat protection section.	Everyone in the network is denied EXE downloads except for users in the specified subnet.
2. Access Control		
1. Access Control	The Threat protection section overrides the Access Control section.	Users in the specified subnet are allowed transactions with the exception of EXE downloads; everyone in the network is also denied EXE downloads.
2. Threat protection - Inbound Policy		

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.

Note: 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" on page 246).
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 316 below for details.

Examples

Substitute the device's serial number.

`${device.serialNumber}`

Substitute the value of the device's Rack attribute.

`${device.attributes.Rack}`

Caution: 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.

Variable	Description
<code> \${device.memberOf}</code>	List of the groups to which a device is assigned
<code> \${device.uuid}</code>	Internal ID of device
<code> \${device.modelNumber}</code>	Device model number
<code> \${device.description}</code>	Text in the Description field in device properties in Management Center
<code> \${device.name}</code>	Text in the Device Name field in device properties in Management Center
<code> \${device.serialNumber}</code>	Device's serial number
<code> \${device.osVersion}</code>	Operating system version running on the device
<code> \${device.type}</code>	The device type, for example, ProxySG.
<code> \${device.attributes.name}</code> where <i>name</i> is the attribute name	System or user-defined device attribute value, including any values inherited from the device group

Device Connection -

`\${device.connection.field}`

The following variables are available for policies and scripts. A variable might not be applicable to every device.

Variable	Description
<code> \${device.connection.host}</code>	Host IP address
<code> \${device.connection.port}</code>	Port number
<code> \${device.connection.connectionType}</code>	Designates the way the connection is established and optionally how authentication is performed. For example, SSH_PUBLIC_KEY
<code> \${device.connection.network}</code>	PRODUCTION or PREPRODUCTION
<code> \${device.connection.username}</code>	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).

Variable	Description
<code> \${policy.author}</code>	Last user who edited and saved the policy
<code> \${policy.description}</code>	Text in the Description field in policy properties
<code> \${policy.name}</code>	Text in the Name field in policy properties
<code> \${policy.referenceId}</code>	Text in the Reference Id field in policy properties
<code> \${policy.revision}</code>	Policy's current Version number
<code> \${policy.revisionDescription}</code>	Comments entered for the last revision
<code> \${policy.attributes.name}</code>	User-defined policy attribute value where <code>name</code> is the attribute name

Policy Fragment- `\${fragment.field}`

The following variables are available for policy fragments.

Variable	Description
<code> \${fragment.author}</code>	Last user who edited and saved the policy fragment
<code> \${fragment.description}</code>	Text in the Description field in policy fragment properties
<code> \${fragment.name}</code>	Text in the Name field in policy fragment properties
<code> \${fragment.referenceId}</code>	Text in the Reference Id field in policy fragment properties
<code> \${fragment.revision}</code>	Policy fragment's current Version number
<code> \${fragment.revisionDescription}</code>	Comments entered for the last revision
<code> \${fragment.attributes.name}</code>	User-defined policy fragment attribute value where <i>name</i> is the attribute name

Script - `${script.field}`

The following variables are available for scripts only (not policies).

Variable	Description
<code> \${script.author}</code>	Last user who edited and saved the script
<code> \${script.description}</code>	Text in the Description field in script properties
<code> \${script.versionDate}</code>	Date of last update
<code> \${script.name}</code>	Text in the Name field in script properties
<code> \${script.type}</code>	Selected Type in script properties
<code> \${script.revision}</code>	Script's current Version number
<code> \${script.revisionDescription}</code>	Comments entered for the last revision
<code> \${script.attributes.name}</code>	User-defined script attribute value where <i>name</i> 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.

Launch Legacy or Web-Based VPM

Select one of the following topics:

- "Launch Legacy Visual Policy Manager (Java)" on page 321
- "Launch Web-Based VPM" on page 337

Legacy VPM—Set Up and Enable Java in Your Browser

When using the legacy VPM editor, Symantec recommends that you use the recommended Java version listed [here](#).

Note: 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, and would like to launch the VPM editor from within Management Center, you will need to upgrade your ProxySG(s) to an appropriate SGOS version:

- For SGOS 6.5.x, use 6.5.9.10 or later
- For SGOS 6.6.x, use 6.6.4 or later
- For SGOS 6.7.x, use 6.7.2 or later

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.

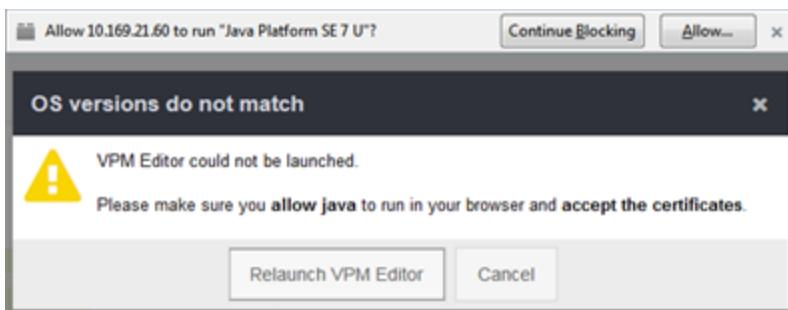
Note: If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the security http enable command. See # security for more information.

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>

Note: You may need to restart your browser after updating Java.

Note: 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:



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 Legacy Visual Policy Manager (Java)

This topic describes the requirements for running the legacy 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.

Legacy VPM Requirements

- When using the legacy 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 and wish to use the Java-based VPM editor from within Management Center, you will need to upgrade the ProxySG to an SGOS version where this issue is addressed. Depending on the branch of SGOS running on your ProxySG appliances, load the appropriate version to support Management Center:

- SGOS 6.5.x: 6.5.9.10 or later
- SGOS 6.6.x: 6.6.4.1 or later
- SGOS 6.7.x: 6.7.2.1 or later

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.

Note: 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 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, 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*.

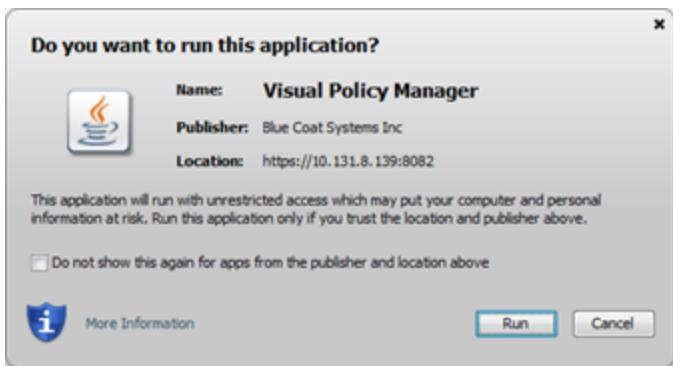
- Ensure that you have the latest VPM resource XML file installed on your ProxySG. You can download the XML file from the Symantec Support site:
<https://support.symantec.com/content/dam/bluecoat/download/modules/security/SGv6/policyclassifier.xml>

Launch the Legacy VPM

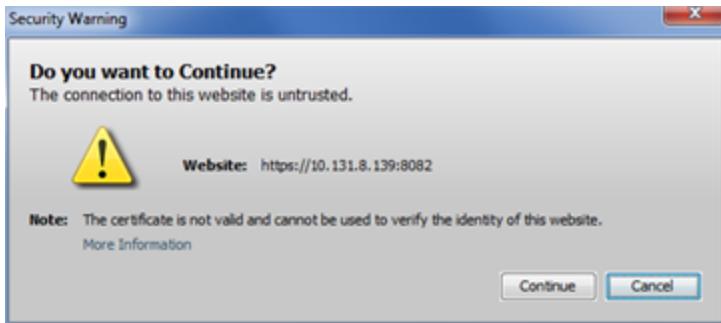
1. Select **Configuration > Policy**. From the **Policy Objects** list, locate the VPM policy object you want to edit. To narrow your search, you can do a "Filter by Attributes and Keyword Search" on page 256.

Note: To add a new VPM policy object, refer to "Add a VPM Policy Object" on the next page.

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 325.
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.

Caution: If Java is not enabled on your browser, the VPM Editor cannot launch. See "Legacy VPM—Set Up and Enable Java in Your Browser" on page 319.

Add a VPM 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.

Note: 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 312 for more information.
8. Click **Next**.
9. Enter or select values for the defined attributes.
10. Click **Finish**.

Select Reference Device for VPM Policy

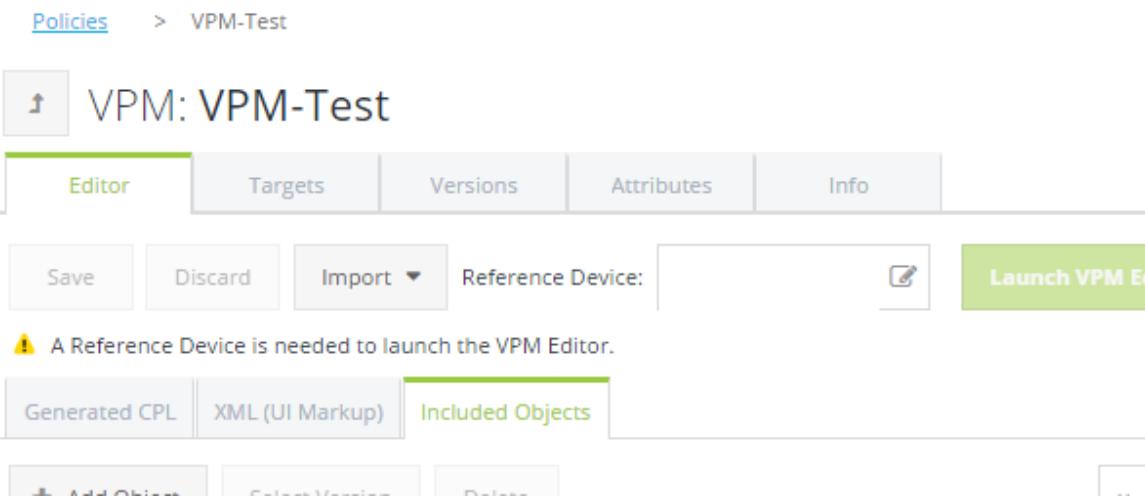
The reference device is the device you designate as the source device for VPM policy configurations. You must select a reference device to launch the VPM editor.

1. Select **Configuration > Policy**. From the Policy Objects list, select a VPM policy. Click **Edit**.

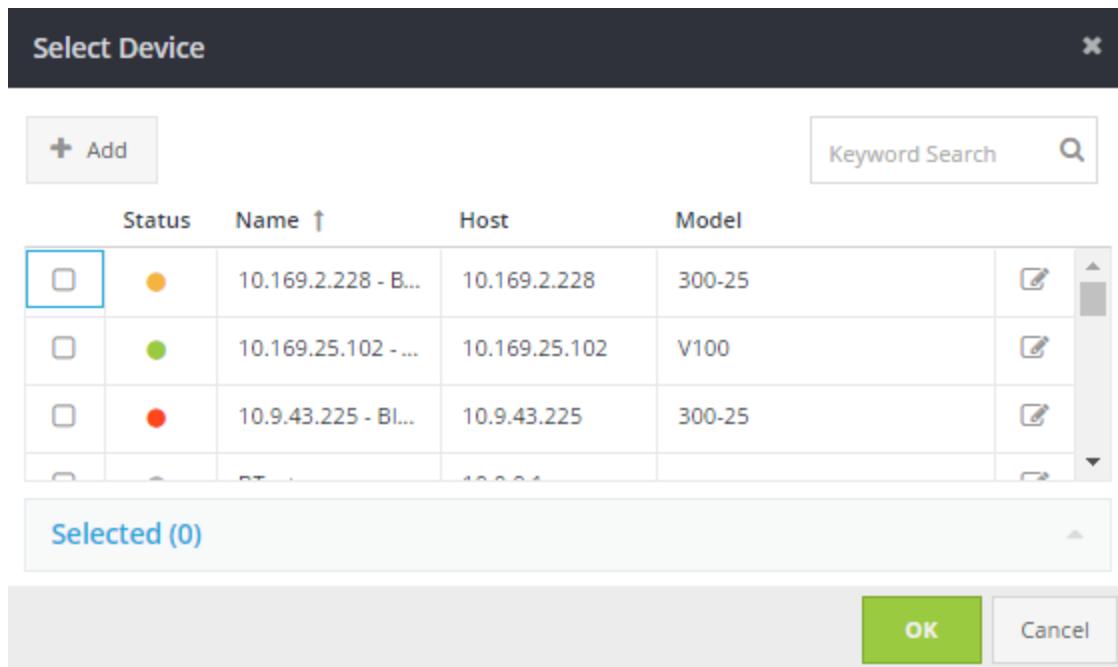
Tip: A default reference device is not automatically populated. Associate a least one deployed device with the policy or manually configure a reference device to enable editing.

2. While the **Editor** tab is selected, select a Reference Device, using the object selector .

Warning: 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

What do you want to accomplish?	Refer to this topic
Add or remove devices associated with the policy.	"Add or Remove Devices Associated with Policy" on page 480
Restore a version of the policy.	"Restore a Version of Policy " on page 493
Create and edit a VPM policy using the VPM Editor.	"Launch Legacy Visual Policy Manager (Java)" on page 321
Import a policy configuration from a device.	"Import Policy or Shared Objects" on page 457

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.

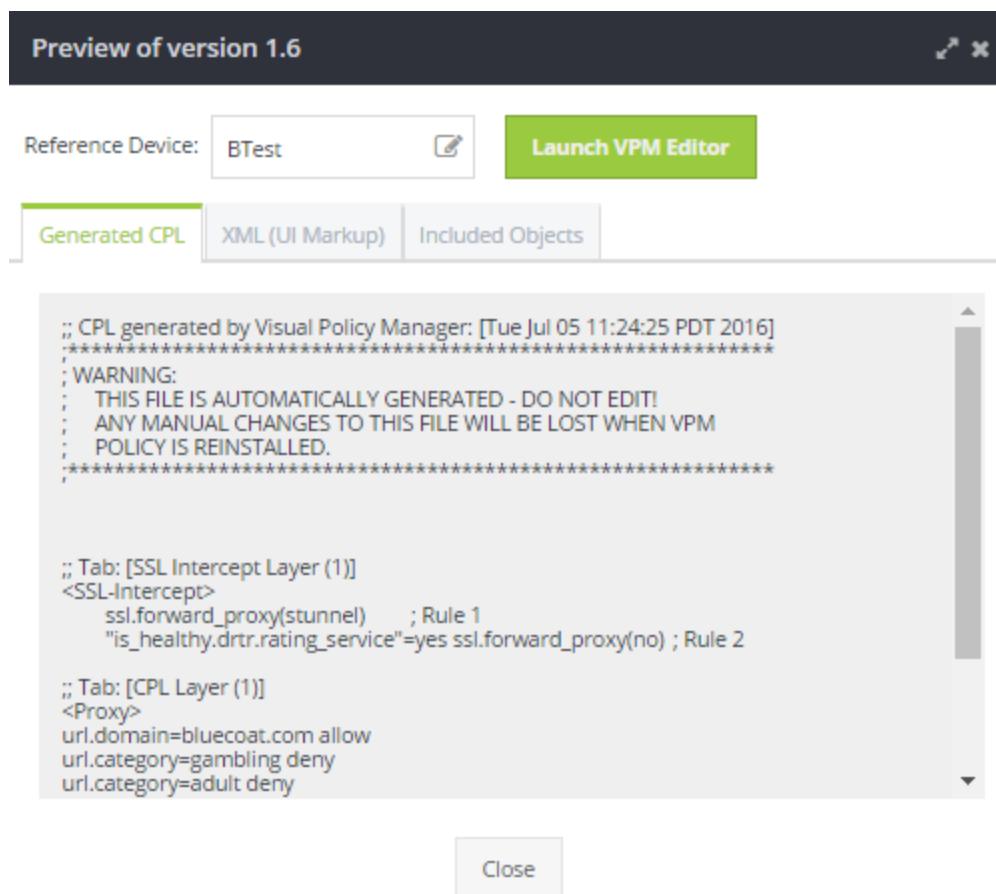
If needed, search for the policy object; see "Filter by Attributes and Keyword Search" on page 256.

Management Center Configuration & Management

3. With the policy selected, click **Editor**. The system displays the editor.

4. View the policy:

- Click **Last Generated CPL** to view the CPL source.
- Click **XML (UI Markup)** to view the XML source.



The screenshot shows a dialog box titled "Preview of version 1.6". At the top, there is a "Reference Device" dropdown set to "BTest" with a edit icon, and a green "Launch VPM Editor" button. Below the title bar are three tabs: "Generated CPL" (which is selected and highlighted in green), "XML (UI Markup)", and "Included Objects". The main content area displays the generated CPL code. It starts with a header indicating it was generated by Visual Policy Manager on Tuesday, July 05, 2016, at 11:24:25 PDT. It includes a warning message: "THIS FILE IS AUTOMATICALLY GENERATED - DO NOT EDIT! ANY MANUAL CHANGES TO THIS FILE WILL BE LOST WHEN VPM POLICY IS REINSTALLED." The code then defines two sections: "SSL Intercept Layer (1)" and "CPL Layer (1)". The "SSL Intercept" section contains rules for "ssl.forward_proxy(stunnel)" and "is_healthy.drtr.rating_service". The "CPL Layer" section contains rules for "url.domain=bluecoat.com", "url.category=gambling", and "url.category=adult". A "Close" button is located at the bottom left of the dialog.

```
;; CPL generated by Visual Policy Manager: [Tue Jul 05 11:24:25 PDT 2016]
*****
:WARNING:
; THIS FILE IS AUTOMATICALLY GENERATED - DO NOT EDIT!
; ANY MANUAL CHANGES TO THIS FILE WILL BE LOST WHEN VPM
; POLICY IS REINSTALLED.
*****

;; Tab: [SSL Intercept Layer (1)]
<SSL-Intercept>
    ssl.forward_proxy(stunnel)      ; Rule 1
    "is_healthy.drtr.rating_service"=yes ssl.forward_proxy(no) ; Rule 2

;; Tab: [CPL Layer (1)]
<Proxy>
url.domain=bluecoat.com allow
url.category=gambling deny
url.category=adult deny
```

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 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.**

The screenshot shows the 'Create New Shared Object: Basic Information' dialog box. At the top, there's a progress bar with 'Basic Information' highlighted. Below it, the 'Basic Information' tab is active. The form fields are as follows:

- Object name:** * Whitelist
- Object type:** * URL List
- Reference ID:** * Whitelist
- Description:** a list of URLs that are allowed
993 of 1024 characters left

At the bottom, there are 'Cancel', 'Back', and 'Next' buttons. The 'Next' button is highlighted in green.

- c. **Reference ID (*)** - Enter a Reference ID that you can filter for when building policy.

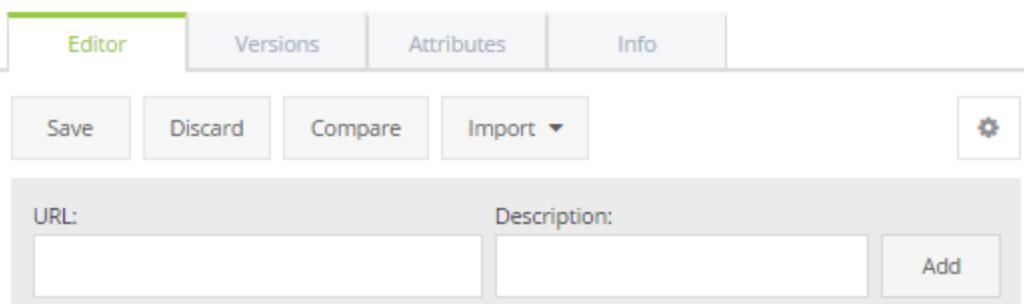
Note: The Reference ID must begin with a letter and must contain only letters, numbers, and "_".

- 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 584.
5. Click **Finish**. The URL list displays in the editor.

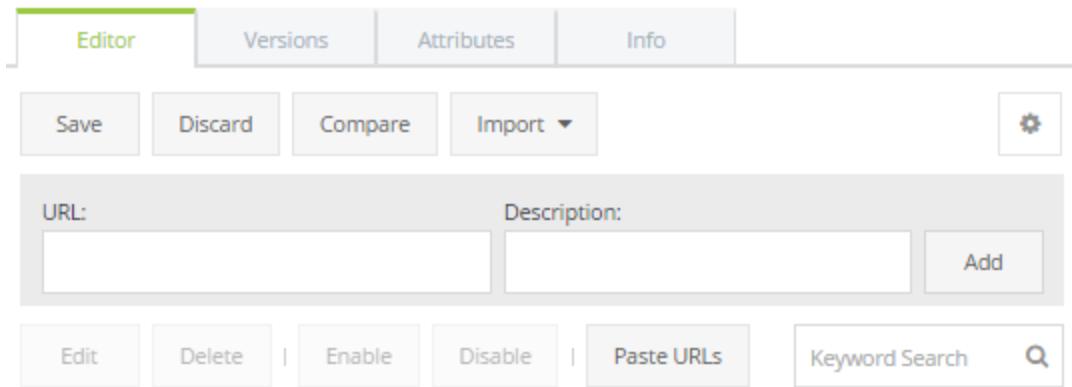
Step 2—Add URLs

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.**



Note: 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.**

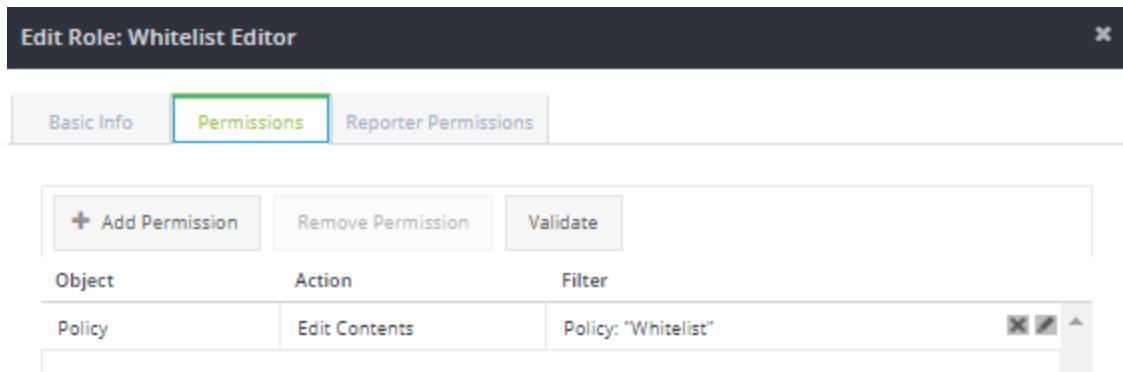


- c. Copy the URLs into the Paste URLs: Enter URLs dialog. Press **CTRL+V** or right-click and click **Paste**. The URLs are added to the list.
 - d. Click **Next**. The system opens the Paste URLs: Validate dialog.
 - e. Click **Finish**.
5. Click **Save**.

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."
- Note:** 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**.

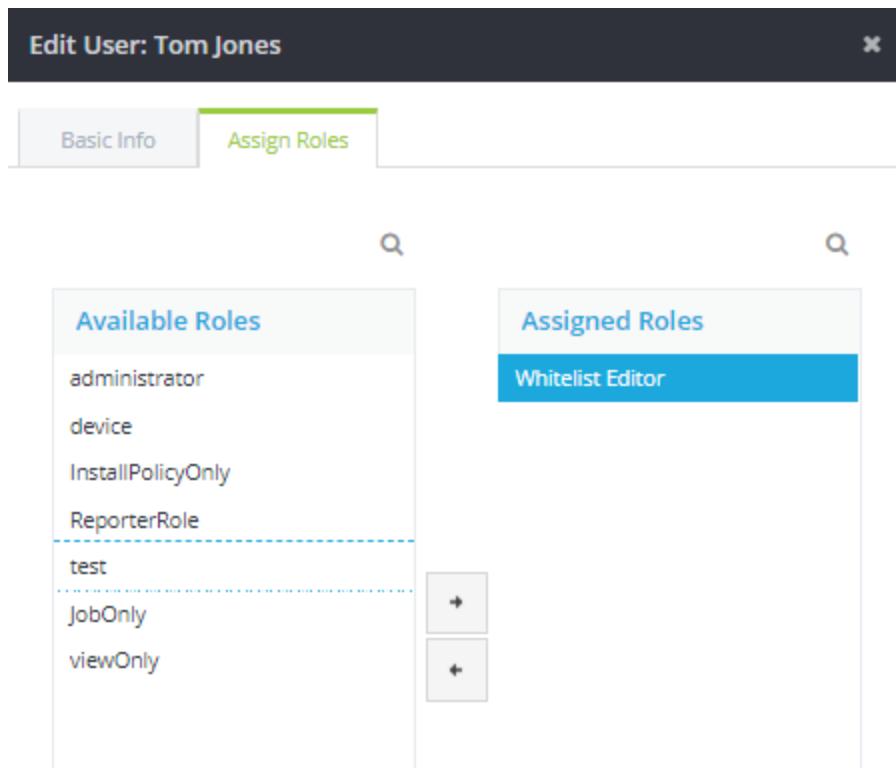
8. In the **Filter** drop-down list, select the URL whitelist you created in steps 1 and 2.



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.
6. Click **Save**. The web console banner displays an alert indicating that the user was saved.

Note: 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

Note: 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.

Note: 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 312 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

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Review the **Included Objects** section.
4. Any lists already included in the policy are displayed in 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**.

Tip: 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**.

Caution: 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**.

Note: The following steps are shown using the legacy VPM editor. If you use the web-based editor, see "Web-Based VPM Shared Include Example" on page 338 and "Launch Web-Based VPM" on page 337.

10. Select or create the desired policy layer.

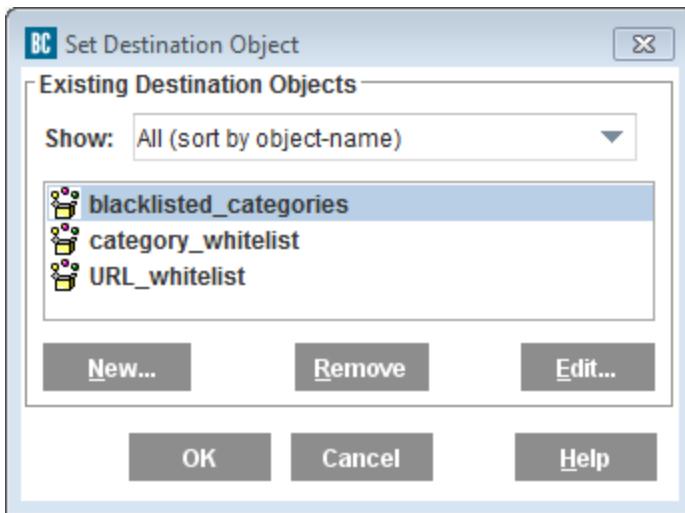
11. On the desired line number, right click the field under Destination and select Set from the menu.

No.	Source	Destination	Service	Action	Track	Comment
1	Any	Any		SSLInterce... None		
2	Any	Any		Disable S... None		

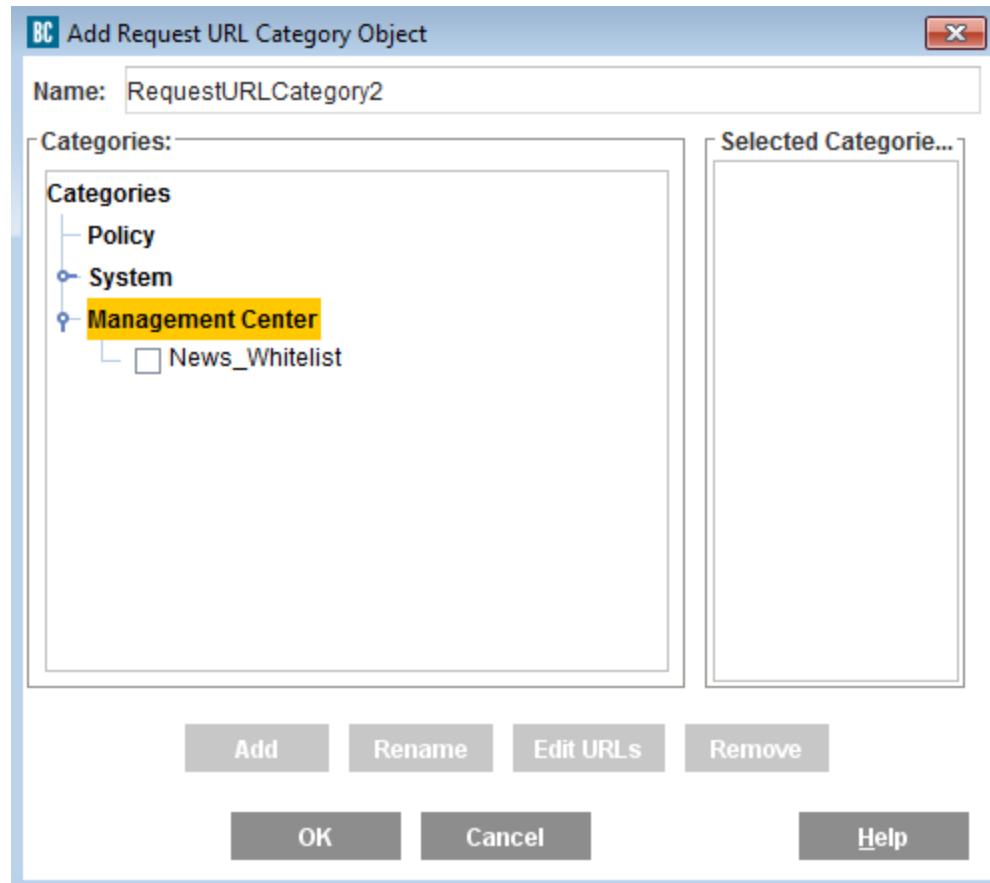
A context menu is open over the second row, with the 'Set...' option highlighted. Other options in the menu include 'Edit...', 'Delete', 'Negate', 'Cut', 'Copy', and 'Paste'.

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.



Note: 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**.

Note: For more information about adding or editing VPM Shared Objects, see [Create Shared Objects](#).

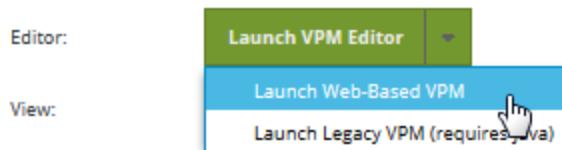
You are now ready to install the policy. From this point on, any user with the correct permissions can edit the list as needed without having to open the VPM.

Launch Web-Based VPM

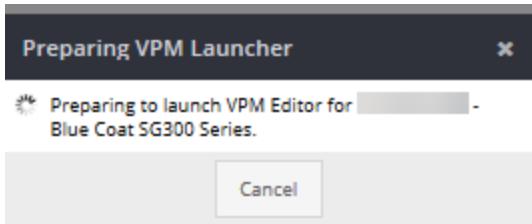
When editing a VPM policy object, you can choose to use the web-based VPM introduced in SGOS 6.7.4.x (if the device supports it).

Note: 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, as well as assigning and changing enforcement domains for policy rules in the VPM, refer to the [Web Visual Policy Manager WebGuide](#) and the [ProxySG Appliance Visual Policy Manager Reference](#).

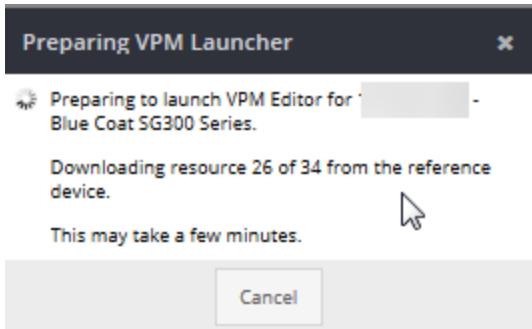
1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Click **Launch Web-Based VPM**.



The status indicates the VPM is launching.



4. Wait for the resources to download.



5. When the resources have finished downloading, the system displays the web-based VPM.

Layer Name	Type	Configuration
Web Access Layer (1)	Web Access	1 Rule

Source	Destination	Service	Time	Action	Track
Any	RequestURLCateg...	Any	Any	Deny	None

Web-Based VPM Shared Include Example

The following procedure describes how to include a shared policy object using the web-based VPM.

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Click **Launch Web-Based VPM**. The VPM opens in your browser.

Management Center Configuration & Management

Visual Policy Manager

The screenshot shows the Visual Policy Manager interface. At the top, there are search bars for 'Search All' and 'Search rules, layers'. A navigation bar includes 'Apply Policy', 'Add Layer', 'Operations', and 'Configuration'. Below this is a table with one row. The first column has a green toggle switch and a blue link 'Web Access Layer (1)'. The second column is 'Web Access TYPE'. The third column is '1 Rule CONFIGURATION'. The table rows are labeled 'SOURCE', 'Destination', 'Service', 'Time', 'ACTION', and 'Track'. The first row contains 'Any', 'RequestURLCateg...', 'Any', 'Any', 'Deny', and 'None'. There are also icons for 'Add rule', 'Edit', and 'Delete' at the top right of the table.

LAYER NAME	Web Access TYPE	1 Rule CONFIGURATION			
Any	RequestURLCateg...	Any	Any	Deny	None

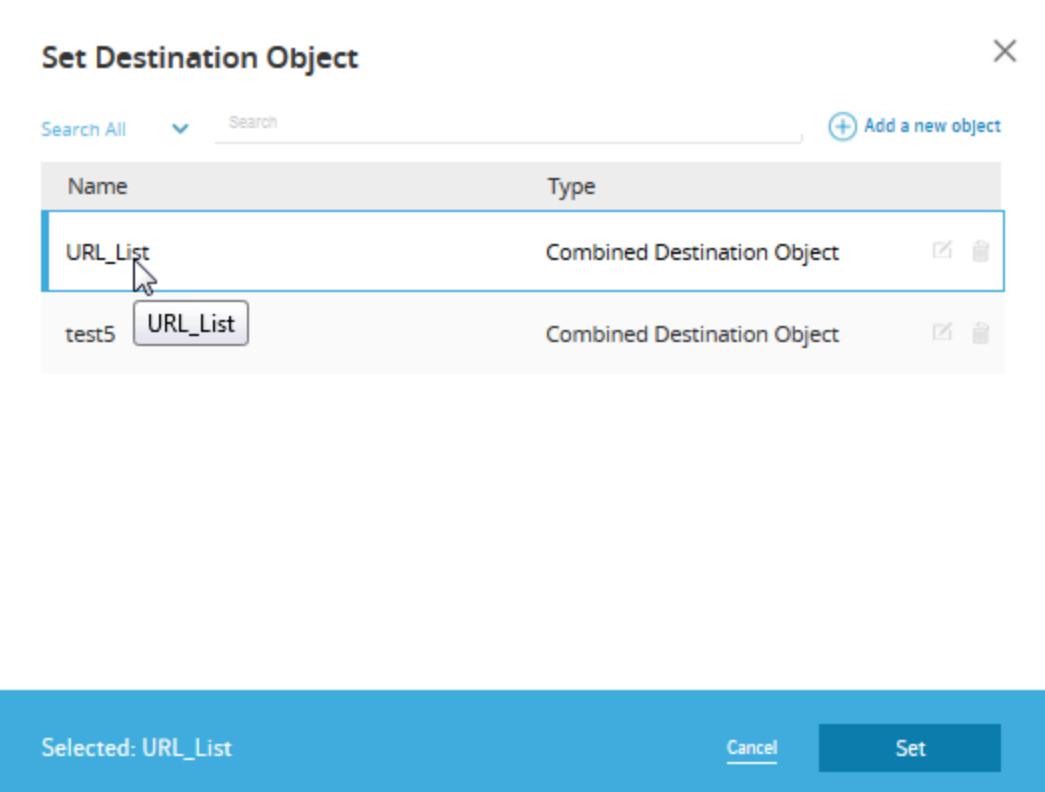
4. Select or create the desired policy layer.
5. **On the desired line number, click the field under Destination and select Set from the menu.**

VPM: VPM Test

The screenshot shows the Visual Policy Manager interface with the title 'VPM: VPM Test'. It features a search bar for 'Search All' and 'Search rules, layers'. The main area displays a table with one row. The first column has a green toggle switch and a blue link 'Web Access Layer (1)'. The second column is 'Web Access TYPE'. The third column is '1 Rule CONFIGURATION'. The table rows are labeled 'Source', 'Destination', 'Service', and 'Time'. The first row contains 'Any', 'Any', 'Any', and 'Any'. A context menu is open over the 'Destination' field of the first row. The menu items are: Set (highlighted with a cursor icon), Edit, Delete, Negate, Cut, Copy, Paste, and View Occurrences.

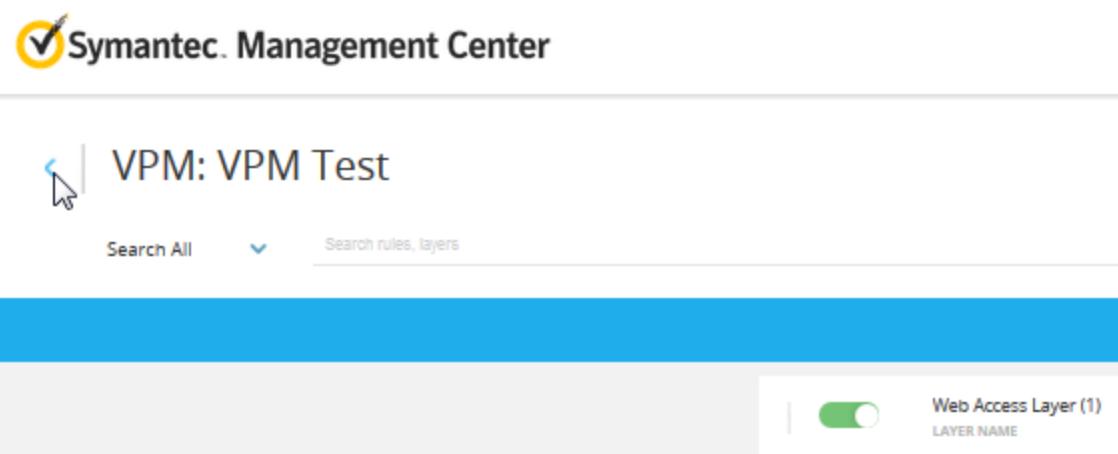
Source	Destination	Service	Time
Any	Any	Any	Any

6. Select the desired list:



7. (Optional) Set the desired action condition by clicking the **Action** field.
8. When finished setting the destination and conditions, click **Save policy**.

To exit the VPM Editor without saving changes, click the back arrow in the upper-left corner.



9. Enter a brief description of the policy changes in the **Save Changes** field, click **Save**.
10. Use the back arrow to exit the VPM Editor.

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.

Note: 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.

Note: 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 344

"Include a Shared Policy Object in CPL or VPM Policy" on page 355

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 363

"Category List Example" on page 368

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 374

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 345

"URL List Example" on page 349

Create an IP Address List

Easily create IP address lists for use on the SSL Visibility appliance.

"Create IP Address List " on page 417

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 353

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 215

Creating a WAF Security Profile is step 3 in "Use WAF Policy To Protect Servers From Attacks" on page 199.

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.

Note: 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.

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.

Note: 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 312.

Note: If Replace substitution variables is NOT selected when creating a CPL Policy, the CPL Policy Fragments *will not* be included in the CPL.

Create New Shared Object: Basic Information ×

Basic Information Attributes

Object name:	* Data Loss Prevention
Object type:	* CPL Fragment
Reference ID:	* Data_Loss_Prevention
Description:	1024 of 1024 characters left

Replace substitution variables

Cancel Back Next

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 584.
4. Click **Finish**. The fragment displays in the Policy Objects list.
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.

Note: 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

Basic Information Attributes

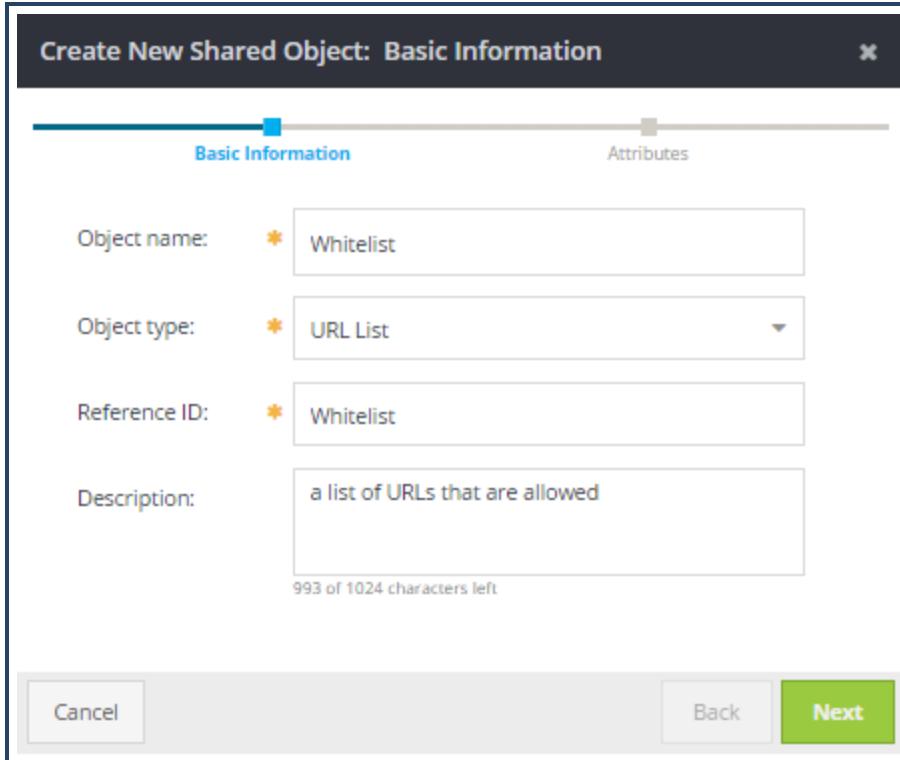
Object name: * Whitelist

Object type: * URL List

Reference ID: * Whitelist

Description: a list of URLs that are allowed
993 of 1024 characters left

Cancel Back Next



- c. **Reference ID (*)** - Enter a Reference ID that you can filter for when building policy.

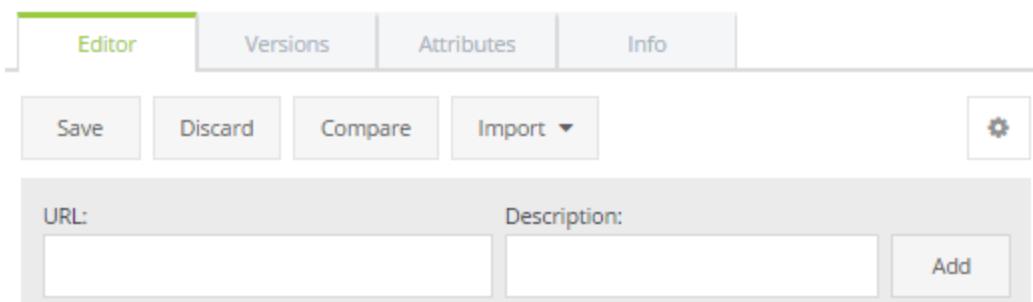
Note: The Reference ID must begin with a letter and must contain only letters, numbers, and "_".

- 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 584.
 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.

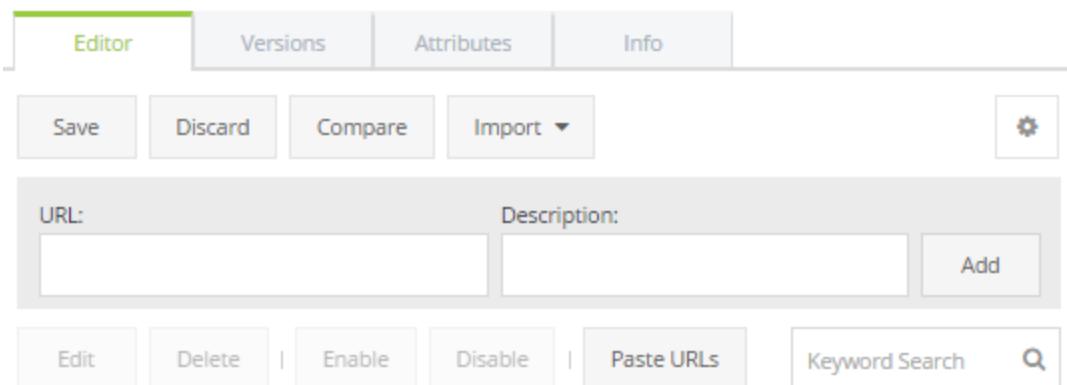
3. Enter the URL in the URL field and click Add.



Note: The system displays the text entered into the **Description** field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:

- Create a URL list and copy the URLs.
- Click Paste URLs. The system opens the Paste URLs: Enter URLs dialog.**

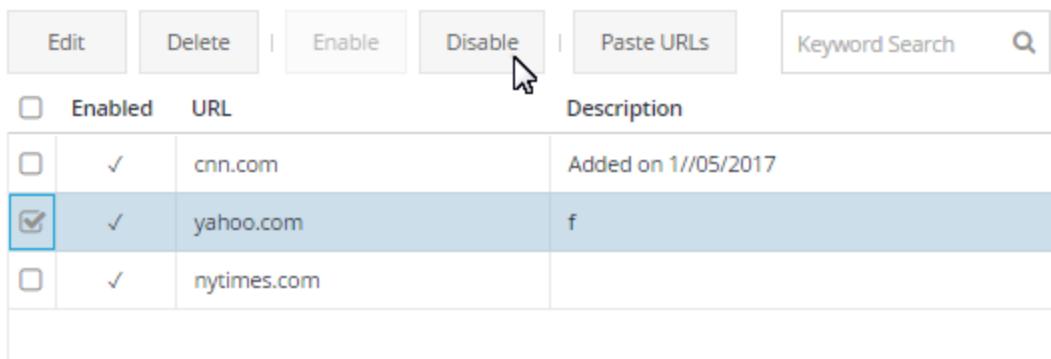


- Copy the URLs into the Paste URLs: Enter URLs dialog. Press **CTRL+V** or right-click and click **Paste**. The URLs are added to the list.
- Click **Next**. The system opens the Paste URLs: Validate dialog.
- Click **Finish**.

5. Click **Save.**

Enabling and Disabling URLs

You can disable an individual URL by selecting it and clicking Disable.



		URL	Description
Enabled	URL	Description	
<input type="checkbox"/>	cnn.com	Added on 1/05/2017	
<input checked="" type="checkbox"/>	yahoo.com	f	
<input type="checkbox"/>	nytimes.com		

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 355. The URL list will be included in the CPL as a named condition that can then be referenced using `condition=referenceld`. See the example below for details.

You can then install your policy as described in "Install Policy" on page 451.

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.

```

Define subnet corporate_subnet
  198.51.100.0/24
end

<proxy "Web Access">
  client.address=corporate_subnet ALLOW

<proxy "Web Auth">
  authenticate(corp_realm)

<proxy "Web Filter">
  url.domain=playboy.com FORCE_DENY
  category=(gambling, hacking, games, news) exception(content_filter_denied)

<proxy "Restricted Access">
  group=execs, managers url.domain=fantasyfootball.com ALLOW

```

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.

	Enabled	URL	Description
<input type="checkbox"/>	✓	cnn.com	Added on 1/05/2017
<input type="checkbox"/>	✓	yahoo.com	f
<input type="checkbox"/>	✓	nytimes.com	

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:

```
Define subnet corporate_subnet
 198.51.100.0/24
end

${include: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=(gambling, hacking, games, news) exception(content_filter_denied)

<proxy "Restricted Access">
  group=execs, managers url.domain=fantasyfootball.com ALLOW
```

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 "Web Auth">
  authenticate(corp_realm)

<proxy "Web Filter">
  url.domain=playboy.com  FORCE_DENY
  category=(gambling, hacking, games, news)  exception(content_filter_denied)

<proxy "Restricted Access">
  group=execs, managers  url.domain=fantasyfootball.com  ALLOW
```

Note: 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)
```

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.

Note: 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. By default, the url.* triggers are used. You can switch to the server_url.* triggers if needed (for example, if the URL list is used in a forwarding layer).

Subcondition	Associated Trigger	Example
<i>list_name/url.domains</i>	url.domain Tests the URL. All URLs that have been entered are included in this subcondition. You cannot disable this subcondition.	example.com/us example.com 198.51.100.10

Subcondition	Associated Trigger	Example
<i>list_name/server_url.domains</i>	server_url.domain	example.com/us example.com 198.51.100.10
	Tests the URL used to fetch content from the origin server. All URLs that have been entered are included in this subcondition.	
	You cannot disable this subcondition when the server_url triggers are enabled.	
<i>list_name/certificate_hostnames</i>	server.certificate.hostname	example.com
	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.	
	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.	
	You can disable this subcondition.	
<i>list_name/addresses</i>	url.address	198.51.100.10
	All IP addresses that have been entered are included in this subcondition.	
	url.address allows the ProxySG to compare an IP-address-based URL list entry to the server's IPv4 address.	
	You can disable this subcondition.	
<i>list_name/server_addresses</i>	server_url.address	198.51.100.10
	Tests the host's IP address used to fetch content from the origin server.	
	All IP addresses that have been entered are included in this subcondition.	
	server_url.address allows the ProxySG to compare an IP-address-based URL list entry to the server's IPv4 address.	
	You can disable this subcondition.	

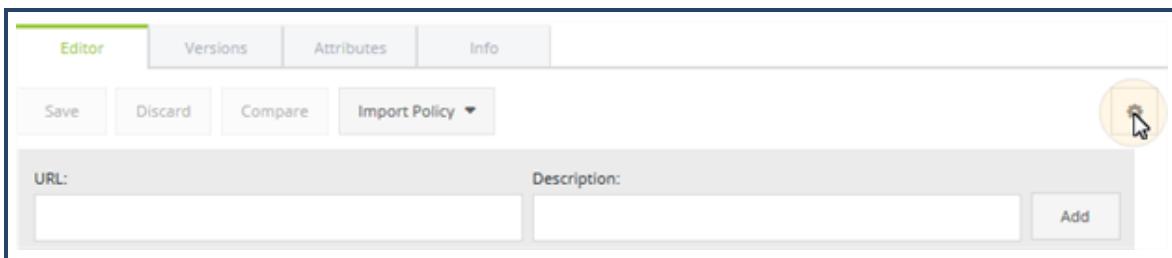
Category List Triggers

The included category list subconditions and triggers are described in the following table.

Subcondition	Associated Trigger	Example
<i>list_name/category</i>	category	category='Adult/Mature Content'
<i>list_name/cert_category</i>	server.certificate.hostname.category	server.certificate.hostname.category='Adult/Mature Content'

Change 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. Select or deselect the desired triggers and click **Save**.

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 344.

CPL Policy Fragments

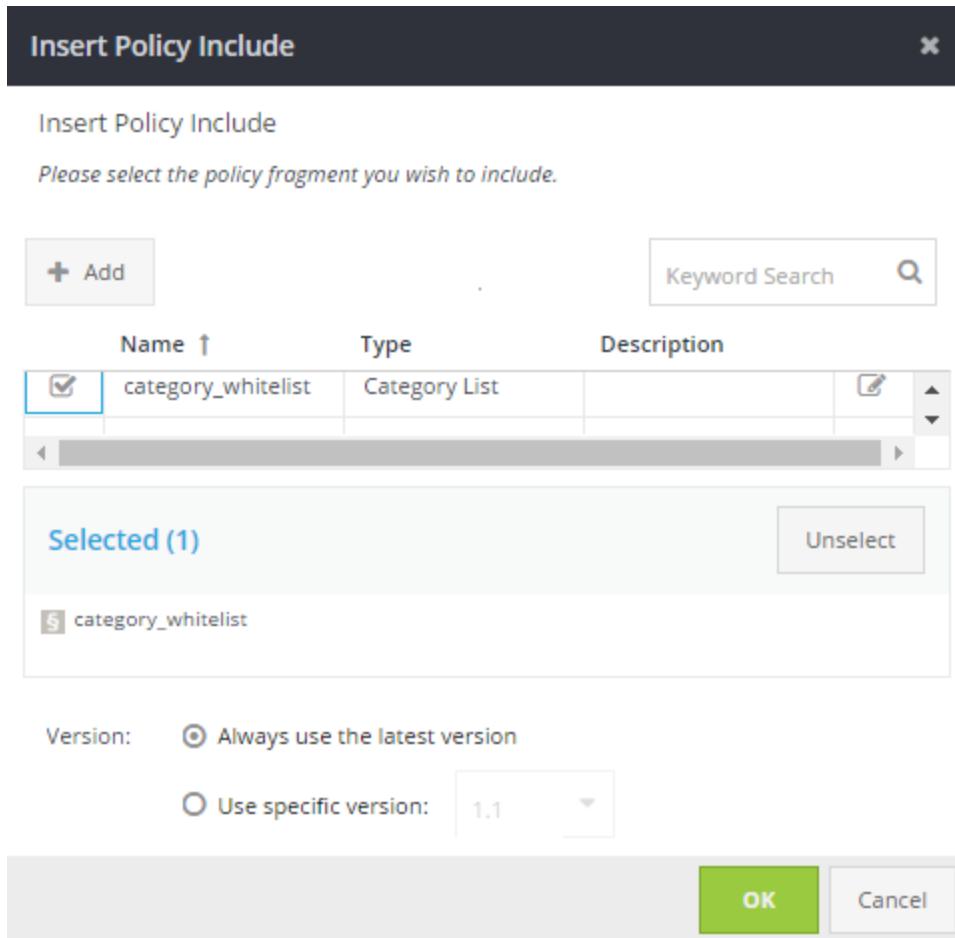
Include a CPL fragment, URL list, or category list as a building block of CPL Policy.

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.

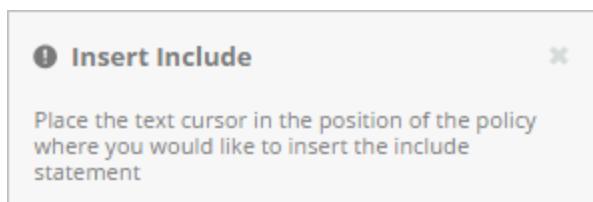
Note: If you do NOT enable variable substitution in the CPL, the CPL Fragments will not be included.

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.**

Management Center Configuration & Management



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.**

[Policies](#) > test12

The screenshot shows the CPL policy editor interface. At the top, it displays "CPL: test12". Below this is a toolbar with tabs for "Editor", "Targets", "Versions", "Attributes", and "Info". The "Editor" tab is selected. To the right of the toolbar, it says "Editor mode: Read-Write" and "Policy type: CPL". Below the toolbar are buttons for "Save", "Discard", "Compare", "Import", "Insert Include", and various icons for selection and modification. The main content area contains a tree view of policy sections. The "Untitled" section is expanded, showing the "default" section which contains the code "\${include:category_whitelist}". Below "default" are collapsed sections for "override" and "mandatory". To the right of the content area is a vertical "Quick Navigation" bar.

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.

Note: For more information about adding or editing CPL Policy sections, see "Add or Edit CPL Policy Sections" on page 298.

VPM Shared Objects

Reference categories, category 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}.

Note: 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.

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Review the **Included Objects** section.
4. Any lists already included in the policy are displayed in 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**.

Tip: 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**.

Caution: 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.

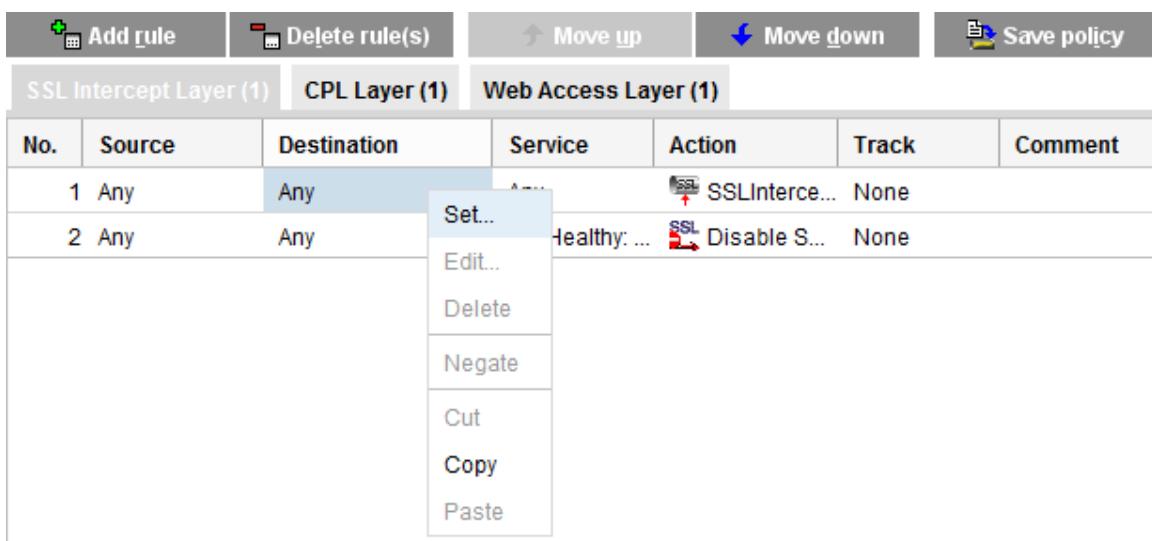
8. Once finished editing the available shared objects for the policy, click **Save**.

9. Click **Launch VPM Editor**.

Note: The following steps are shown using the legacy VPM editor. If you use the web-based editor, see "Web-Based VPM Shared Include Example" on page 338 and "Launch Web-Based VPM" on page 337.

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.**

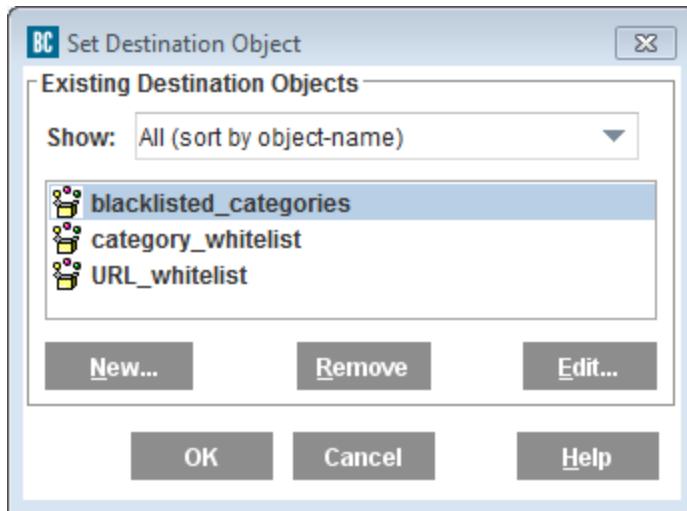


The screenshot shows the VPM Editor interface with the 'SSL Intercept Layer (1)' selected. A context menu is open over the second rule, which has 'Any' listed in both the Source and Destination columns. The menu options include 'Set...', 'Edit...', 'Delete', 'Negate', 'Cut', 'Copy', and 'Paste'. The 'Set...' option is highlighted.

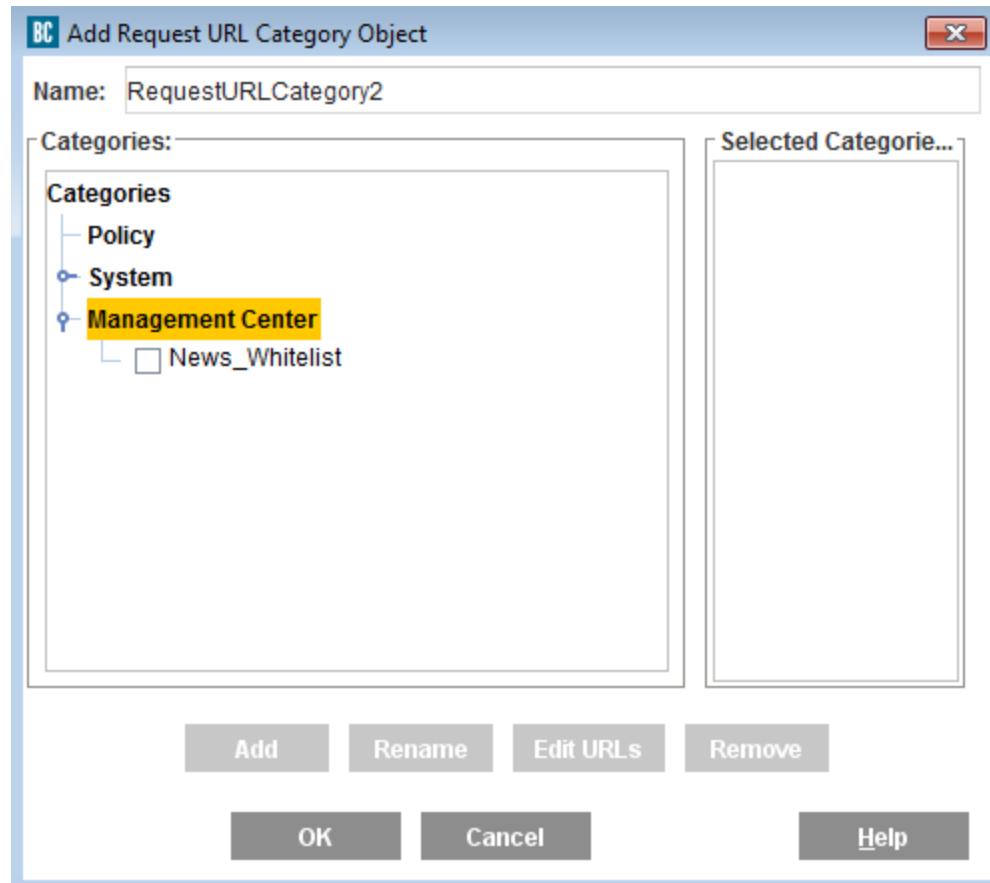
No.	Source	Destination	Service	Action	Track	Comment
1	Any	Any		SSLInterce...	None	
2	Any	Any	healthy: ...	SSL Disable S...	None	

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.



Note: 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**.

Note: For more information about adding or editing VPM Shared Objects, see [Create Shared Objects](#).

Work with Categories

Refer to the following topics:

- "Create Category Lists" below
- "Category List Example" on page 368
- "Use Category List Templates" on page 374
- "Create Custom Categories" on page 382
- "Custom Category Example" on page 386

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](#).

Note: Before completing this procedure, you might want to verify that your [categories are up-to-date](#).

Category lists include [policy triggers that you may want to disable](#) to improve performance.

Note: 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

Basic Information Attributes

Basic Information

Object name: * [Text input field]

Object type: * [Select dropdown] Category List

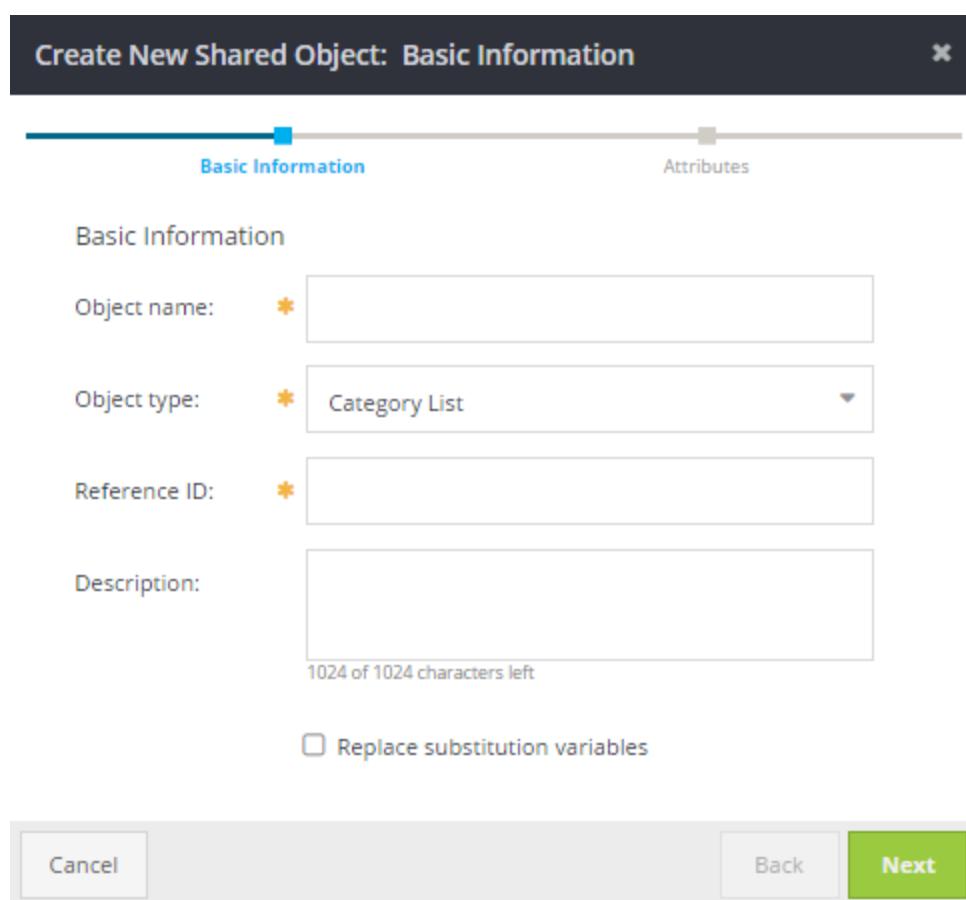
Reference ID: * [Text input field]

Description:

1024 of 1024 characters left

Replace substitution variables

Cancel **Back** **Next**



- **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.

Note: 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 374 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 584.
 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.**

[Shared Objects](#) > blacklisted_categories

Category	Description	Examp...
- <input type="checkbox"/> <input checked="" type="checkbox"/> Business Related (5 of 23)		
+ <input type="checkbox"/> <input checked="" type="checkbox"/> Commerce		
+ <input type="checkbox"/> <input checked="" type="checkbox"/> Information Related		
+ <input type="checkbox"/> <input checked="" type="checkbox"/> Technology (5 of 7)		
- <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> Legal Liability (15 of 15)		
+ <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> Adult Related (8 of 8)		

Note: 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.

Management Center Configuration & Management

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 and examples as well.

Shared Objects > blacklisted_categories

* Category List: blacklisted_categories

Editor mode: Read-Write
Object type: Category List

Category	Description	Examples
Technology (4 of 7)		
Computer/Information Secur...	Sites that provide information or too...	metasploit.com...
Content Servers	Servers that provide commercial hos...	cdnetworks.co...
Internet Connected Devices	Sites that allow management and m...	online.wilife.co...
Non-Viewable/Infrastructure	Servers that provide Internet infrastr...	safebrowsing.cl...
Office/Business Applications	Sites with interactive, Web-based offi...	docs.google.co...
Technology/Internet	Sites that sponsor or provide inform...	pcworld.com, c...
Web Hosting	Sites of organizations that provide to...	blogspot.com, a...
Legal Liability (15 of 15)		
Adult Related (8 of 8)		

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 355. In addition, you must create an allow/deny condition using `condition=referenceld`. See the "Category List Example" below for details.

You can then install your policy as described in "Install Policy" on page 451.

Tip: If you want to check into which category Symantec WebPulse categorizes a URL, go to 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.

Management Center Configuration & Management

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.**

Category	Description
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Adult Related (8 of 8)	
<input checked="" type="checkbox"/> <input type="checkbox"/> Adult/Mature Content	Sites that contain material of adult nature that does not necessarily include nudity or explicit sexual content.
<input checked="" type="checkbox"/> <input type="checkbox"/> Extreme	Sites that are extreme in nature and are not suitable for general audiences.
<input checked="" type="checkbox"/> <input type="checkbox"/> Intimate Apparel/Swimsuit	Sites that contain images or offer the sale of swimsuits or intimate apparel.
<input checked="" type="checkbox"/> <input type="checkbox"/> Mixed Content/Potentially Ad...	Sites with generally non-offensive content but that also have some potentially sensitive or controversial material.
<input checked="" type="checkbox"/> <input type="checkbox"/> Nudity	Sites containing nude or seminude depictions of the human body.
<input checked="" type="checkbox"/> <input type="checkbox"/> Pornography	Sites that contain sexually explicit material for the purpose of arousal or stimulation.
<input checked="" type="checkbox"/> <input type="checkbox"/> Sex Education	Sites that provide information (sometimes graphic) on reproductive health and sexual education.
<input checked="" type="checkbox"/> <input type="checkbox"/> Sexual Expression	Sites that provide information about, promote, or cater to sexual expression and behavior.
<input checked="" type="checkbox"/> <input type="checkbox"/> Liability Concerns (7 of 7)	
<input checked="" type="checkbox"/> <input type="checkbox"/> Child Pornography	Sites that include a visual depiction of a minor engaging in sexual activity or being used for sexual purposes.
<input checked="" type="checkbox"/> <input type="checkbox"/> Controlled Substances	Sites that discuss, encourage, promote, offer, sell, supply or distribute controlled substances.
<input checked="" type="checkbox"/> <input type="checkbox"/> Gambling	Sites where a user can place a bet or participate in a betting game.
<input checked="" type="checkbox"/> <input type="checkbox"/> Piracy/Copyright Concerns	Sites that provide information or technology for cracking or bypassing digital rights management (DRM).
<input checked="" type="checkbox"/> <input type="checkbox"/> Scam/Questionable/Illegal	Sites that advocate or give advice on performing acts that are illegal, deceptive, or harmful.
<input checked="" type="checkbox"/> <input type="checkbox"/> Violence/Hate/Racism	Sites that depict extreme physical harm to people, animals or property, or promote hate or racism.

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.**

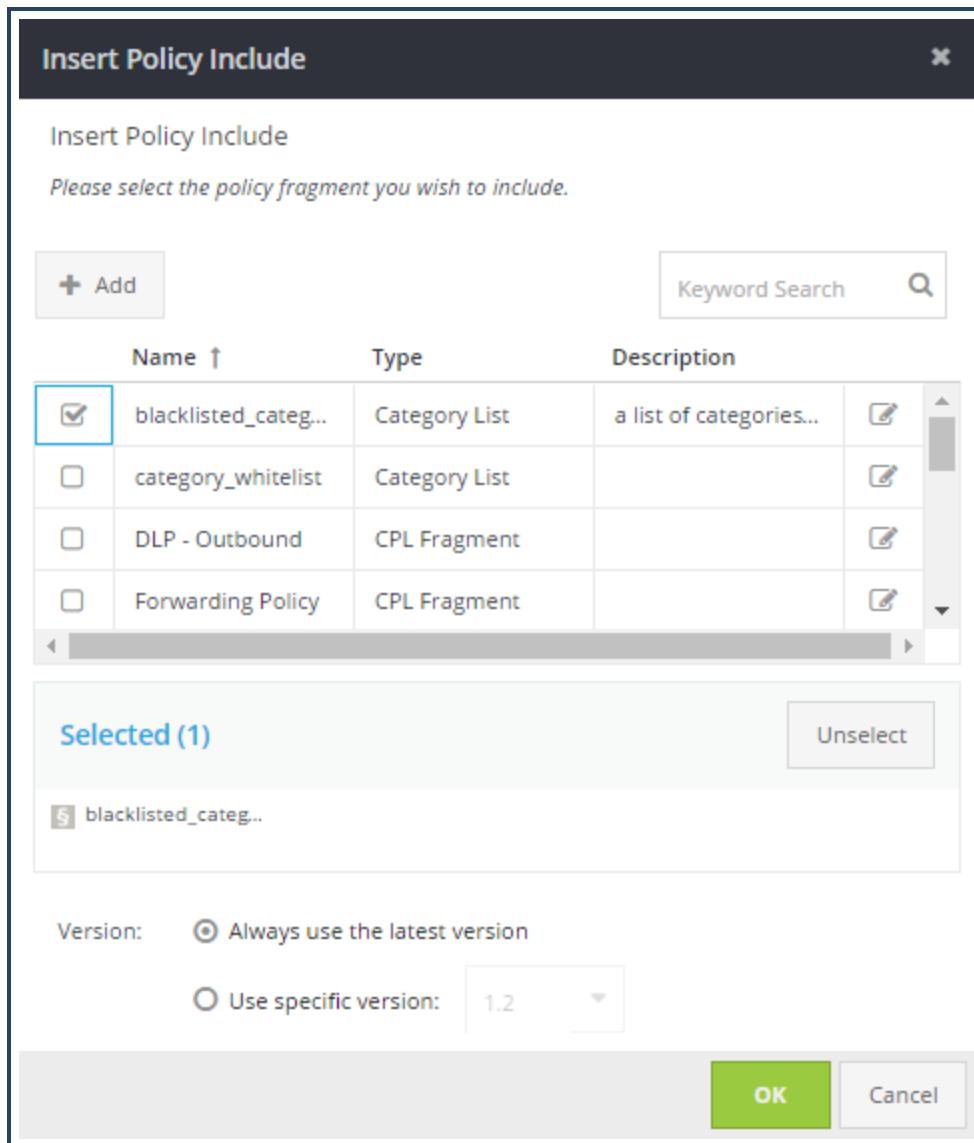
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Security (4 of 14)	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> File Transfer	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Security Concerns	
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Security Threats (4 of 4)	
<input checked="" type="checkbox"/> <input type="checkbox"/> Malicious Outbound Data/Bo...	Sites to which botnets or other mal
<input checked="" type="checkbox"/> <input type="checkbox"/> Malicious Sources/Malnets	Sites that host or distribute malwar
<input checked="" type="checkbox"/> <input type="checkbox"/> Phishing	Sites that are designed to appear a
<input checked="" type="checkbox"/> <input type="checkbox"/> Proxy Avoidance	Sites that provide information on h
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Uncategorized	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Uncategorized	

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.**

Management Center Configuration & Management



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
```

```
 ${include:blacklisted_categories}
```

```
<Proxy>
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.**

Management Center Configuration & Management

```
Preview N X

define condition blacklisted_categories/url_category
    category='Adult/Mature Content'
    category='Child Pornography'
    category='Computer/Information Security'
    category='Content Servers'
    category='Controlled Substances'
    category=Extreme
    category=Gambling
    category='Internet Connected Devices'
    category='Intimate Apparel/Swimsuit'
    category='Malicious Outbound Data/Botnets'
    category='Malicious Sources/Malnets'
    category='Mixed Content/Potentially Adult'
    category=Nudity
    category='Office/Business Applications'
    category=Phishing
    category='Piracy/Copyright Concerns'
    category=Pornography
    category='Proxy Avoidance'
    category='Scam/Questionable/Illegal'
    category='Sex Education'
    category='Sexual Expression'
    category='Violence/Hate/Racism'
    category=Weapons
    category='Web Hosting'
end

define condition blacklisted_categories/cert_category
    server.certificate.hostname.category='Adult/Mature Content'
    server.certificate.hostname.category='Child Pornography'
    server.certificate.hostname.category='Computer/Information Security'
    server.certificate.hostname.category='Content Servers'
    server.certificate.hostname.category='Controlled Substances'
    server.certificate.hostname.category=Extreme
    server.certificate.hostname.category=Gambling
    server.certificate.hostname.category='Internet Connected Devices'
    server.certificate.hostname.category='Intimate Apparel/Swimsuit'
    server.certificate.hostname.category='Malicious Outbound Data/Botnets'
    server.certificate.hostname.category='Malicious Sources/Malnets'
    server.certificate.hostname.category='Mixed Content/Potentially Adult'
    server.certificate.hostname.category=Nudity
    server.certificate.hostname.category='Office/Business Applications'
    server.certificate.hostname.category=Phishing
    server.certificate.hostname.category='Piracy/Copyright Concerns'
    server.certificate.hostname.category=Pornography
    server.certificate.hostname.category='Proxy Avoidance'
    server.certificate.hostname.category='Scam/Questionable/Illegal'
    server.certificate.hostname.category='Sex Education'
    server.certificate.hostname.category='Sexual Expression'
    server.certificate.hostname.category='Violence/Hate/Racism'
    server.certificate.hostname.category=Weapons
    server.certificate.hostname.category='Web Hosting'
end

define condition blacklisted_categories
    condition=blacklisted_categories/url_category
    condition=blacklisted_categories/cert_category
end

<Proxy>
condition=blacklisted_categories DENY

Close
```

Note: 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.

Note: Before completing this procedure, you might want to verify that your [categories are up-to-date](#).

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**.

Create New Shared Object: Basic Information

Basic Information Attributes

Basic Information

Object name: * category_list_restricted

Object type: * CPL Fragment

Reference ID: * category_list_restricted

Description: a subset of categories for a user with restricted permissions
963 of 1024 characters left

Replace substitution variables

Cancel **Back** **Next**

- **Reference ID** - Enter a Reference ID (or accept the default name).

Note: 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 584.
 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

Category	Description	Examples
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Legal Liability		
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Adult Related		
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Liability Concerns		
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Non-Productive (32 of 32)		
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Communication (5 of 5)		
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Health Related (6 of 6)		
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Leisure (6 of 6)		
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Multimedia (4 of 4)		
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Social Interaction (4 of 4)		
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Society/Government (7 of 7)		
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Security (4 of 14)		
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> File Transfer		

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 ×

Basic Information Attributes

Basic Information

Object name: *

Object type: *

Reference ID: *

Description:
1024 of 1024 characters left

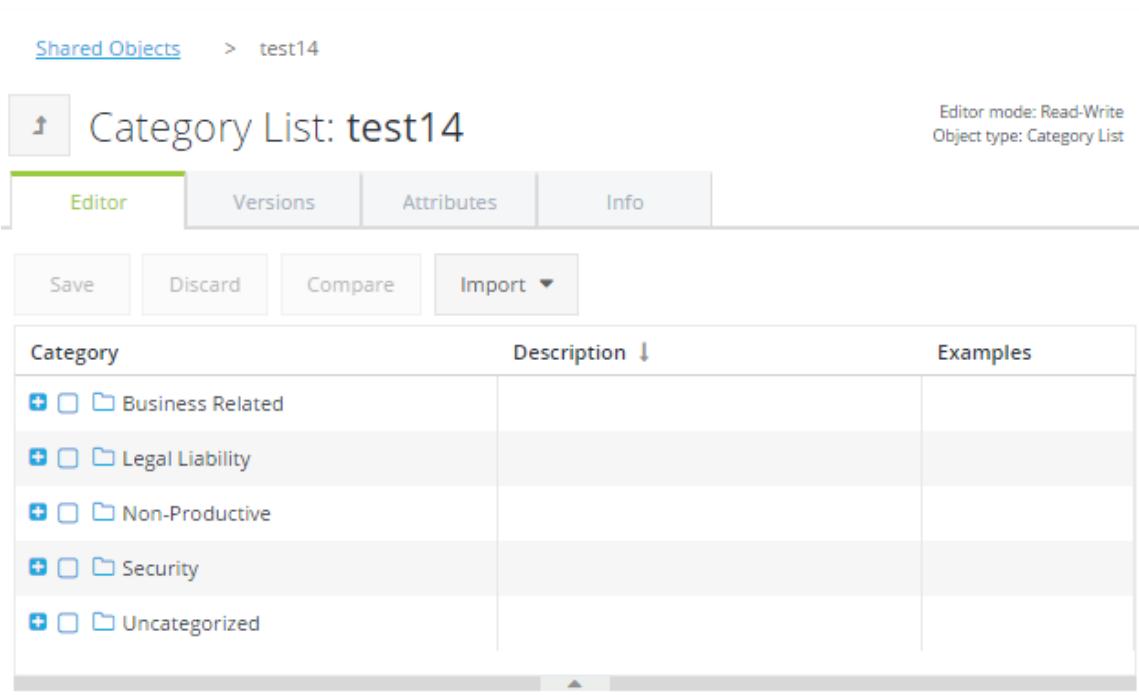
Replace substitution variables

Cancel Back Next

- **Reference ID (*)** - Enter a Reference ID (or accept the default name) that you can use when building policy. The ID can be specified as the condition name in CPL.

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

- **Template** — Click  and select the template. The template will restrict what categories can be defined in the list.
 - **Description** - Enter a meaningful description to help you when reusing this category list.
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 584.
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.**



Category	Description ↓	Examples
+ <input type="checkbox"/> Business Related		
+ <input type="checkbox"/> Legal Liability		
+ <input type="checkbox"/> Non-Productive		
+ <input type="checkbox"/> Security		
+ <input type="checkbox"/> Uncategorized		

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 355.

Note: 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.

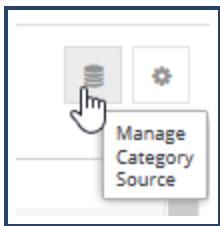
Note: When the CPL for a category list is generated and the list contains categories not present in the template (most likely because the template had been changed since last saving the list), those categories are not included in the condition definition CPL. If this occurs, a warning is included as a comment above the condition CPL, indicating which categories were removed.

Update Symantec Global Intelligence Network (BCIS/BCWF) Category Lists

The category list used to select the categories associated with category list or category list template objects (**Policy > Shared Objects**) might not match the list provided by sitereview.bluecoat.com. To ensure that the list of categories are synchronized with the latest updates, complete the following actions.

Note: You must have the **Settings > Update** permission to perform this operation.

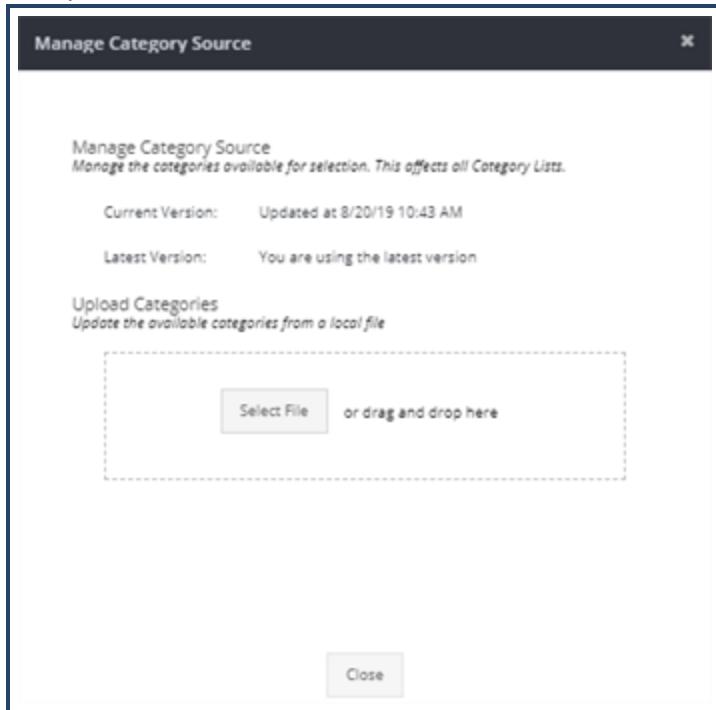
1. Select **Policy > Shared Objects**.
2. Edit an existing category list or category list template, or create a new category object. See "Create Category Lists" on page 363 and "Use Category List Templates" on page 374 for more information.
3. Click the **Manage Category Source** icon.



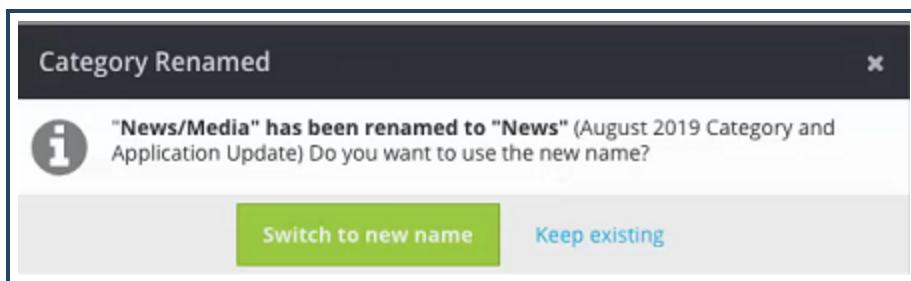
The system displays the **Manage Category Source** dialog. If an update is available, the Latest Version section displays "**An update is available. Download Now.**"

4. To update the categories, select the **Download Now** link. If you are in an offline network, retrieve the `categories.xml` file from the Management Center download site at mysymantec and drag and drop it into the dialog (2.3.2.1 and

later).



5. If any of the existing categories were out-of-date, the system notifies you of each change and prompts you to accept the changes.



Note: If you choose to keep an existing category, the system displays the category as **Unrecognized** because the metadata for that category no longer exists.

6. If managed Reporter devices update their category lists, you must examine your saved reports to identify any out-of-date categories. For example, Reporter 10.4.1.1 includes new categories and you must complete this action or your saved reports will not work after the Reporter upgrade.

To do this, open the report, identify any disparities, and update the filter with the new name(s). See "Customize Reporter Report Options" on page 722 for more information about adding report filters.

Note: For more information about content filtering by category, refer to the SGOS Administration Guide.

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:

```
; 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.

Note: 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**.

The screenshot shows the 'Create New Shared Object: Basic Information' dialog. It has two tabs at the top: 'Basic Information' (which is selected) and 'Attributes'. The 'Basic Information' section contains the following fields:

- Object name:** Whitelist (with an asterisk indicating it is mandatory)
- Object type:** Category (with an asterisk indicating it is mandatory)
- Reference ID:** Whitelist (with an asterisk indicating it is mandatory)
- Description:** (Empty text area)

A note at the bottom of the dialog says "1024 of 1024 characters left".

- c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.

Note: 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 584.
5. Click **Finish**. The new category displays in the editor.

Step 2 - Add URLs

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired category. The system displays the category editor.

3. Enter the URL in the URL field and click Add.

The screenshot shows the 'Editor' tab selected in the top navigation bar. Below it are buttons for 'Save', 'Discard', 'Compare', and 'Import'. On the right is a gear icon. The main area has two input fields: 'URL:' and 'Description:', separated by a vertical line. To the right of each field is a 'Save' button. Below these is a large 'Add' button.

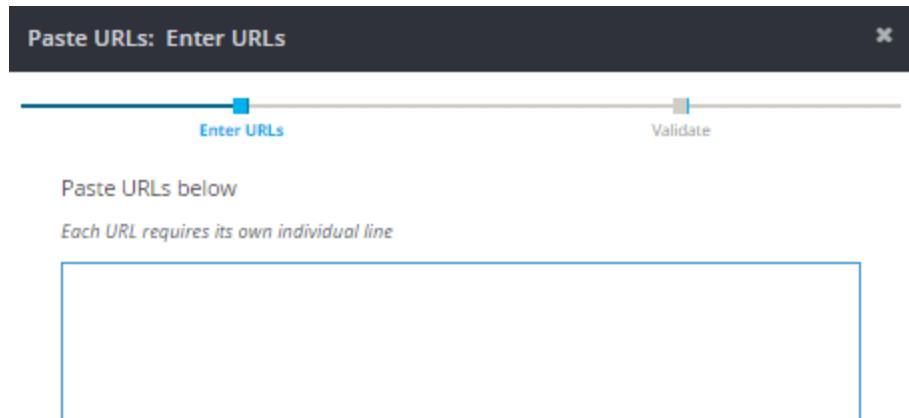
Note: The system displays the text entered into the **Description** field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:

- Create a category and copy the URLs.
- Click Paste URLs.**

The screenshot shows the 'Editor' tab selected. Below it are buttons for 'Save', 'Discard', 'Compare', and 'Import'. On the right is a gear icon. The main area has 'URL:' and 'Description:' fields with 'Save' buttons. At the bottom are buttons for 'Edit', 'Delete', 'Enable', 'Disable', 'Paste URLs', 'Keyword Search', and a magnifying glass icon.

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.

<input type="checkbox"/> Enabled	URL	Description
<input type="checkbox"/>	cnn.com	Added on 1/05/2017
<input checked="" type="checkbox"/>	yahoo.com	f
<input type="checkbox"/>	nytimes.com	

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 355. 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 451.

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 "Web Auth">
  authenticate(corp_realm)

<proxy "Web Filter">
  url.domain=playboy.com FORCE_DENY
  category=(gambling, hacking, games, news) exception(content_filter_denied)

<proxy "Restricted Access">
  group=execs, managers url.domain=fantasyfootball.com ALLOW
```

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.

	Enabled	URL	Description
<input type="checkbox"/>	✓	cnn.com	Added on 1/05/2017
<input type="checkbox"/>	✓	yahoo.com	f
<input type="checkbox"/>	✓	nytimes.com	

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
  
```

Note: The name of the category 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**.

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.

Note: 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**.

The screenshot shows the 'Create New Policy: Basic Information' wizard. The title bar says 'Create New Policy: Basic Information'. Below it is a progress bar with 'Basic Information' highlighted in blue and 'Attributes' to its right. The main area is titled 'Basic Information'. It contains four input fields:

- 'Policy name': A text input field containing 'Example_Local_Database' with a yellow asterisk icon indicating it is required.
- 'Policy type': A dropdown menu set to 'Local Database' with a yellow asterisk icon.
- 'Reference ID': A text input field containing 'Local_Database'.
- 'Description': A large text area with a placeholder '1024 of 1024 characters left' at the bottom.

- c. **Reference ID (*)** - Enter a Reference ID that you can filter for when building policy.

Note: 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 584 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.



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 supports importing of local database categories included in text files with an **.ldb** extension. For more information, see "Create a Local Database File" on page 397. If you have previously created a local database file, you can import it into your new database by clicking **Import**.

Note: Management Center can also 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 **Import**. For more information on exporting policy objects, see "Export Policy or Shared Objects to Local Disk" on page 491.

Note: 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.

The screenshot shows the Management Center interface for a 'Shared_Local_Database'. The navigation path is 'Policies > Shared_Local_Database'. The main title is 'Local Database: Shared_Local_Database'. Below the title, there are tabs: 'Editor' (disabled), 'Versions' (selected and highlighted in green), 'Attributes', and 'Info'. Under the 'Versions' tab, there is a 'Version Control' section with buttons for 'Compare', 'View', 'Restore', and a refresh icon. A table lists the database's history:

Version ↓	Author	Date	Comments
1.2	admin	8/28/17 2:24 PM	Added an entry to allowed category.
1.1	admin	8/28/17 2:24 PM	Initial database
1.0	admin	8/28/17 2:20 PM	Initial revision

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.

Compare Policy			
	Revision 1.2		Revision 1.4
1	define category Allowed	1	define category Allowed
1	google.com		
3	usa.gov	2	usa.gov
3	test.com		
5	symantec.com	3	symantec.com
		3	mycompany.com
		4	example.com
		5	test.net
6	end	7	end

Step 3 - Deploy the Local Database

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.

The screenshot shows a web-based management interface for a local database. At the top, there's a header with a back arrow and the title "Local Database: Shared_Local_Database". Below the header is a navigation bar with four tabs: "Editor", "Versions", "Attributes", and "Info", with "Info" being the active tab. The main content area has a section titled "General Information". Under "Identifier", it shows a "Unique Id" of "79C54BD1-1BD1-450E-9E74-91D668241FAB". Below this, there's a "Direct URL" field containing the value "https://MC_IP:8082/direct/policy/F5kdjR6lt". To the right of this field are two small icons: a circular arrow for refresh and a clipboard for copy.

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.

Local Database URL Protocol Note

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/F5kdjR6lt**

Note: If you enable HTTP after using HTTPS, you must delete the HTTPS cookie from your browser to be able to use the HTTP connection for the UI.

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.**

The screenshot shows the 'Edit Host Categorization Database Settings' dialog box. The provider is set to 'Local'. The URL field contains 'https://MC_IP:8082/direct/policy/F5kdJR6lt'. The 'Update Interval (minutes)' field is set to 120. There are fields for Username, Password, Confirm Password, Proxy Host, Proxy Port, Proxy Username, Proxy Password, and Confirm Proxy Password. A note at the bottom says 'Leave password fields blank if you do not wish to change the passwords.' At the bottom right are 'OK' and 'Cancel' buttons.

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.

Note: If your SSL Visibility appliance does not have the HTTPS certificate in its PKI stores, refer to the **Local Database URL Protocol Note** above.

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.

Tip: For more information on writing configuration scripts, see "Create and Distribute Configurations Using Scripts" on page 246.

Create a Local Database File

Management Center supports importing of local database categories included in text files with an **.ldb** extension. To create the local database file, open a text file and save it with your preferred name and then change the extension **.ldb**.

Example 1

1. Open a text file and save it as **example1**.
2. Change the file extension to **.ldb**.

The file should now be named **example1.ldb**.

3. Add the following:

```
define category TestLocalPolicy1
www.facebook.com ;test facebook
www.linkedin.com ;test linkedIn
```

```

end
define category TestLocalPolicy2
www.stackoverflow.com ;test stackoverflow
end

```

4. Save the file again.

These entries create a local database policy with two categories named `TestLocalPolicy1`, and `TestLocalPolicy2`. Notice that comments need to have an empty space and ";" after the URL.

Example 2

1. Open a text file and save it as `testPolicy2`.
2. Change the file extension to `.ldb`.

The file should now be named `testPolicy2.ldb`.

3. Add the following:

```

define category HTTP_whitelist
symantec.com ;here's a comment
www.geeksforgeeks.org
www.linkedin.com
end
define category FTP_whitelist
facebook.com ;here's another comment
linkedin.com
end

```

4. Save the file again.

After creating a local database file, you can import it into Management Center as described in "Create a Local Content Filter Database " on page 388.

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**.

The screenshot shows the 'Create New Shared Object: Basic Information' dialog box. At the top, there are tabs for 'Basic Information' (which is selected) and 'Attributes'. Below the tabs, the 'Basic Information' section is displayed. It includes four input fields: 'Object name' with a value of 'IP_List', 'Object type' set to 'IP Address List', 'Reference ID' with a value of 'IP_List', and a large 'Description' field which is currently empty. A note at the bottom of the description field area says '1024 of 1024 characters left'.

- c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.

Note: 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 584.
5. Click **Finish**. The new list displays in the editor.

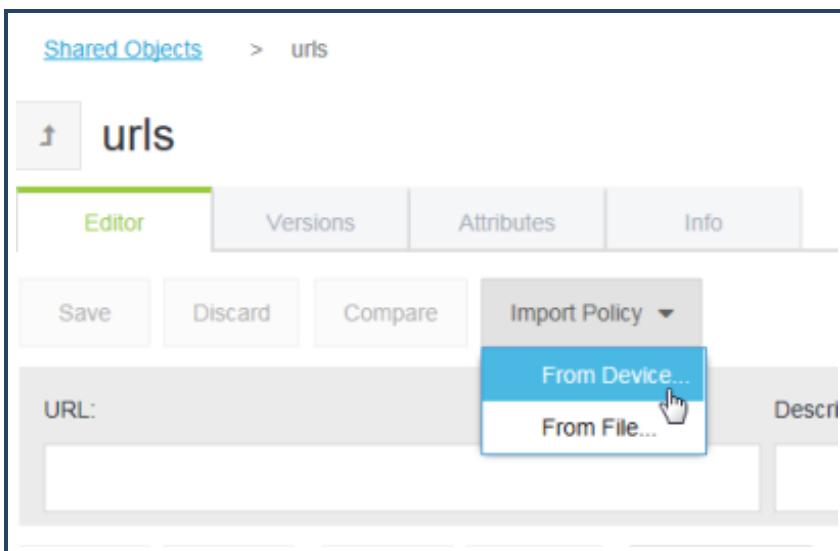
Step 2 - Add URLs or IP addresses to the List (Optional)

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).

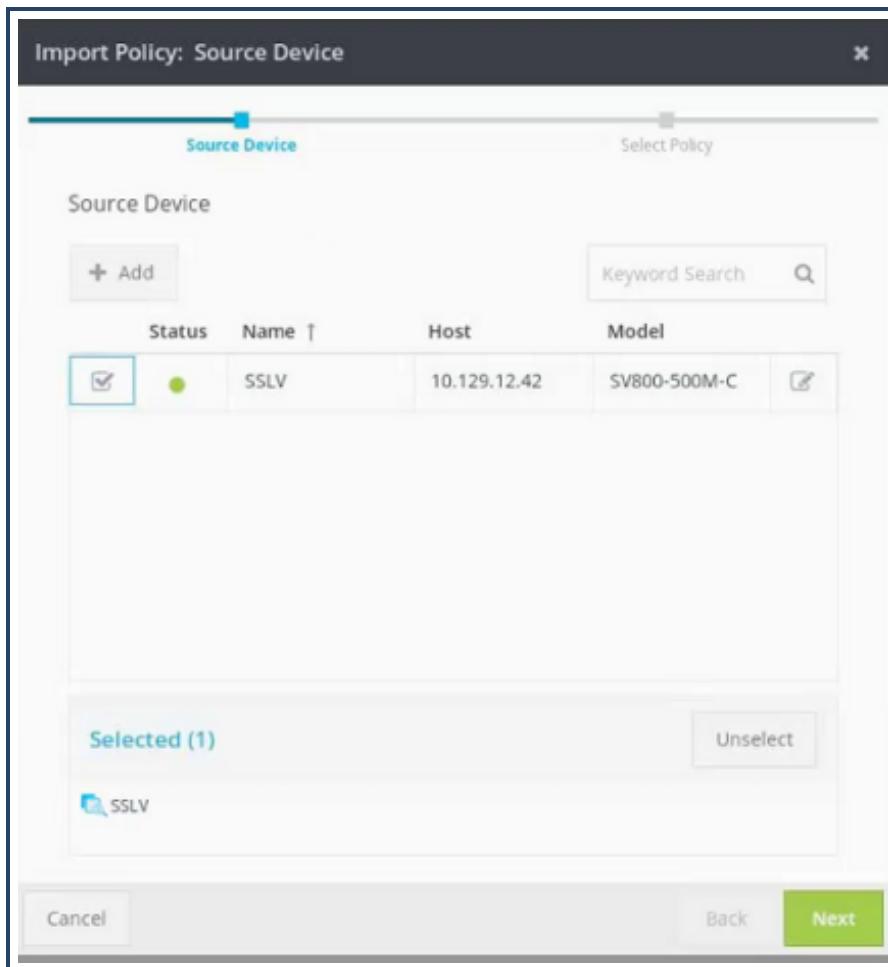
Step 3 - Import URLs or IP addresses from an SSL Visibility Appliance

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).

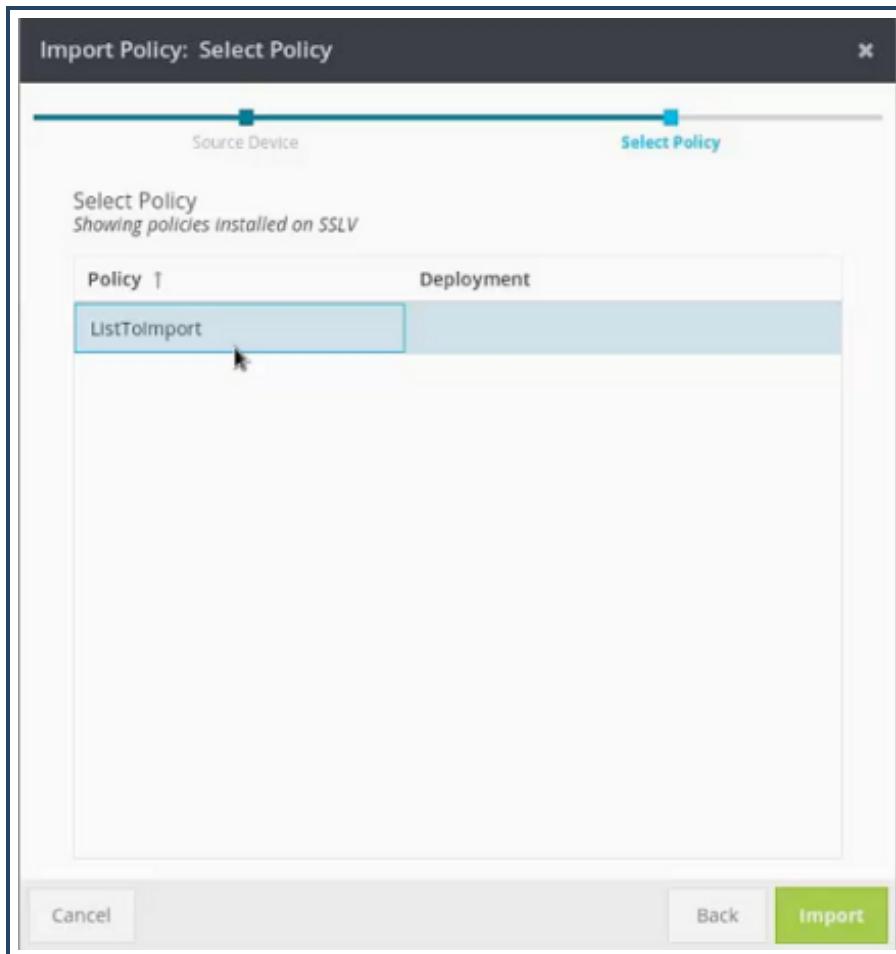
1. Select **Configuration > Shared Objects**.
2. **Select the URL or IP address list you created in Step 1.**



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.

The screenshot shows the 'Create New Policy: Basic Information' wizard step. The form has tabs for 'Basic Information' and 'Attributes'. The 'Basic Information' tab is selected. It contains the following fields:

- Policy name:** (marked with a yellow asterisk)
- Policy type:** (marked with a yellow asterisk)
- Reference ID:**
- Description:**
1003 of 1024 characters left

A checkbox labeled 'Replace substitution variables' is also present. At the bottom, there are buttons for 'Cancel', 'Back', and 'Next' (highlighted in green).

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.

The screenshot shows the 'URL Lists' window. At the top, there is a header bar with the title 'URL Lists' and a close button. Below the header is a toolbar with a '+ Add' button and a 'Keyword Search' input field. The main area is a table with columns: 'Name ↑', 'Type', and 'Description'. There are six rows in the table:

	Name ↑	Type	Description	
<input type="checkbox"/>	IP List	IP Address List		<input type="button" value="Edit"/>
<input type="checkbox"/>	IP_List	IP Address List		<input type="button" value="Edit"/>
<input type="checkbox"/>	New Whitelist	URL List		<input type="button" value="Edit"/>
<input checked="" type="checkbox"/>	test	URL List		<input type="button" value="Edit"/>
<input type="checkbox"/>	urls	URL List		<input type="button" value="Edit"/>
<input type="checkbox"/>	URL_whitelist	URL List		<input type="button" value="Edit"/>

Below the table is a section titled 'Selected (1)' containing a list with one item: 'test'. To the right of this section is a 'Unselect' button. At the bottom of the window, there is a 'Subject/List Name on SSLV:' field with a required asterisk (*) and the value 'test'. Finally, at the very bottom are 'OK' and 'Cancel' buttons.

2. Select the check box next to the list you want to include in the policy.

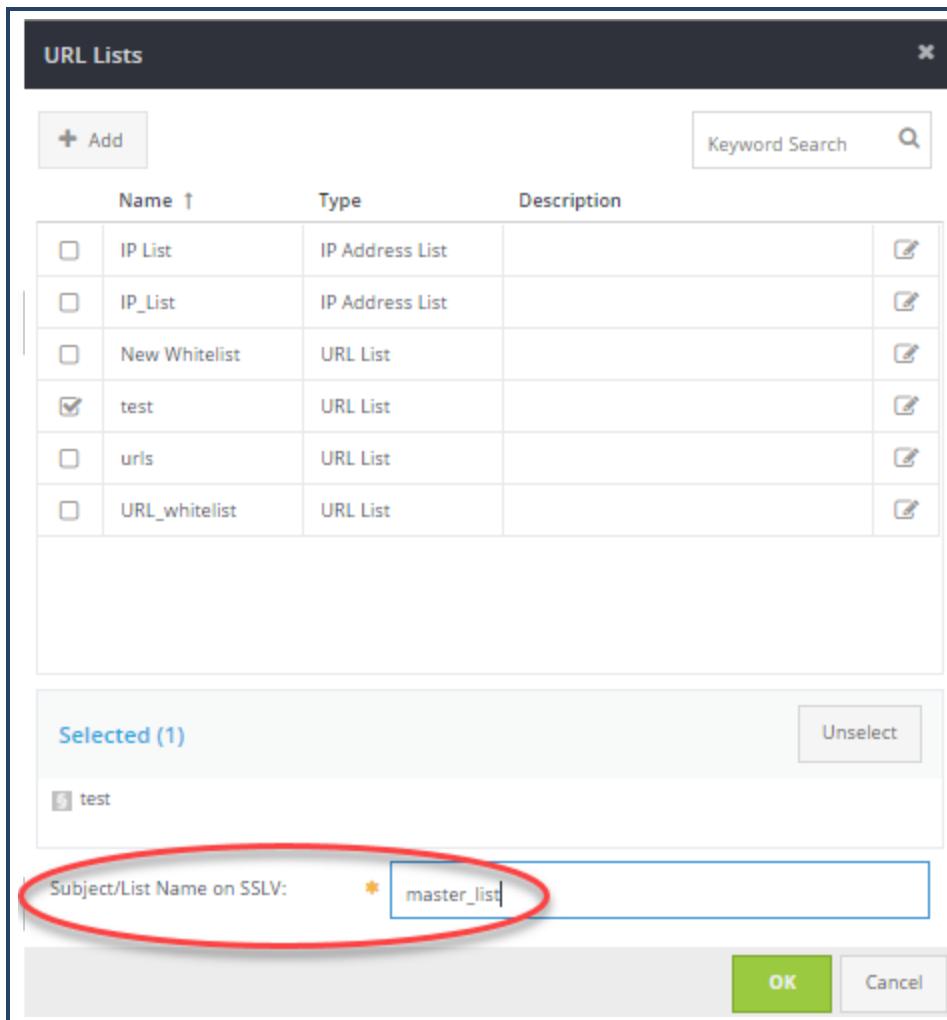
3. Click **OK**. The list(s) are shown in the policy.
4. Click **Save**.

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**.

Note: 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.

New Job: Operation

Basic Info **Operation** Targets Schedule

Single Job Multistep Job

Operation: * Install Policy

Select Policies to Install

Policies: * SSLV Policy

Force Installation

Force installation (don't abort the job on [installation warnings](#))

Cancel Back **Next**

Troubleshooting SSLV List Execution

If an SSLV List policy contains a shared object that has been deleted, policy execution will fail. To help you identify the problem before executing the policy, the system displays **Error: List not found** in the policy list.

List Name	Type	Reference ID	Subject/List Name on ...	Version Used
Error: List not found			IP_List1	Latest Version
URL List	URL List	URL_List	URL_List	Latest Version

If the SSLV list policy that contains a deleted shared object is executed, the system returns a specific error stating that one or more lists could not be found. You must remove all missing lists before successfully executing the policy.

Create SSL Visibility URL List Policy

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.

Create New Shared Object: Basic Information

Basic Information Attributes

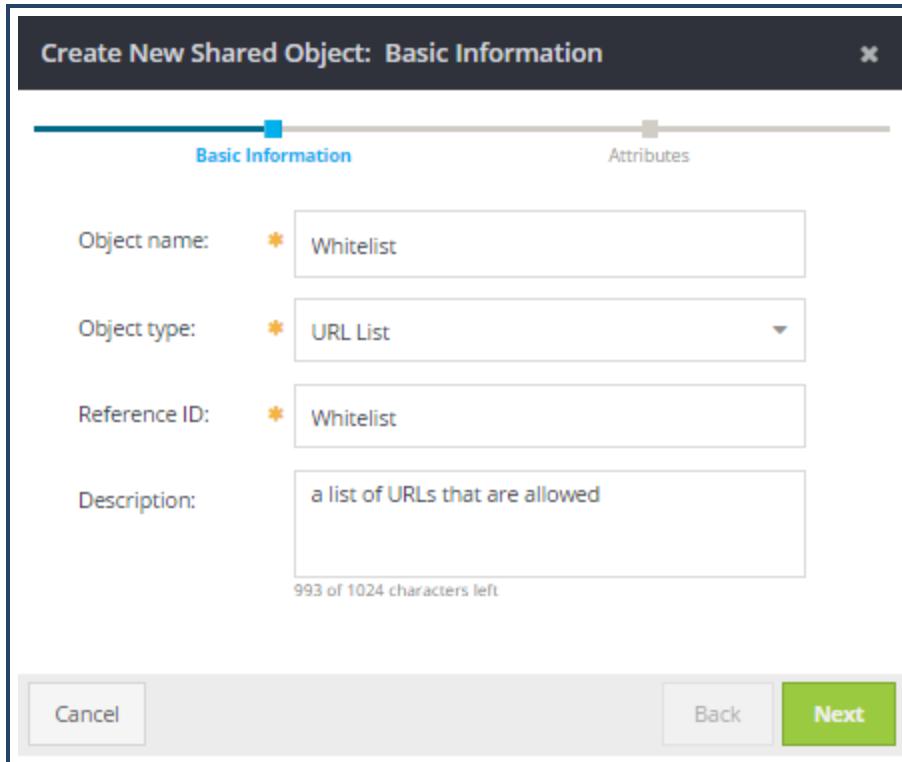
Object name: * Whitelist

Object type: * URL List

Reference ID: * Whitelist

Description: a list of URLs that are allowed
993 of 1024 characters left

Cancel Back Next



- c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.

Note: 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 584.
5. Click **Finish**. The URL list displays in the editor.

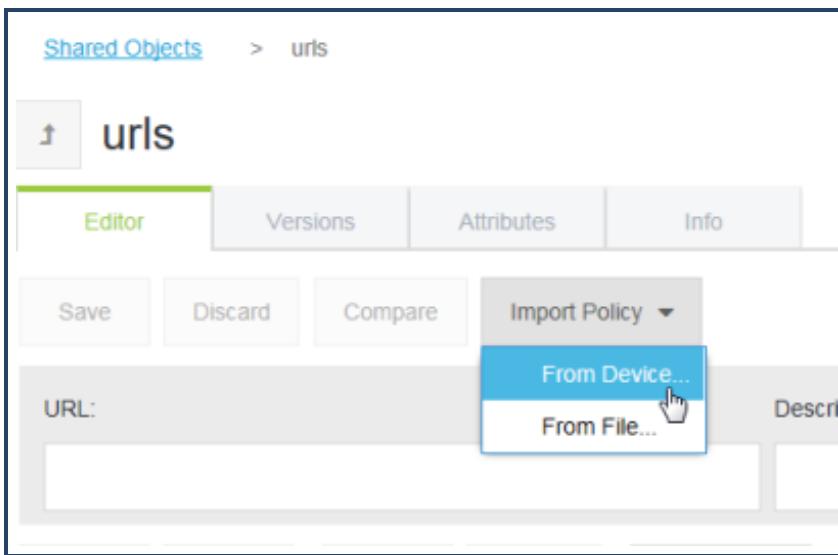
Step 2 - Add URLs to the List (Optional)

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).

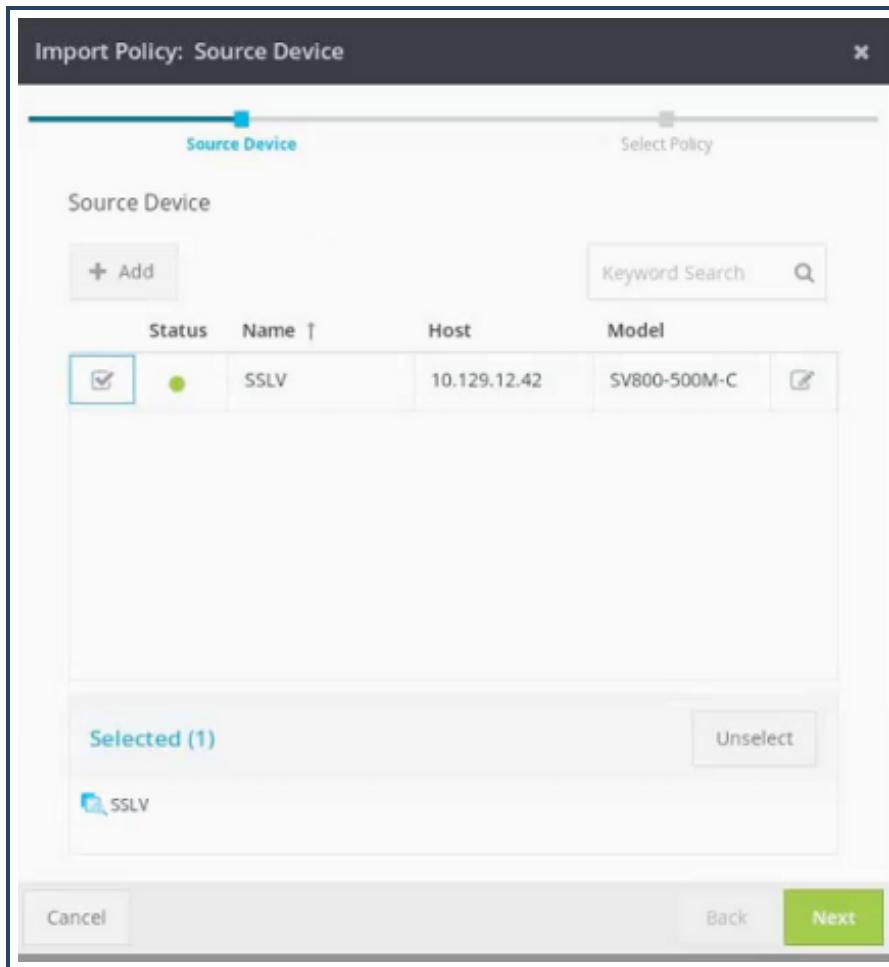
Step 3 - Import URLs from an SSL Visibility Appliance

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).

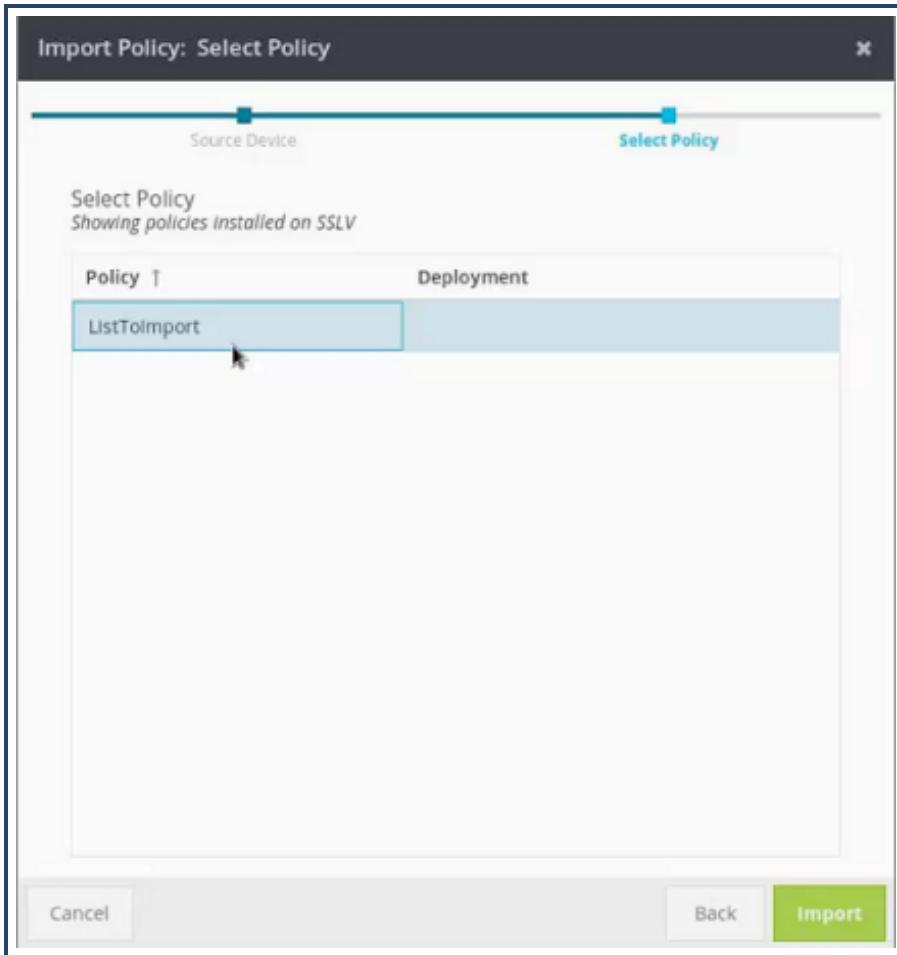
1. Select **Configuration > Shared Objects**.
2. **Select the URL list you created in Step 1.**



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.**

Create New Policy: Basic Information

Basic Information

Policy name: **SSLV Policy**

Policy type: **SSLV Lists**

Reference ID: **SSLV_Policy**

Description: **policy for SSLV lists**
1003 of 1024 characters left

Replace substitution variables

Cancel **Back** **Next**

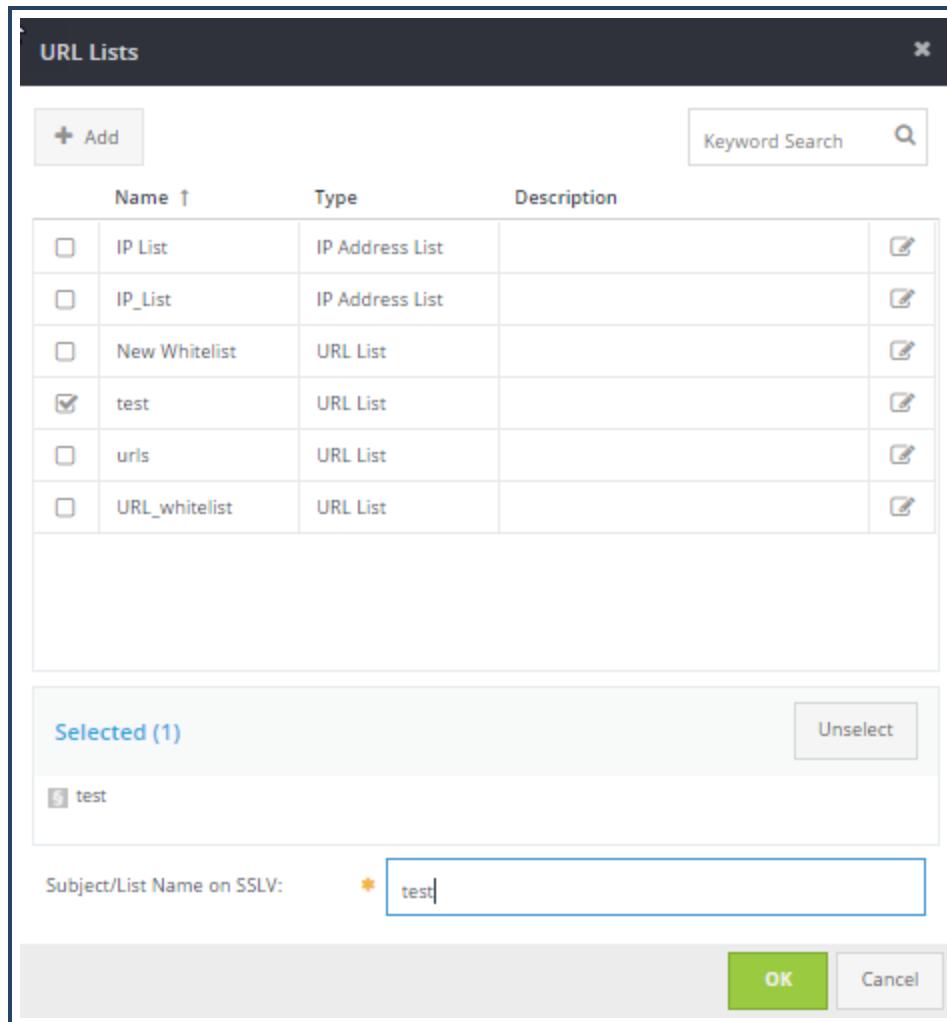
3. **Policy name:** Enter a descriptive name for the policy.
4. **Policy type:** Choose **SSLV Lists** from the drop-down.
5. **Reference ID:** This is supplied automatically, based on the policy name (spaces are replaced with underscores).
6. (Optional) **Description:** Enter a description up to 1024 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.**



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.

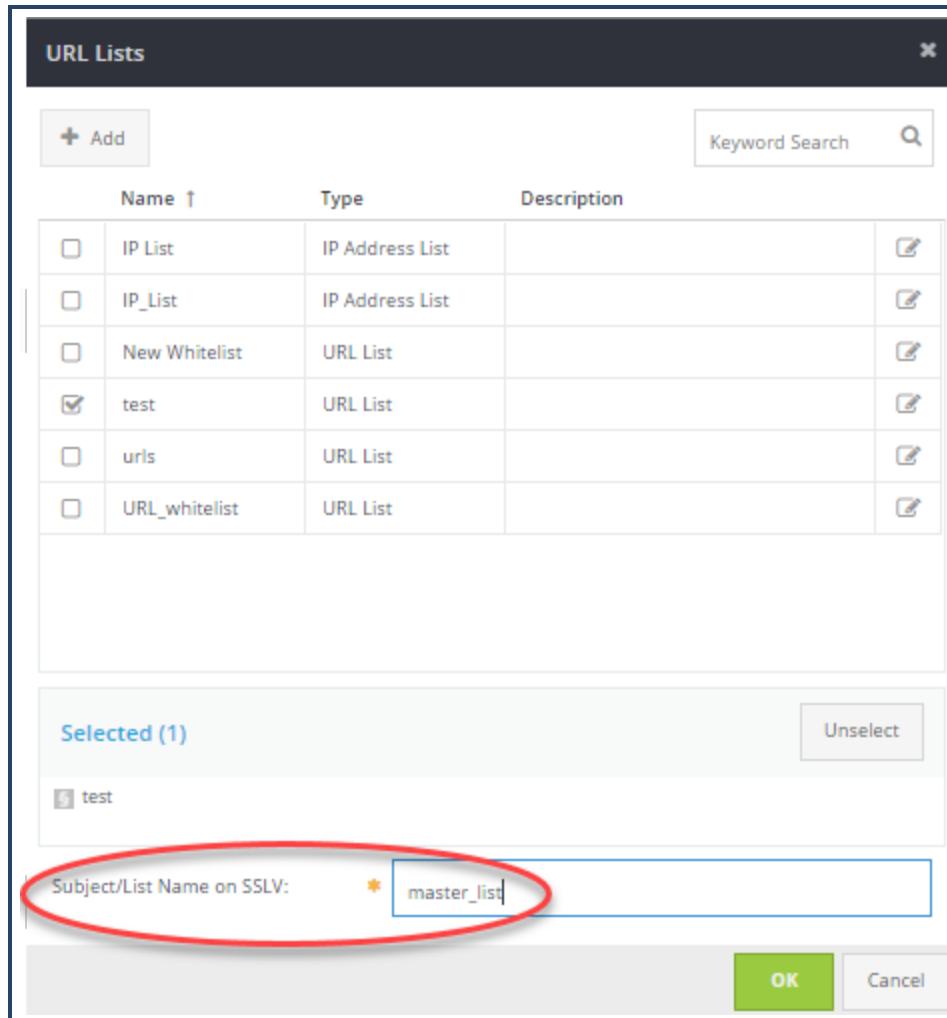
Step 6 - Mapping Management Center URL Lists to SSL Visibility URL Lists

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**.

Note: 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.

New Job: Operation

Basic Info Operation Targets Schedule

Single Job Multistep Job

Operation: * Install Policy

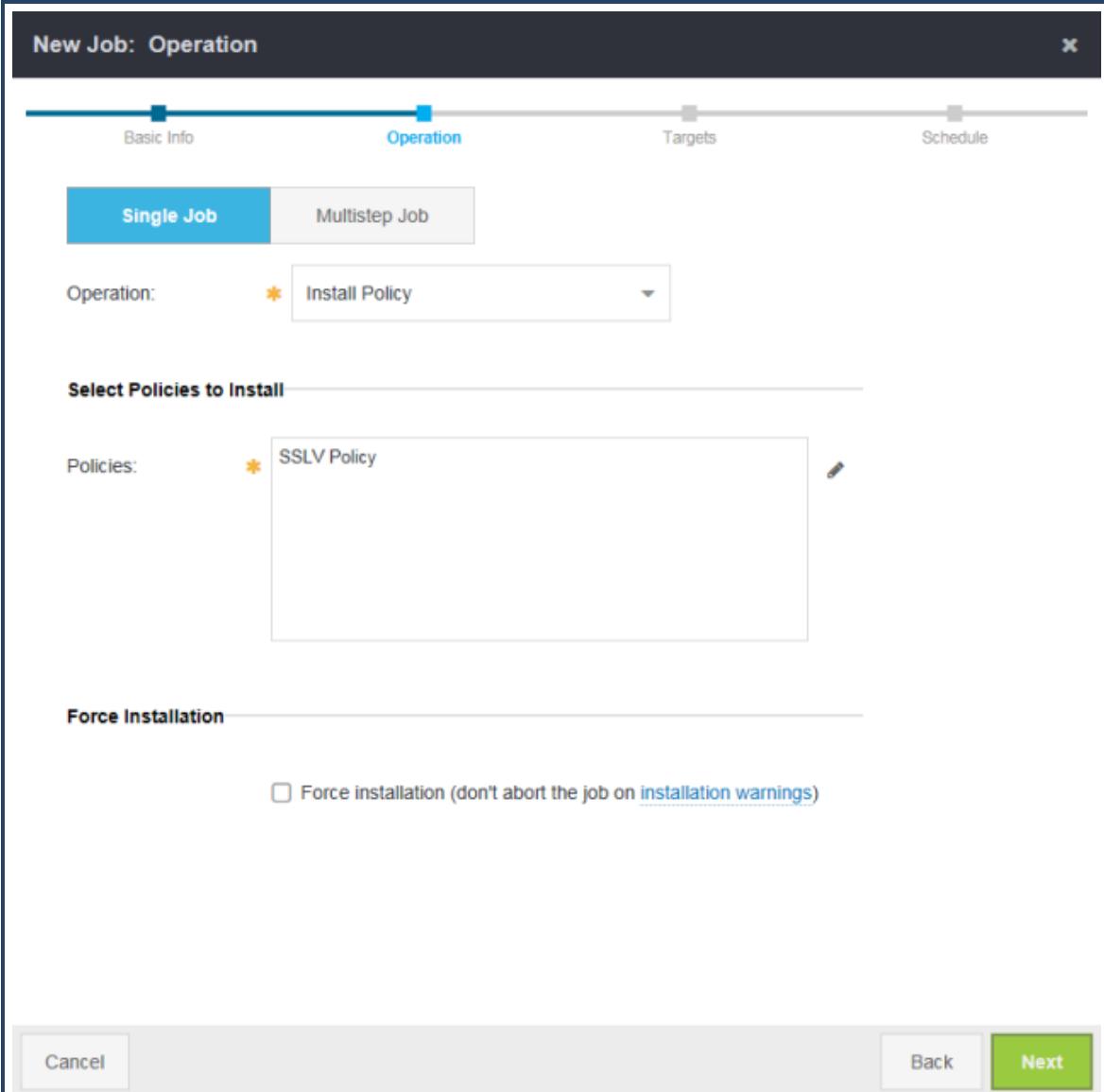
Select Policies to Install

Policies: * SSLV Policy

Force Installation

Force installation (don't abort the job on [installation warnings](#))

Cancel Back Next



Troubleshooting SSLV List Execution

If an SSLV List policy contains a shared object that has been deleted, policy execution will fail. To help you identify the problem before executing the policy, the system displays **Error: List not found** in the policy list.

List Name	Type	Reference ID	Subject/List Name on ...	Version Used
Error: List not found			IP_List1	Latest Version
URL List	URL List	URL_List	URL_List	Latest Version

If the SSLV list policy that contains a deleted shared object is executed, the system returns a specific error stating that one or more lists could not be found. You must remove all missing lists before successfully executing the policy.

Create IP Address List

Using this feature, you can create IP address lists for use on the SSL Visibility appliance, Blue Coat ProxySG appliance, or Advanced Secure Gateway (ASG). IP address lists are [shared objects](#), and are similar to [URL lists](#).

Note: 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**.

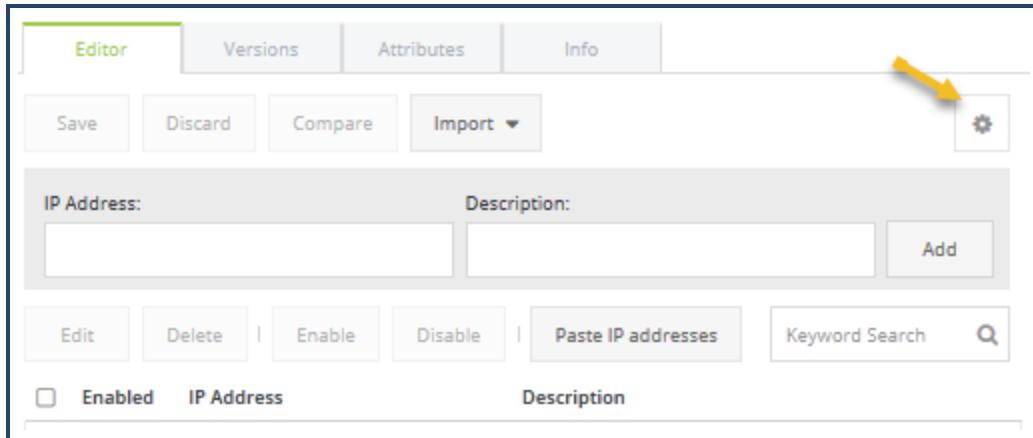
The screenshot shows the 'Create New Shared Object: Basic Information' dialog. At the top, there are two tabs: 'Basic Information' (which is selected) and 'Attributes'. Below the tabs, the 'Basic Information' section contains four fields:

- Object name:** IP_List (with an asterisk indicating it is required)
- Object type:** IP Address List (with an asterisk indicating it is required)
- Reference ID:** IP_List (with an asterisk indicating it is required)
- Description:** A large text area with a character count indicator '1024 of 1024 characters left'.

- c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.
- Note:** The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
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 584.
5. Click **Finish**. The new IP address list displays in the editor.

Step 2 - ProxySG and ASG Only: Configure CPL Settings

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired IP address list. The system displays the IP address list editor.
3. Click the gear box. Show screen.



4. In IP List - Advanced Settings, select the appropriate CPL trigger and click save.

CPL Generation
Customize how the policy is generated for ProxySG and ASG. These options do not affect SSLV devices

Triggers:

- Use client.address trigger
- Use client.effective_address trigger
- Use url.address trigger
- Use server_url.address trigger

The triggers allow you to add an IP address list object as either a source or destination object:

- Source Object Triggers:
 - **client.address**
 - **client.effective_address**

- Destination Object Triggers:
 - url.address
 - url.server_address

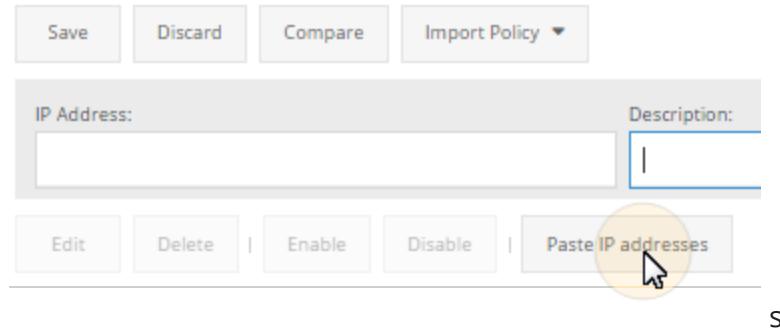
Refer to the [Content Policy Language Reference](#) for more information about these triggers.

Step 3 - 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.**

Note: The system displays the text entered into the Description field as a comment in the generated policy.

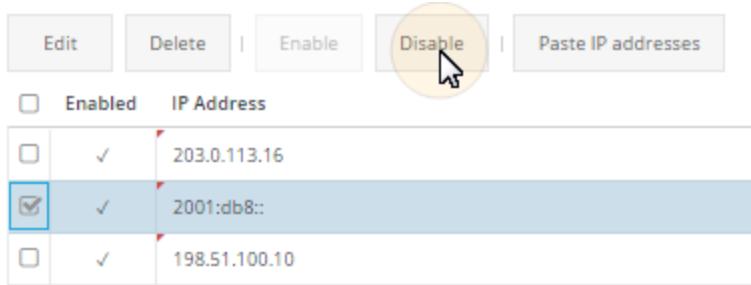
4. Alternatively, paste in multiple IP addresses:
 - a. Create an IP address list and copy it in.
 - b. **Click Paste IP addresses. The system opens the Paste IP addresses: Paste IP addresses dialog.**



- 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.



You can enable an IP address by selecting it and clicking **Enable**.

Step 4 - Include the IP Address List in Policy

SSL Visibility

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 398.

You can then install your policy as described in "Install Policy" on page 451.

ProxySG

When you have completed your changes, you can include the IP address list in your ProxySG or ASG VPM or CPL policy object, as described in "Include a Shared Policy Object in CPL or VPM Policy" on page 355.

Note: See "Add a VPM Policy Object" on page 323 and "Create a CPL Policy Object" on page 295 for information.

You can then install your policy as described in "Install Policy" on page 451.

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 "View and Edit Device Information" on page 69.
4. Create administrator roles with different sets of permissions. After you "Define Roles " on page 567 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 499 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 166).
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 572.
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 facing page for instructions.
9. Create tenant policy in VPM ("Create a VPM Tenant Policy Object" on page 431 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 477.

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.

Note: The Management Center WAF interface leverages option #2 to control tenancy determination via the Tenant Determination object. See "About WAF Policy" on page 202 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 199. 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

Management Center Configuration & Management

1. Select Configuration > Tenants.

The screenshot shows the Symantec Management Center interface. On the left, there's a vertical sidebar with icons for Home, Configuration, Policy, Scripts, Shared Objects, Tenants, and Files. The 'Tenants' icon is highlighted with a blue box and has a blue arrow pointing to it from the left. The main area is titled 'CONFIGURATION Device Policies and Configuration'. It features a large circular gauge with the number '7' in the center, labeled 'Total Devices'. Below the gauge are buttons for 'Add Widgets', 'Options', and a refresh icon.

2. Click Add Tenant.

The screenshot shows the 'Tenants' list page. At the top, there's a header with the word 'Tenants'. Below it is a row of buttons: '+ Add Tenant' (which is highlighted with a yellow circle and has a cursor arrow pointing to it), 'Edit', and 'Delete'. Below these buttons is a search bar with the placeholder 'Display Name ↑' and 'Tenant ID'.

The web console displays the Add Tenant dialog.

Add Tenant

Display Name: * Outlook_Lab3

Tenant ID: * OutLa3

Description: Test environment
1008 of 1024 characters left

Save **Cancel**

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.**

Management Center Configuration & Management

Tenants	
Add Tenant Edit Delete Sync	
Display Name ↑	Tenant ID
Default	default
Outlook_Lab3	OutLa3
Sharepoint	Sharepoint
WAF App	WAFApp

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	
Add Tenant Edit Delete Sync	
Display Name ↑	Tenant ID
Default	default
Outlook_Lab3	OutLa3
Sharepoint	Sharepoint
WAF App	WAFApp

4. Select **Yes** to delete the selected tenants.

Caution: 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.

Note: 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.

Note: 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 312 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.

What do you want to accomplish?	Refer to
Add policy.	"Launch Legacy Visual Policy Manager (Java)" on page 321
Import policy.	"Launch Legacy Visual Policy Manager (Java)" on page 321
Learn about deploying multi-tenancy policy on ProxySG appliances.	<i>Multi-Tenant Policy Deployment Guide</i>
Create and manage tenants from Management Center.	"Manage Tenants" on page 426
View policies deployed to each slot on a device.	"View Deployed Policy for each Device Slot" on page 477

Import VPM Tenant Policy from Source Device

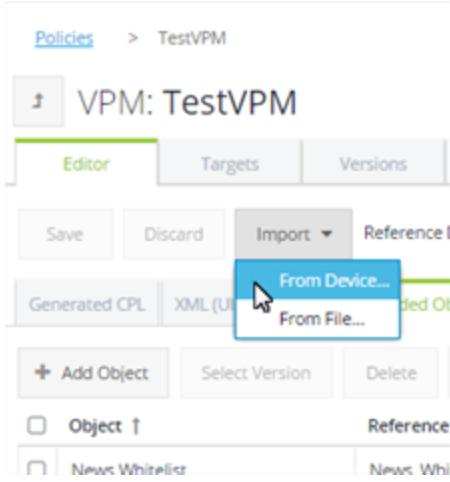
A *VPM Tenant policy object* can be used to define the policy used in a tenant slot. After creating the VPM Tenant (as described in "Create a VPM Tenant Policy Object" on the previous page), you must add policy to it. You can add policy by the [legacy](#) or [web-based](#) VPM or by importing existing 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.

Note: To write tenant policy in CPL, see [Create the Content Policy Language](#).

Management Center Configuration & Management

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.**

Import Policy: Source Device

Source Device Select Policy

+ Add Keyword Search

Status	Name ↑	Host	Model	
<input type="checkbox"/>	●	10.169.2.228 - B...	10.169.2.228	300-25 <input type="button" value="Edit"/>
<input type="checkbox"/>	●	10.169.25.102 - ...	10.169.25.102	V100 <input type="button" value="Edit"/>
<input type="checkbox"/>	●	10.9.43.225 - Bl...	10.9.43.225	300-25 <input type="button" value="Edit"/>

Selected (0) Unselect

Cancel Back Next

5. Click Import.

Import Policy: Select Policy

Source Device Select Policy

Policy ↑	Deployment
VPM policy	<input type="checkbox"/> V <input type="checkbox"/> L <input type="checkbox"/> C <input type="checkbox"/> F VPM

Cancel Back Import

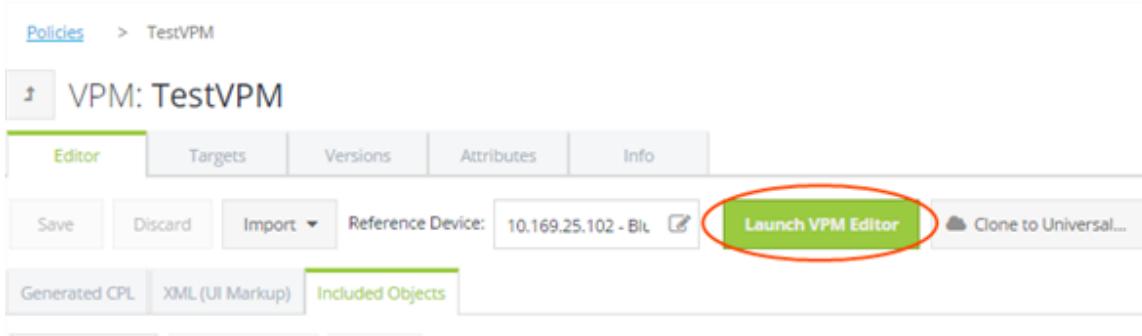
Management Center Configuration & Management

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.

What do you want to accomplish?	Refer to
Learn about deploying multi-tenancy policy on ProxySG appliances.	Multi-Tenant Policy Deployment Guide
Create and manage tenants from Management Center.	"Manage Tenants" on page 426
View policies deployed to each slot on a device.	"View Deployed Policy for each Device Slot" on page 477

Schedule Removal of Unused Tenant Policy

You can delete unused policy from a tenant slot. Management Center considers policy in a tenant slot to be unused if policy is installed on the appliance but does not exist in the tenant

slot in Management Center, regardless of whether or not the policy was created or deployed through Management Center. Consider the following examples:

- If you create tenant policy in Management Center, deploy it to an appliance, and then remove it from Management Center, it is considered to be unused.
- If you create tenant policy on the appliance without importing it to Management Center, it is considered to be unused.

Note: This operation is not supported in Multistep Device Jobs.

Note: See also "Remove Unused Tenant Policy" on page 100.

1. Select **Jobs > Add > New Job**.

2. On the **Add New Job** page, select **Remove Unused Policy**.

3. **Configuration:**

- To remove all unused tenant policy, skip to step 2 **Targets**. To exclude some tenant IDs, click the + and enter those tenant IDs.

The tenant ID is 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. Go to **Configuration > Tenants** to view the existing tenant IDs.

4. **Targets::**

- Select the **Devices** or **Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

5. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. **Name:**

- Verify or change the name and add an optional description.

8. Click **Save**.

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.

For more information about how UPE integrates with WSS, refer to the [**Universal Policy Enforcement WebGuide**](#).

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

Appliance	Version
ProxySG appliance	6.7.1.1 or later; 6.5.9.14 or later (6.6.x is not supported at this time)
Web Security Service	6.9.5.1 or later
Management Center	1.8.1.1 or later (1.10.1.1 or later for CPL universal policy)

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](#).

Note: 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.

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

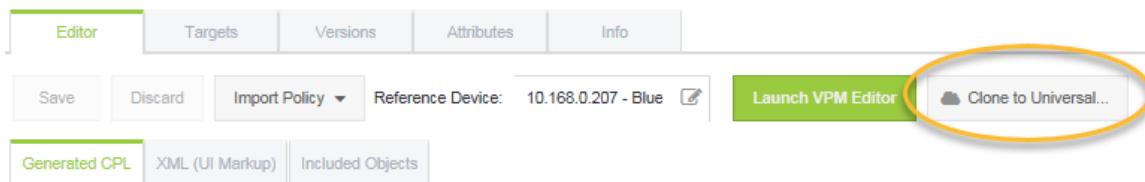
6. Enter a description in the **Description** field. Although entering a description is not required, the description helps differentiate versions of the same policy.
7. Indicate whether to **Replace Substitution Variables**. See "Use Substitution Variables in Policies and Scripts" on page 312 for more information.
8. Click **Next**.
9. Enter or select values for the defined attributes.
10. Click **Finish**.

Management Center Configuration & Management

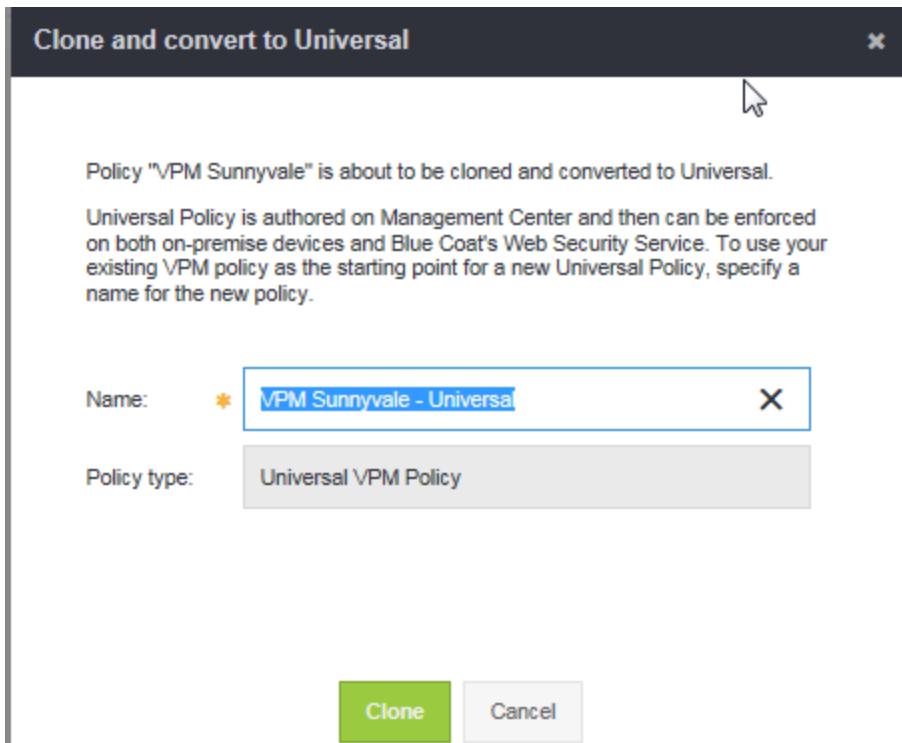
Transform Existing VPM Policy into Universal VPM Policy

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. Then, use the VPM to edit and finalize your policy.

Legacy VPM Requirements

- When using the legacy 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 and wish to use the Java-based VPM editor from within Management Center, you will need to upgrade the ProxySG to an SGOS version where this issue is addressed. Depending on the branch of SGOS running on your ProxySG appliances, load the appropriate version to support Management Center:

- SGOS 6.5.x: 6.5.9.10 or later
- SGOS 6.6.x: 6.6.4.1 or later
- SGOS 6.7.x: 6.7.2.1 or later

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.

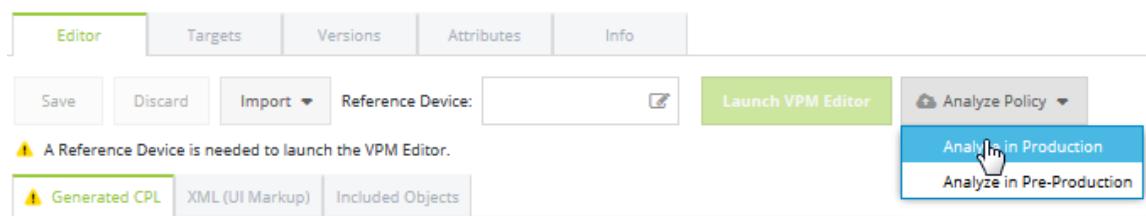
Note: If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command. See `# security` for more information.

Management Center Configuration & Management

- 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, 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>

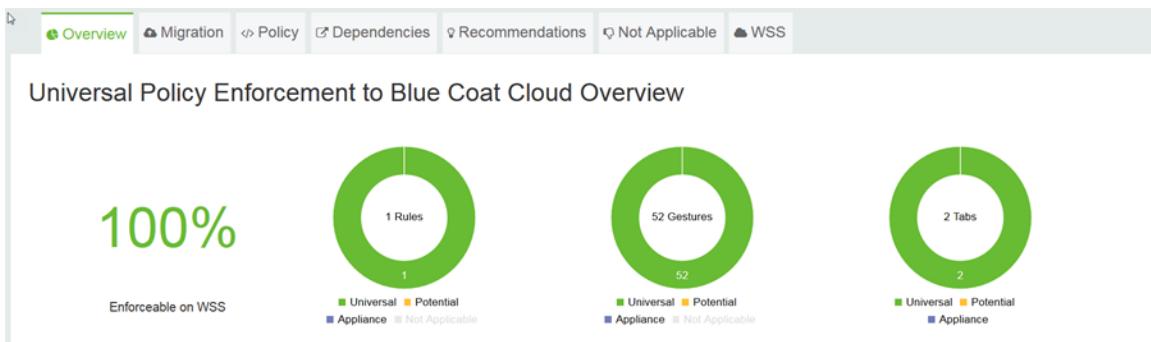
Procedure

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 256.
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 325.
4. **Click Analyze Policy > Analyze in Production to open the policy classifier.**



Note: 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.



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.
- The **WSS** tab provides general information about the WSS.

Use this information to inform your policy edits.

6. Open the or [web-based](#) VPM:

- a. Navigate back to the policy editing page and click **Launch VPM Editor**.
- b. The web console displays the Visual Policy Manager.

7. Keeping both the classifier and VPM open, edit your policy rules.

Note: 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.

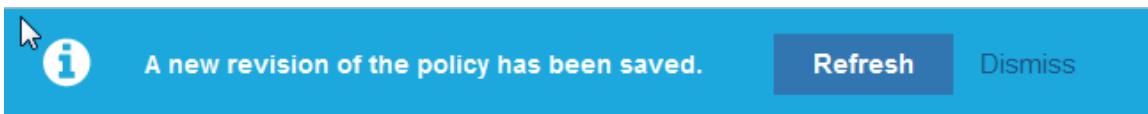
For each rule, specify whether it should apply only to appliances (Appliance), both appliances and the WSS (Universal), or the WSS only.

Management Center Configuration & Management

No.	Source	Destination	Service	Time	Action	Track	Enforcement	Comm
1	Authenticat...	Any	Using HTT...	Any	Allow Acce...	None	Universal	
2	Any	Destinatio...	Any	Any	Deny	None	WSS	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">Appliance Universal WSS (selected) Copy Paste</div>

Note: 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.**



Note: You might notice blank lines in the classifier. Appliance-only rules are blanked out before sending to the WSS. The rules are replaced with blank lines.

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.

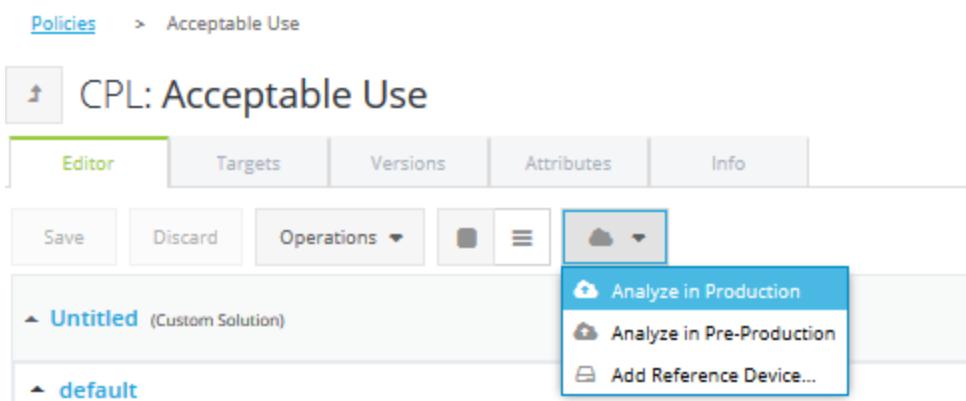
1. [Create a new CPL policy object](#) or [edit an existing CPL policy object](#).
2. Analyze the CPL policy.
3. Make changes to optimize the on-premise and WSS portions of the policy.
4. Repeat steps 2 and 3 until you are satisfied with the policy.

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

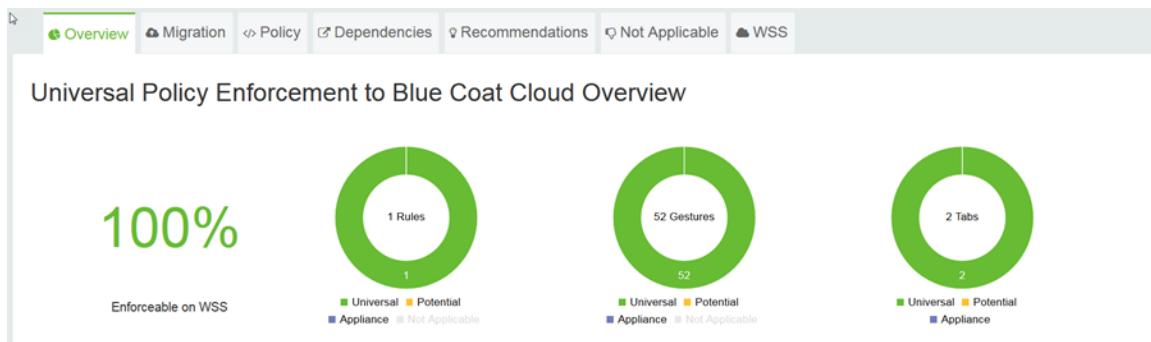
1. Select **Configuration > Policy**.
2. Click the policy name hyperlink or highlight the row and click **Edit**. Verify that you are in the **Editor** tab.
3. Click the cloud icon and select **Analyze Policy > Analyze in Production** to open the policy classifier.

Note: 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.

Management Center Configuration & Management



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.

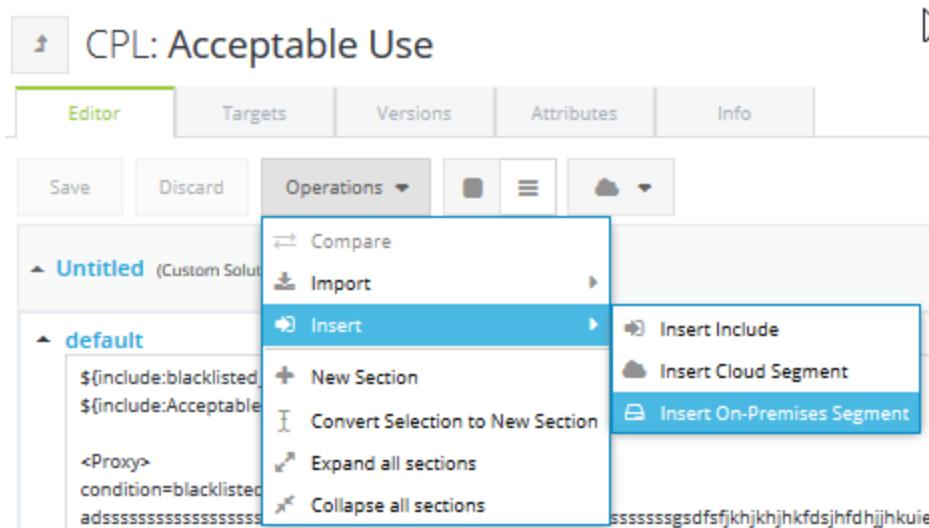
5. Using what you have learned from the classifier, edit your CPL policy. For example, if you think a section should apply only to on-premise appliances, do the following:

a. **Highlight the section.**

```
<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
```

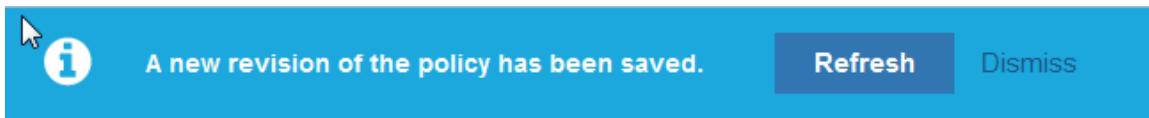
b. **Select Operations > Insert > Insert On-Premises Segment.**



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.



Note: 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.

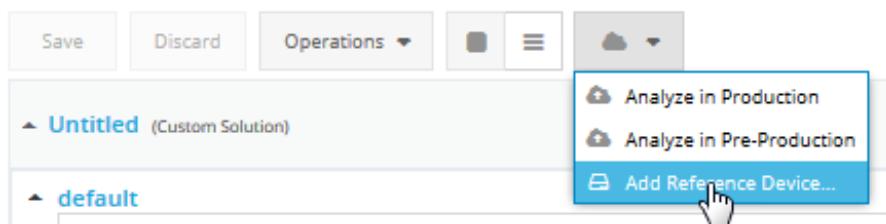
Select Reference Device for Universal CPL Policy

You must associate a reference device with your universal CPL policy before you can install it to the Web Security Service Production Network.

1. Select **Configuration > Policy**. From the Policy Objects list, select the CPL policy. Click **Edit**.

Tip: 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

What do you want to accomplish?	Refer to this topic
Deploy universal policy.	"Apply a Single Policy to Both On-Premises and Cloud Users" on page 438
Add or remove devices associated with the policy.	"Add or Remove Devices Associated with Policy" on page 480
Restore a version of the policy.	"Restore a Version of Policy " on page 493
Import a policy configuration from a device.	"Import Policy or Shared Objects" on page 457

Install or Import Policy

To install or import policy, refer to the following.

"Preview Policy Before Installing It" below

"Install Policy" on the next page

"Install Multiple Policies" on page 455

"Import Policy or Shared Objects" on page 457

"Import External Policy " on page 465

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** and select the device for which you want to preview policy.
4. Click **Preview**.

If you have unsaved policy changes, choose **Unsaved Changes** or view the **Latest Saved Version**. The web console displays the CPL in a Preview dialog.

Tip: Only saved policy can be installed. Use **Preview** to verify your unsaved policy before saving it. Then save and install it.

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 312.

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.

Warning: You cannot install a shared object. Shared objects are used to augment policy, not to replace policy. See "Create Shared Objects" on page 495.

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 493.

Policy Installation Methods

Install policy using one of the methods described in the following table.

Type	Location	Notes
Install	Configuration > Policy	Install policy using job wizard. You can select more than one script to install in the same job.
Install to All	Configuration > Policy > <i>Policy_Name</i> > Edit > Targets	Install policy using job wizard.
Install to Target	Configuration > Policy > <i>Policy_Name</i> > Edit > Targets	One click policy installation. Does not use the job wizard.
Install Policy	Jobs > Add > New Job > Install Policy	Install policy using job wizard.

Install Policy

The following procedure also applies to **Install to All**.

1. Select **Configuration > Policy** and highlight one or more policy rows. Click **Install**.

2. **Policies:**

- For each policy, click **All Predefined Targets** to install the policy to all target devices specified for the policy (**Policy > Edit > Targets**), or click **Selected Targets** to select specific target devices.
- Select **Force installation (don't abort the job on installation warnings)** if you want the job to run even if installation warnings are encountered. When you select this option, Management Center will install the policy even if it is identical to that already installed on the device. If this option is not selected and the policy is identical, the job will execute successfully (without reporting any associated warnings) with a note that no installation was actually performed.

If you run a job many times a day and force installation, a large number of policy deployment records can be recorded in your database. In that case, Symantec recommends that you do not select this option if you want to limit the number of deployment entries in the database.

- Click **Add More Policies** to add other policies to your installation.
- If you selected multiple policies, verify the order of policy installation. Click the **Remove** button to remove a policy file or the arrows to move them up or down in the installation order.

3. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

4. **Schedule:**

Choose to trigger job execution using a "Schedule" below or an "Event" on the next page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

5. Name:

- Verify or change the name and add an optional description.

6. Click **Save**.

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**.

Note: If you attempt to install policy that is identical to that already installed on the device, the system informs you that they are identical and prompts you to confirm the installation. If you proceed with installation, the policy is installed. This can be useful if you want to view policy warnings associated with the installation.

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

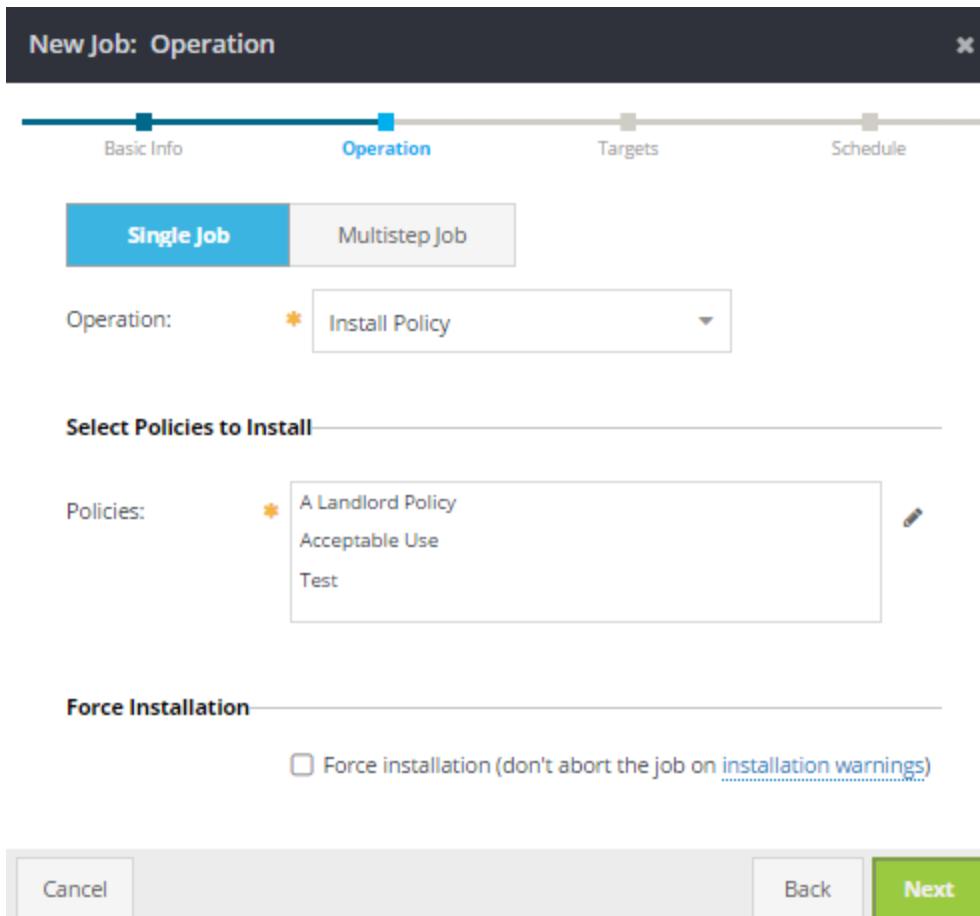
Tip: By forcing the Installation, you are ensuring that large deployments of policies DO NOT fail when encountering devices that may have the above issues.

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.

Tip: 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).

Note: 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 600 and "Install Policy" on page 451.

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)" below
- "Import Policy from a File (Object Edit)" on page 461
- "Import Policy from a Device" on page 462

Note: 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`)

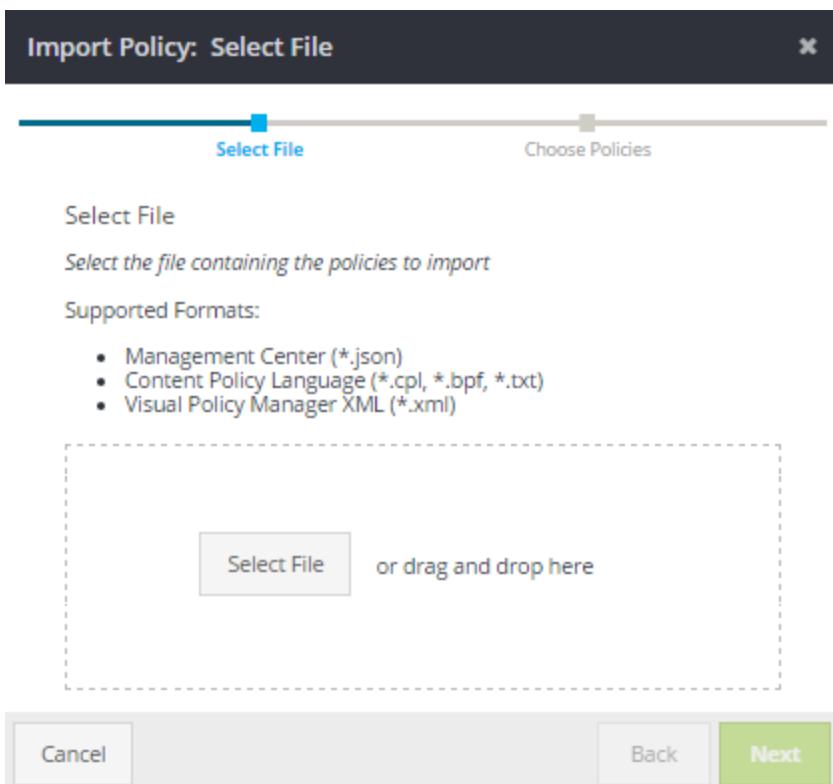
Procedure

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.

2. Click **Import**.



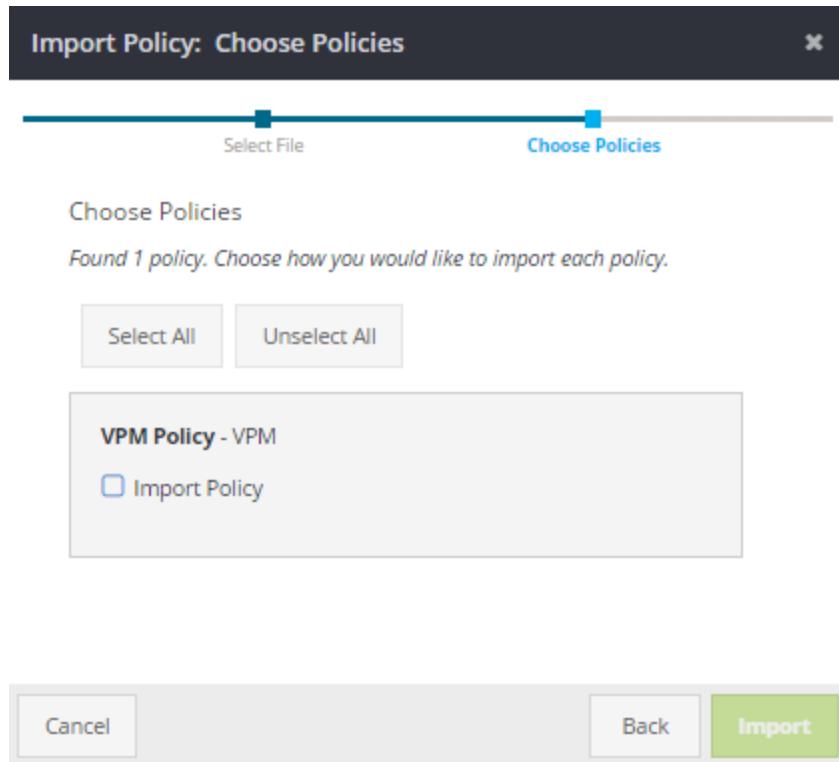
The system displays the Import Policy wizard.



3. Drag and drop the file into the **Select File** dotted-line area. Alternatively, browse to the file.

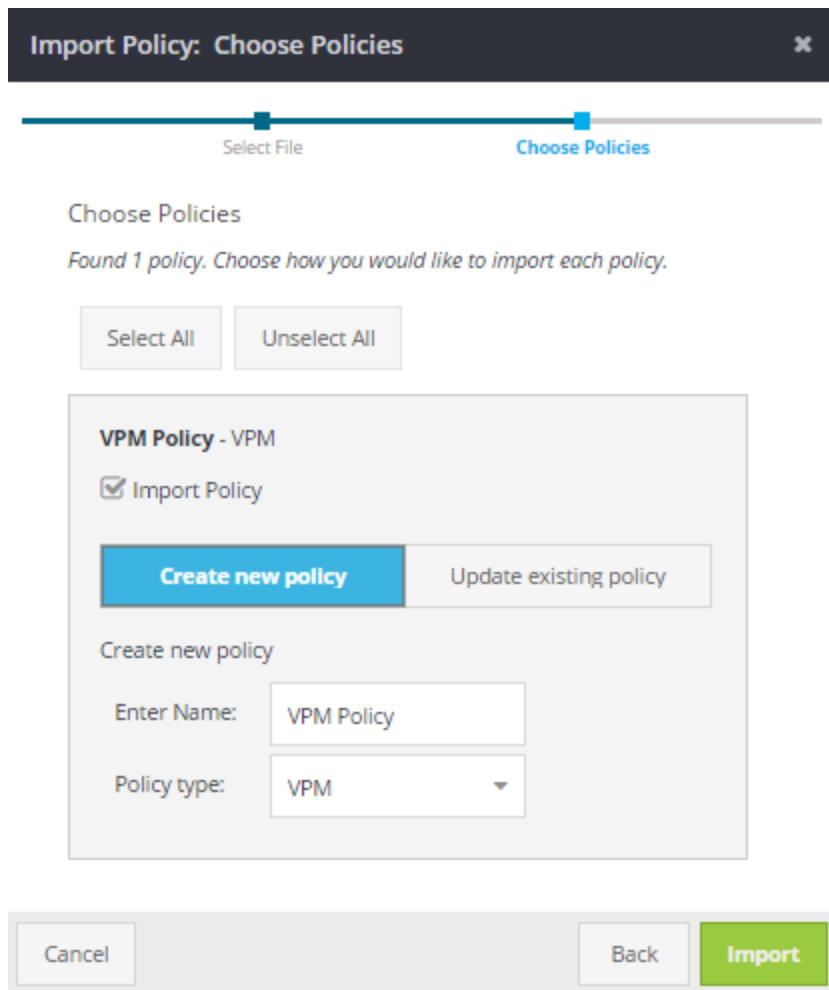
4. Click **Next**.

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.

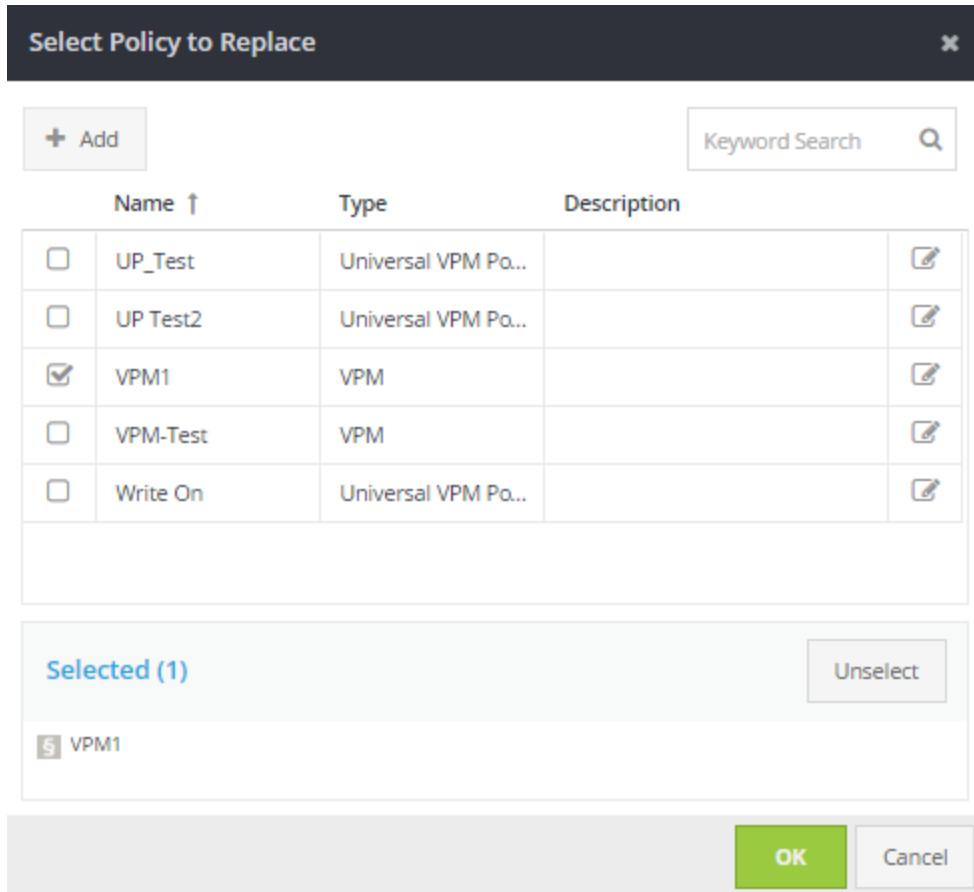
6. Choose whether to create a new policy or to update an existing policy.



Note: 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 replace, and click OK.

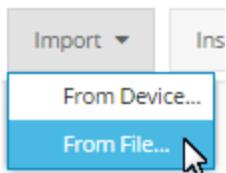


7. Click **Import**. The system displays the results of the import.
8. Click **Close** to exit the wizard.

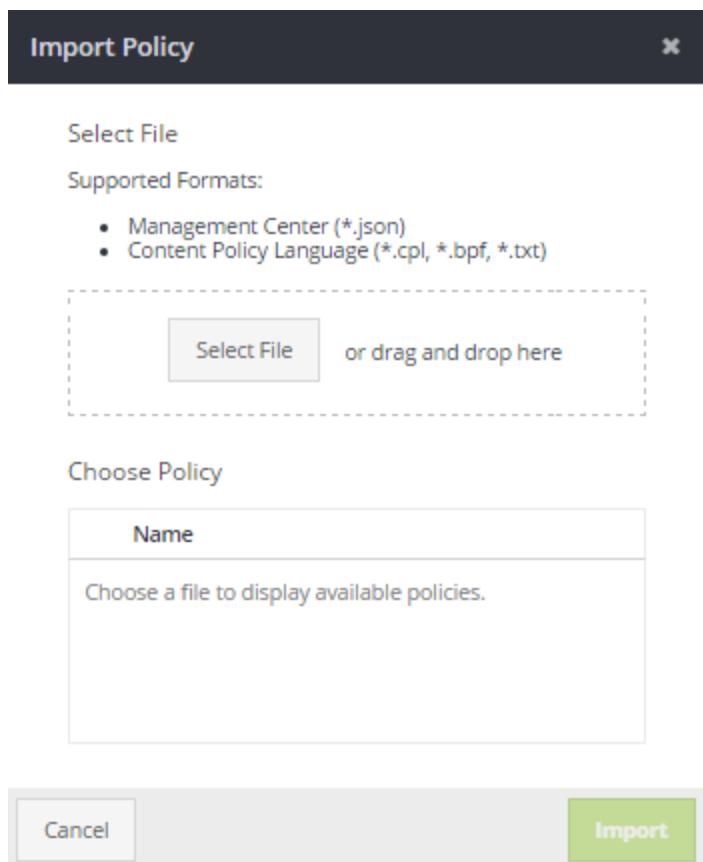
Import Policy from a File (Object Edit)

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.

Note: 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 488.
9. Enter a comment for the commit operations and click **Save**. The comment that you enter is saved as metadata.

Determine Your Next Step

What do you want to accomplish?	Refer to this topic
Export policy	"Export Policy or Shared Objects to Local Disk" on page 491
View existing policy information	"View Existing Policy Information" on page 472
Restore a version of the policy	"Restore a Version of Policy " on page 493
Deploy the policy, as is, to devices	"Install Policy" on page 451

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.

Note: This operation is not supported in Multistep Device Jobs.

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 295.
3. (Optional) If you intend to use the URL as an absolute path to the policy target file, select **Use URL as absolute path to file**.
4. If you intend to import policy from a directory that contains UUID .bpf files, do the following*:
 - 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

5. Store a file that contains the contents of the policy on a web, FTP, or SCP server.
6. 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.

Create Job to Import External Policy

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Import External Policy**.
3. **Source:**
 - **Import from URL:** The path to the file on the external web, FTP, or SCP server. The filename must be the ID assigned to the target policy.
 - Directory URL Example: `ftp://company.com/policies/`
 - Absolute Path to File Example: `ftp://company.com/policies/mypolicy.txt`
 - **Use URL as absolute path to file:** This option is not selected by default. Leave this option 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).
 - **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.

Note: 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.

4. **Destination:**

- Select the policies to update.
- Add multiple policies by selecting the check box next to the name of the policy.

5. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. **Name:**

- Verify or change the name and add an optional description.

8. Click **Save**.

Distribute ProxySG Policy to Multiple Devices

When you want multiple ProxySG appliances to run the same policy, you can create the policy once and then distribute it to all devices that require this same policy. To accomplish this goal, you create and test the policy on a reference device, assign targets to the policy, and then create a job to install the policy on the predefined targets.

1. (Optional) Create a device group for the ProxySG devices to which you want to distribute the same policy. See "Add a Device Group" on page 166.
2. Create and test a VPM policy on a single device; this ProxySG is called the *reference device*. See "Select Reference Device for VPM Policy" on page 325.

Note: You can also use CPL to write the policy. See "Create a CPL Policy Object" on page 295.

3. Select the target devices to which you want to distribute the policy:
 - a. Select **Configuration > Policy**.
 - b. Select the policy you created in step 2 and click **Edit**.
 - c. Click **Targets > Add Targets**.
 - d. Click the **Groups** tab and selected the group created in step 1.
 - e. Click **Next** and **Finish**.

4. Create a job to install the policy on the target devices. See "Install Policy" on page 451.
5. After Management Center runs the policy installation job, confirm that the policy was installed on the target devices.

View Policy

To view policy, refer to the following.

"Preview Policy Before Installing It" on page 450

"View Existing Policy Information" on page 472

"View Deployed Policy for each Device Slot" on page 477

"View Devices Associated with Policy" on page 478

View Policy Versions

Management Center enables you to view CPL or VPM policy versions.

Note: 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 256.
3. With the policy selected, click **Edit**. The system displays the editor.
4. **Select the Versions tab.**

The screenshot shows a navigation bar with tabs: Editor, Versions (highlighted in green), Attributes, and Info. Below the navigation bar is a section titled "Version Control". Under "Version Control" are three buttons: Compare, View (circled in blue), and Restore. A table lists two versions:

Version ↓	Author	Date	Comments
1.1 (circled in blue)	Admin23	12/7/16 2:52 PM	asd
1.0	Admin23	12/7/16 2:51 PM	Initial revision

5. Select the policy version you want to view.
6. Click **View**. The Preview dialog displays.

CPL example:

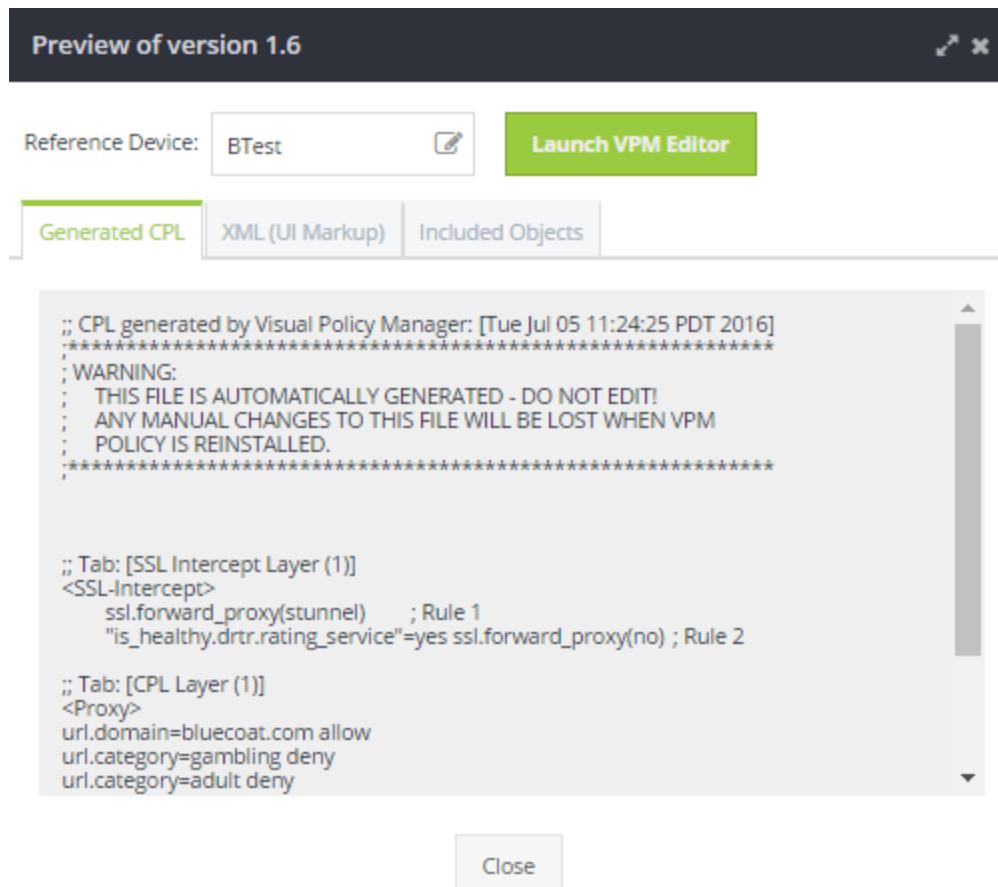
The screenshot shows a "Preview of version 1.1" dialog. At the top right are close and minimize buttons. On the left is a toolbar with two icons. In the center is a "Keyword Search" input field with a magnifying glass icon. To the right is a "Quick Navigation" pane with a list of policy components:

- Untitled (Custom Solution)
 - default
 - # test
 - override
 - mandatory

At the bottom right is a "Close" button.

VPM example:

Management Center Configuration & Management



7. (Optional) To compare policy versions, see "Compare Different Versions of the Same Policy" on page 488.
8. (Optional) To restore an earlier version of the policy, See "Restore a Version of Policy " on page 493.
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**.

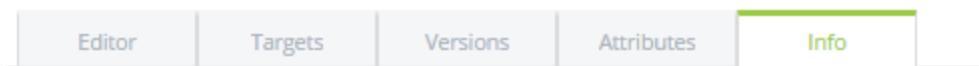
View Policy Object Information

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**

Tip: Variable substitution is powerful and can be applied to policies and scripts. See "Use Substitution Variables in Policies and Scripts" on page 312.

3. Metadata displays under **Latest Revision**:

Management Center Configuration & Management



General Information

Identifier

Unique Id: EC967540-F286-40EB-9A42-7645FEB2C262

Overview

Policy name: * Administrative Access to Web Filter

Policy type: * VPM

Reference ID: VPM1

Description: This policy is for Super Admins only. It gives full access to the web filter database.

938 of 1024 characters left

Replace substitution variables

Latest Revision

Version: 1.6

Author: admin

Date: 2/10/17 3:18 PM

Comments: added "test" list

Save

Cancel

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.

Policies > VPM1

VPM: VPM1

Editor mode: Read-Write
Policy type: VPM

Version ↓	Author	Date	Comments
1.6	admin	2/10/17 3:18 PM	added "test" list
1.5	admin	12/5/16 12:08 PM	Changed reference device ...
1.4	admin	8/10/16 3:32 PM	VPM Reference multiple o...
1.3	admin	7/5/16 12:25 PM	asd

- **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.

Tip: 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 584 or "Edit Attributes" on page 587.
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. Click **Save** and then **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.
 - 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 256.
2. Click **Edit**. Select the **Targets** tab.

Note: 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.

What do you want to accomplish?	What you can do	Refer to this topic
Write new policy; the behavior that you want is not yet expressed in policy in Management Center.	Create policy, which involves first creating a policy object.	"Create a CPL Policy Object" on page 295
Create a policy using the Visual Policy Manager.	Create a VPM Policy Object.	"Add a VPM Policy Object" on page 323 and "Launch Legacy Visual Policy Manager (Java)" on page 321
Create rules to route traffic to the proper tenant.	Create tenant determination rules.	"Specify Tenant Determination Rules " on page 210
Specify rules to protect your WAF applications.	Create a WAF Application object.	"Configure WAF Application Objects" on page 229
Remove devices from policy or add devices to policy; you want to keep the policy but change the devices that use it.	Associate devices with, or disassociate devices from, a specific policy.	"Add or Remove Devices Associated with Policy" on the facing page
Modify existing CPL policy because it does not behave as intended or has to be improved.	Refine the existing policy.	"Refine Existing CPL Policy" on page 302
	Change the order of policy rules so that the device evaluates correctly.	"Change the Order in which Policy Rules are Evaluated" on page 311
Verify information about existing policy.	Check information about an existing policy.	"View Existing Policy Information" on page 472

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.

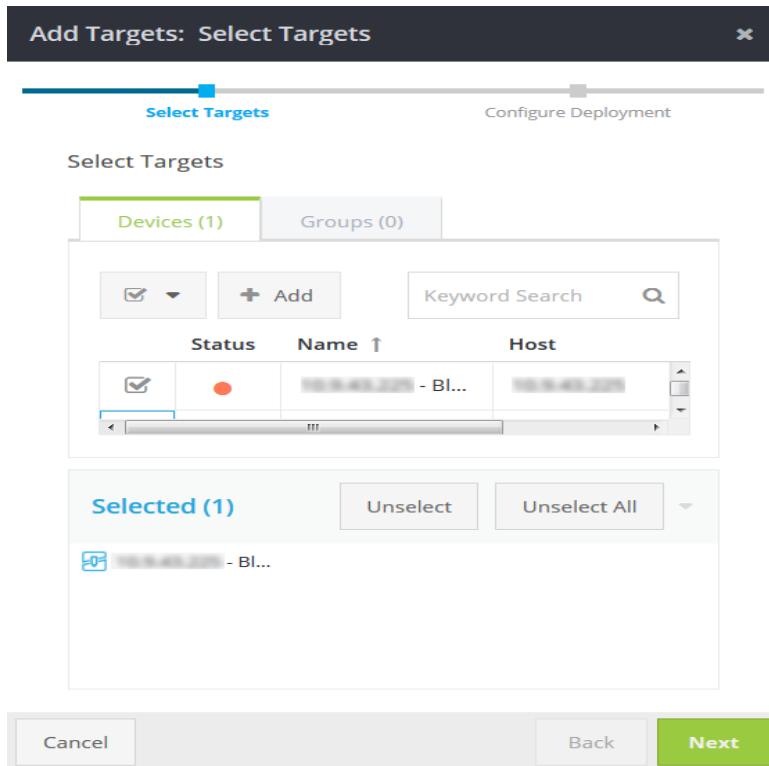
- You cannot add WSS and other devices (for example, a Content Analysis) as targets in the same operation because they have different deployment types. You must add WSS devices in a separate operation.
- Management Center must have a connection to the reference device at the time of installation. When 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 256.
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).

Note: Only those targets that can support the policy selected are shown. This helps to know which policies can be installed on which targets (devices).

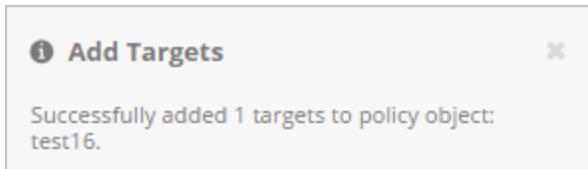
Management Center Configuration & Management



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.

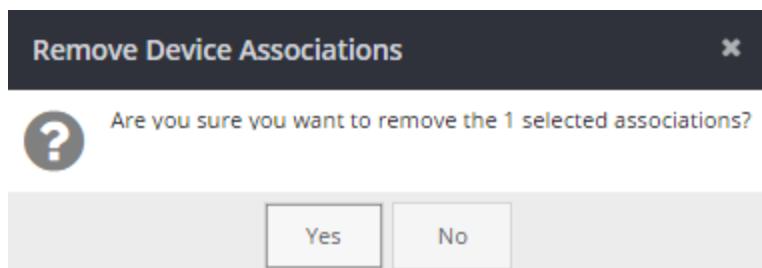
Note: If you select **Tenant Slot** and a tenant is not configured, a "Tenant not configured" warning appears in the Deployment column on the Targets tab.

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

What do you want to accomplish?	Refer to this topic
View associated devices (targets)	"View Devices Associated with Policy" on page 478
Compare policy versions	"Compare Different Versions of the Same Policy" on page 488
Install a policy	"Install Policy" on page 451
Compare the policy version installed on the device, with the most current version saved in Management Center	"Compare the Device Policy Version with Current Policy Version" on page 491
Schedule a policy installation	"Add a Job" on page 600
Install multiple policies to multiple devices	"Install Multiple Policies" on page 455

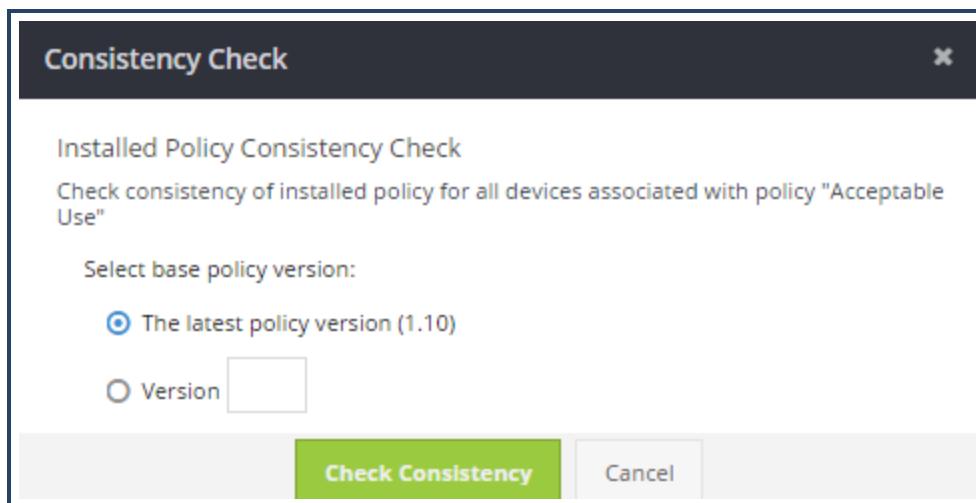
Check Consistency between Policy and Devices

You can check if the policy saved in Management Center is different from the policy installed on devices. You can also create a job to check consistency. See "Create Job to Check Consistency of Policy" on page 485.

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.

Note: 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.**



Warning: 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.

The screenshot shows the Management Center Policies page with the URL [Policies > ASUP](#). The policy name is CPL: ASUP. The Editor mode is Read-Write and the Policy type is CPL. The Targets tab is selected, showing the following table:

En...	Name	Device Co..	Deployment	Device Model	Installed Version	Matching ver. 1.4	OS Type
✓	10.169....		VLCF Local	300-25		☒ Mismatch	SGOS 6....

6. (Optional) For each device listed, verify the following:

Note: 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 32.

Determine Your Next Step

What do you want to do next?	Refer to this topic
Add or remove associated devices.	"Add or Remove Devices Associated with Policy" on page 480
Compare different versions of the same policy.	"Compare Different Versions of the Same Policy" on page 488
Install a policy or policies.	"Install Policy" on page 451 or "Install Multiple Policies" on page 455
View policy information.	"View Existing Policy Information" on page 472

Create Job to Check Consistency of Policy

This job checks if the policy saved in Management Center is different from the policy installed on devices.

Note: This operation is not supported in Multistep Device Jobs. See also "Check Consistency between Policy and Devices" on page 483.

Schedule Consistency Check of Policy

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Check Consistency**.
3. **Policy:**
 - **Policy to check:** Select the reference policy to use for comparison. The job will check the policy against all associated targets.
4. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. **Name:**

- Verify or change the name and add an optional description.

7. Click **Save**.

Warning: 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.

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 256.
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.

Revision 1.3		Revision 1.5	
1	<code>\$(include:blacklisted_categories)</code>	1	<code>\$(include:blacklisted_categories)</code>
2	<code>\$(include:Acceptable_Class_Whitelist_Categories[1.1])</code>	2	<code>\$(include:Acceptable_Class_Whitelist_Categories[1.1])</code>
3		3	
4	<code><Proxy></code>	4	<code><Proxy></code>
5	1	5	1
6	2	6	2
7	3	7	3
8	4	8	4
9	5	9	5
10	6	10	6
		10	7
		11	8
		12	9
		13	10
		14	11
		15	12

Close

- 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 screenshot shows a 'Compare Policy' dialog with two tabs: 'XML (UI Markup)' and 'Generated CPL'. The 'Generated CPL' tab is selected, displaying a side-by-side comparison of two policy versions. The left column, labeled 'Revision 1.0', contains a single line: '1 : Empty vpm policy object'. The right column, labeled 'Revision 1.3', contains several lines of policy code:
1 :: CPL generated by Visual Policy Manager: [Fri Jan 29 14:15:42 MST 2016]
2 ;*****
3 ;*****
4 ; WARNING:
5 ; THIS FILE IS AUTOMATICALLY GENERATED - DO NOT
6 ; EDIT!
7 ; ANY MANUAL CHANGES TO THIS FILE WILL BE LOST WHEN
8 ; VPM
9 ; POLICY IS REINSTALLED.
10 ;*****
11 ;*****

A 'Close' button is visible at the bottom right of the dialog.

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 493.
6. Click **Close**.

View Effective Policy for each Slot on a Device

Effective Policy is the policy that will be applied to the device in situations where more than one policy could be applied. For example, administrators sometimes inadvertently assign a policy to a specific device and a different policy to the group that device resides in. The Effective Policy shows the policy that takes precedence—in this case, the device-specific policy.

1. From the **Network** tab, select a device to view the effective policy.
2. Click **Edit**.
3. From the Edit Device dialog, select the **Policies** tab.
 - **VPM** - The VPM slot is a unique policy created by Visual Policy Manager.
 - **Local**
 - **Central**
 - **Forward**
 - **Tenant Policies** - The Tenant Policies slot included policy for every tenant that will be passing traffic through the ProxySG appliance.

How the effective policies are assigned

- 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. CPL Policy is displayed in the following slots:
 - Local
 - Central
 - Forward
- Merged - Because there can be thousands of tenants passing traffic through the device, no specific mapping of the tenant policies to the slot is possible. As a result, if there are 2 or more tenant policies mapped to the slot, the policies display as Merged.

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. This can help you determine if you the desired policy version is installed on the device.

1. Select **Configuration > Policy** and click the policy to open the editor.
2. Click the **Targets** tab.
3. Select the target device and click **Compare**.

Compare			
	Version on Device		Current Version (1.6)
1	Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia volupta ...	1	Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia volupta ...

[Close](#)

Determine Your Next Step

What do you want to accomplish?	Refer to this topic
View all of the details about an existing policy, including policy object information, the policy version, and the associated attributes.	"View Existing Policy Information" on page 472
Compare different versions of the same policy.	"Compare Different Versions of the Same Policy" on page 488

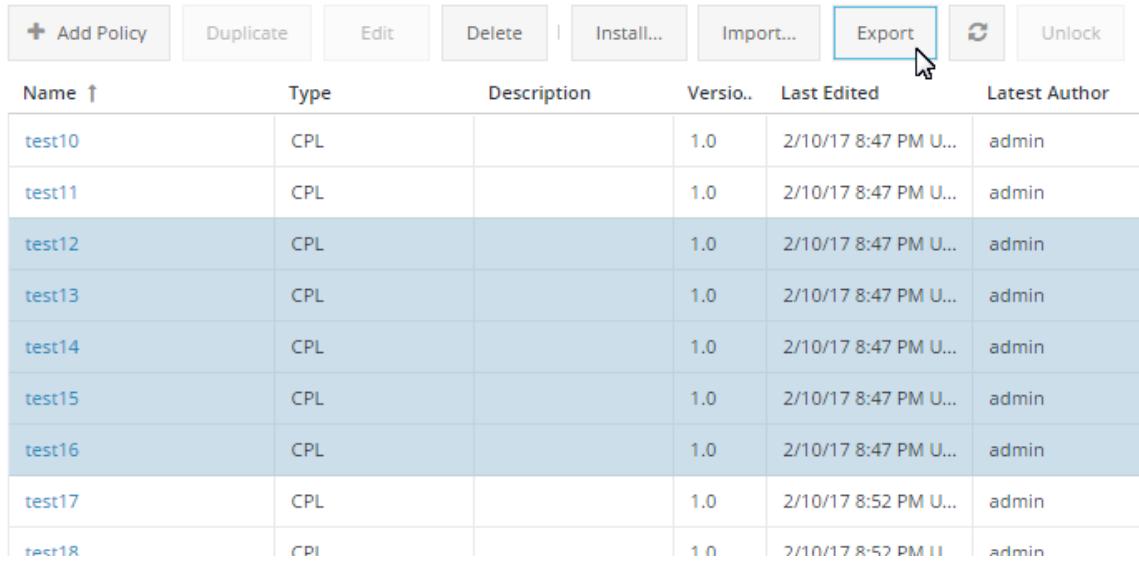
Export Policy or Shared Objects to Local Disk

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**.

Policy Objects



Name ↑	Type	Description	Versio..	Last Edited	Latest Author
test10	CPL		1.0	2/10/17 8:47 PM U...	admin
test11	CPL		1.0	2/10/17 8:47 PM U...	admin
test12	CPL		1.0	2/10/17 8:47 PM U...	admin
test13	CPL		1.0	2/10/17 8:47 PM U...	admin
test14	CPL		1.0	2/10/17 8:47 PM U...	admin
test15	CPL		1.0	2/10/17 8:47 PM U...	admin
test16	CPL		1.0	2/10/17 8:47 PM U...	admin
test17	CPL		1.0	2/10/17 8:52 PM U...	admin
test18	CPI		1.0	2/10/17 8:52 PM U...	admin

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 256.
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 472.
 - Compare versions of policy. See "Compare Different Versions of the Same Policy" on page 488
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 451.

Use Specific Attribute Values to Control Access to Policy

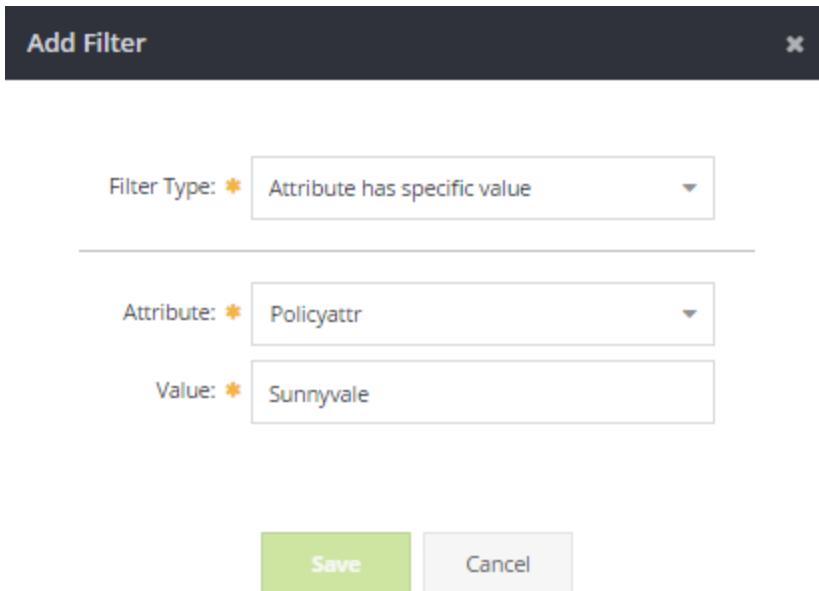
You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Attributes are custom metadata used to refine and edit devices, device groups policy, and scripts. These attributes can be used to control access to policy, as described below.

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**.

Tip: 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.

- e. 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**.

About Universal Policy Enforcement

Management Center can be used in conjunction with the Symantec Web Security Service to create universal policy enforcement (UPE) rules. For more information, see "Apply a Single Policy to Both On-Premises and Cloud Users" on page 438.

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.

Note: 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.

Note: 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 344

"Include a Shared Policy Object in CPL or VPM Policy" on page 355

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 363

"Category List Example" on page 368

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 374

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 345

"URL List Example" on page 349

Create an IP Address List

Easily create IP address lists for use on the SSL Visibility appliance.

"Create IP Address List " on page 417

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 353

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 215

Creating a WAF Security Profile is step 3 in "Use WAF Policy To Protect Servers From Attacks" on page 199.

Permissions Reference

When defining users, groups, roles and grant permissions, refer to the following for important information.

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.

Note: 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

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Perform all functions in all areas of the web console	None
View	View all areas of the web console	None

Attribute Definition

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Add, delete, and edit attributes	None
Add	Add attributes	Attribute Definition - View
Delete	Delete attributes	None
Update	Edit attributes	None
View	View attributes	None

Audit

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Perform all audit log functions	None
View	Read-only access to audit log records	None

Backup Image

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Import, export, delete, and restore image backups	Management Center - View Management Center - Update
Delete	Delete backups	
Export	Export backups	
Import	Import backups	
Update	Restore backups	Management Center - View Management Center - Update
View	View information about existing backups	
View Contents	View the backup contents	

Device

Note: 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 589 and "Reference: Permissions Filters Object and Attributes" on page 513.

Management Center Configuration & Management

Permission Action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
All operations	All device functions	Hierarchy - View Device Group - View	To see the effective policy for a device: Policy - View To change membership in device properties: Device Group - Change Membership
Add	Add devices	Hierarchy - View Device Group - Change Membership Device - View	To add devices by importing from a file: Device - Add Device - Update
Backup	Back up devices	Device - Manage Hierarchy - View Device Group - View Backup Image - Update	
Delete	Delete devices	Hierarchy - View Device Group - View	
Manage	Activate and deactivate devices	Device - View Device - Manage	
Execute Scripts	Execute scripts on devices	Hierarchy - View Device Group - View Device - View Device - Manage Device Script - View	

Permission Action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
Install Policy	Install policy to devices	Hierarchy - View Device Group - View Device - View Device - Update Policy - Assign Targets Policy - Publish	
Restore	Restore configuration backups to devices	Hierarchy - View Device Group - View Backup Image - Update	
Update	Edit device basic information, connection parameters, and attributes	Hierarchy - View Device Group - View	To change membership in device properties: Device Group - Change Membership To add devices by importing from a file: Device - Add Device - Update
View	View device information	Hierarchy - View Device Group - View	

Device Group

Note: 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 589 and "Reference: Permissions Filters Object and Attributes" on page 513.

Management Center Configuration & Management

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
All operations	Perform all device group functions	Hierarchy - View	To see the devices in groups: Device - View
Add	Add device groups	Hierarchy - View Device Group - Change Membership	To associate devices while adding a group: Device - View To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update
Change Membership	Change associated groups in device properties	Hierarchy - View Device - Update	
Delete	Delete device groups	Hierarchy - View Device - View	
Update	Edit device groups' basic information and attributes	Hierarchy - View	To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update
View	Read-only access to device groups	Hierarchy - View	

Device Script

Prior to Management Center 2.0, Device - Manage was required to execute scripts on a device. In 2.0 and later, Device Script enables you to execute scripts on a device without requiring the Device-Manage permission. This means you can limit users to only being able to manage and execute scripts, without providing them with additional device permissions.

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	All functions related to script	None
Add	Add script objects	Device Script - View Device - View
Delete	Delete script objects	None
Edit Metadata	Edit script object attributes and information	None
Update	Edit and execute script content	Device - View Device - Execute Script
View	View script	None
Note: "Compare Versions of the Script" on page 248 is available at this level.		

File

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for ancillary functions
All operations	Add, delete, and edit files	None	
Add	Add file	None	
Delete	Delete files	None	
Edit Metadata	Edit file attributes and information	None	
View	View files	None	

Hierarchy

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for ancillary functions
All operations	Add, delete, and edit hierarchies	Device Group - All operations	

Management Center Configuration & Management

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for ancillary functions
Add	Add hierarchies	Hierarchy - View Device Group - All operations	To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update
Delete	Delete hierarchies (except for the predefined hierarchies)	Device Group - Delete	
Update	Edit hierarchies	Device Group - Update	To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update
View	View hierarchies	Device Group - View	To see devices: Device - View

Management Center

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Perform all Management Center functions.	None
Backup	Perform Management Center backup and restore.	None

PKI

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Perform all operations pertaining to the Management Center data protection key.	None
Add	View Administration > Data Protection tab and view and change the Management Center data protection key.	None
Delete	Delete Management Center data protection key.	None

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
Update	For future use.	None
View	For future use.	None

Policy

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
All operations	All functions related to policy	None	
Add	Add policy objects	Policy - View	To assign targets while adding a policy object: Policy - Assign Target Device - View
Assign Targets	Add and remove target devices	Device - View	
CPL - Add Section	Add policy sections to existing policy objects	None	To add policy sections while adding a new policy object: Policy - Add
CPL - Delete Section	Delete policy sections	None	
CPL - Edit Default	Edit the default sub-section in policy sections	* 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.	
CPL - Edit Mandatory	Edit the mandatory sub-section in policy sections		
CPL - Edit Override*	Edit the override sub-section in policy sections		
CPL - Move Section	Move policy sections within policy objects	None	
CPL - Update Section	Edit the name and purpose of sections	None	
Delete	Delete policy objects	None	

Management Center Configuration & Management

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
Edit Contents	Restore previous versions of policy and edit policy	None	To select a reference device: Device - View
Edit Metadata	Edit policy object attributes and information	None	
Import	Import policy from devices	Device - View Policy - Edit Contents 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).	
Publish	Install policy on target devices	None	To add/remove target devices to policy before installing: Device - View Device - Manage Device - Install Policy Policy - Assign Targets
View	View policy	None	Note: Edit > Check Consistency is available at this level.

REST API

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Grants access to all REST API functions.	
Add	Users can perform POST/GET/PUT operations.	
Delete	Users can perform DELETE operations.	
Update	Users can modify API methods.	
View	Users can view API methods.	

Role

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	All role functions	None
Add	Users can add roles	Role - View
Delete	Users can delete roles	None
Update	Users can update roles	None
View	Read-only access to roles	None

Scheduled Job

Note: 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 517.

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
All operations	Add, edit, delete, enable, disable, and run jobs; view job progress, current jobs, and job history	None	

Management Center Configuration & Management

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
Add	Add jobs Caution: Scheduled Job - Add is an elevated permission. See "Reference: Understanding Job Permissions" on page 517.	Scheduled Job - View Device - View (For policy jobs) Policy - View	
Cancel Running Job	Cancel all active, running jobs	Scheduled Job - View Device - View (For policy jobs) Policy - View	
Delete	Delete jobs	None	
Run Manually	Run jobs manually using the Run Now option	None	
Update	Edit jobs' information and schedule; enable/disable jobs Caution: Scheduled Job - Update is an elevated permission. See "Reference: Understanding Job Permissions" on page 517.	None Device - View To add/remove policies from a job: Policy- View	
View	View all scheduled and current jobs and job history Note: All users can see the Jobs tab in the web console, even if they do not have a Scheduled Job - View permission.	None	

Session

Note: Session permissions are specifically to control access to user sessions.

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	View, kill, disable logins	None
View	View active sessions	None
Kill Session	Kill an active session	None
Enable/Disable User Login	Enable or Disable logins to Management Center	None

Settings

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Perform all settings functions in Administration Settings (Hardware Diagnostics is always read-only)	None
Update	Edit Management Center Settings	None
View	View Management Center Settings, and Hardware Diagnostics	None

Statistics

Permission action	Allows access to these areas/functions	Requires these permissions to be useful	Grant these permissions for more functions
All operations	Perform all Appliance Monitoring reports and functions	None	To filter reports and report widgets by device or device group: Device Group - View
View	Read-only access to reports		Device - View

Tenant

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
All operations	Allows access to the tenant definitions in Management Center.	None
Add	Users can add tenants	None

Management Center Configuration & Management

Permission action	Allows access to these areas/functions	Requires these permissions to be useful
Delete	Users can delete tenants	None
Update	Users can edit tenants	None
View	View Configuration > Tenants	None

User

Permission action	Allows access to these areas/functions	Requires permissions to be useful	Grant these permissions for more functions
All operations	Perform all user functions	None	
Add	Add users and specify basic information	User - View Role - View	To assign roles while adding a user
Delete	Delete users	None	
Update	Update users' basic information and change/expire user passwords	None	To add or remove roles from a user: Role - View
View	View users	None	

User Group

Permission action	Allows access to these areas/functions	Requires permissions to be useful	Grant these permissions for more functions
All operations	Perform all user group functions	None	
Add	Add user groups	User Group - View	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

Permission action	Allows access to these areas/functions	Requires permissions to be useful	Grant these permissions for more functions
Delete	Delete user groups	None	
Update	Update user groups' basic information	None	To add/remove users from groups: User - View
View	View user groups	None	

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 589 for information.

Select the Attributes type	Specify the Attributes	What a user can access
Attribute has specific value	Attribute: Select Rack . Value: Specify the rack. Click Save . The Filter field displays " Rack is ' <i><value></i> '".	Devices specified with this rack in device properties under Attributes > User-Defined .
	Attribute: Select Location . Value: Specify the location. Click Save . The Filter field displays " Location is ' <i><value></i> '".	Devices specified with this location in device properties under Attributes > User-Defined .
Attribute has any value	Attribute: Select Rack . Click Save . The Filter field displays " Rack is not empty". Attribute: Select Location . Click Save . The Filter field displays " Location is not empty".	Devices specified with any rack specified in device properties under Attributes > User-Defined .
		Devices specified with any location in device properties under Attributes > User-Defined .

Select the Attributes type	Specify the Attributes	What a user can access
Specific Device	<p>Device: Select a device from the drop-down list.</p> <p>Click Save. The Filter field displays "Specified Device".</p>	This selected device.
Members of specific group	<p>Hierarchy: Select a hierarchy. Your selection determines the values for device group.</p> <p>Device Group: Select the device group.</p> <p>Click Save. The Filter field displays "Members of specified group".</p>	All devices in the specified group or its sub-groups.

Set Filters for Device Group Object

Specify Primary Contact and Location attributes. See "Set User-Defined Device Attributes for Access Control" on page 589 for information.

Select the Filter type	Specify the Attributes	What a user can access
Attribute has specific value	<p>Attribute: Select Primary Contact Value: Specify the contact.</p> <p>Click Save. The Filter field displays "Primary is '<value>'".</p>	Groups specified with this primary contact in group properties under Attributes > User-Defined .
	<p>Attribute: Select Location Value: Specify the location.</p> <p>Click Save. The Filter field displays "Location is '<value>'"</p>	Groups specified with this location in group properties under Attributes > User-Defined .
Attribute has any value	<p>Attribute: Select Primary Contact Click Save. The Filter field displays "Primary Contact is not empty".</p> <p>Attribute: Select Location Click Save. The Filter field displays "Location is not empty".</p>	Groups specified with any primary contact in group properties under Attributes > User-Defined . Groups specified with any location in group properties under Attributes > User-Defined .
Specific Device Group	<p>Hierarchy: Select a hierarchy. Your selection determines the values for device group.</p> <p>Device Group: Select the device group.</p> <p>Click Save. The Filter field displays "Specified Device Group".</p>	The specified device group.

Select the Filter type	Specify the Attributes	What a user can access
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 587.

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 583.

Reference: Understanding Job Permissions

A job is distinct from the *operation* (such as backing up devices and installing policy) that the job executes. When users create a job, they define its operation, targets, and schedule. If a user has permissions to add or update jobs, that user 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.

Note: 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 a potential security risk.

Tip: 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

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 524
- "View, Edit, or Delete User Accounts" on page 550
- "Manually Reset a User's Web Console Password" on page 558
- "Expire a User's Web Console Password" on page 558

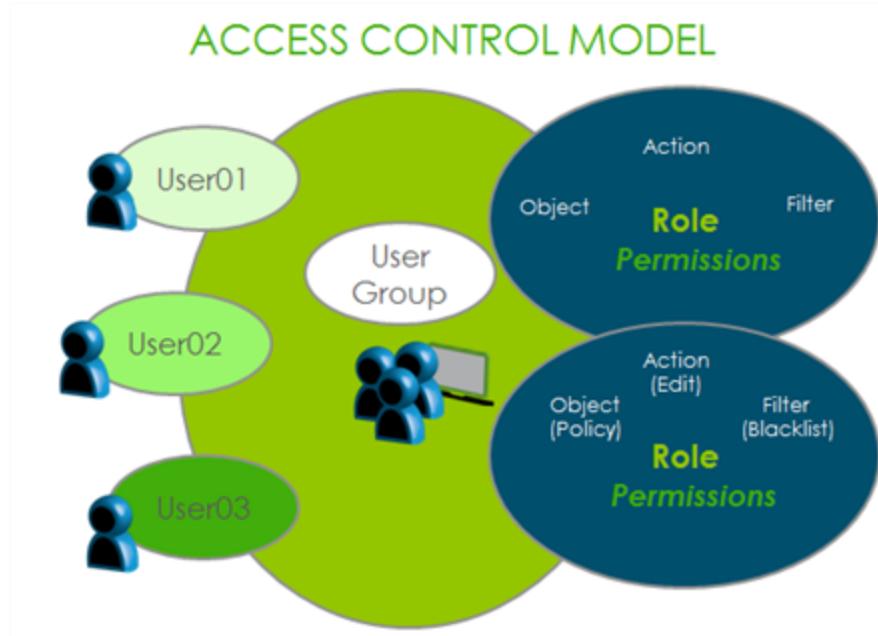
Add Users and Grant Permissions

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 567.
 - To duplicate an existing role, see "Duplicate an Existing Role" on page 569

- (Optional) "Edit an Existing Role" on page 570.
2. "Add Local Users" on page 524 after you have created a role structure and defined roles.

(Optional) "Add User Groups" on page 561. 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 499.

- "Grant Permissions" on page 572 to users. See "Reference: Permissions Filters Object and Attributes" on page 513.
- (Optional) Grant job permissions to users. See "Reference: Understanding Job Permissions" on page 517

(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 575.
- To specify object filters, see "Reference: Permissions Filters Object and Attributes" on page 513.

(Optional) Add Users from External Directory Services

Management Center Configuration & Management

To authenticate users using RADIUS, LDAP or Active Directory services, see "Authenticate Users and User Groups using Existing Directory Service" on page 541. Available directory services to which you can authenticate users include:

- "Authenticate Users Against Active Directory LDAP" on page 535
- "Authenticate Users Against LDAP" on page 531
- "Authenticate Users Against RADIUS" on page 538

Add Local Users

Use these setting to provide Management Center access to local users.

Security Considerations

The following items are supported:

- Management Center logs all access attempts to the audit log and syslog.
- Users with the administrator role can manually expire a user's password and force them to enter a new one.
- Management Center tracks the last access attempt in the user record and displays the record when viewing the user's details (**Administration > Users**).
- 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" on page 541.

Note: 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 513 and "Reference: Permissions Interdependencies" on page 499.

Add Users

Note: Management Center includes a default administrator account named **admin**. You cannot delete this account, but you can change the password from the web management console from **Administration > Users > Management Center**.

Tip: 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.

Note: Management Center 2.0 introduces a default password policy. All new user accounts you define must have at least 6 characters by default, and common words are prohibited. See this topic for more information.

Field	Description
Username *	Usernames are case-sensitive and cannot be changed. Note: Although the username/password combination successfully authenticates if the username has a mixture of cases, Management Center recognizes the users as different users. For example: A user signs in as "joe" and access is setup using that specific case for username. Then later the user signs in as "Joe". The login using "Joe" will have no access because the account created is for the user "joe".
Password *	Example: admin1234
Verify Password *	Example: admin1234
Password expired on:	Does not expire
First Name	The actual first name that the person uses.
Last Name	The actual last name that the person uses.
Email	The Email associated with this user and organization. Example joe@heremail.com
Phone	The Phone number associated with this user and organization (including extension, if any)
Mobile	The personal mobile or cell number associate with this person.
Description	1024 character description can include anything from what town she resides to average commute time to security certifications in this user's possession.

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 567 or "Edit an Existing Role" on page 570.
5. Click **Finish**. The new user displays in the Users list and has access to Management Center based on their defined role.

View All Users and Associated Roles and Permissions

The [Summary Report](#) includes a section for user accounts, which includes a summary of all Management Center user accounts and their roles and permissions. To receive this report, select **User Accounts** when creating the Summary Report.

The **Management Center Users** section of the Summary Report includes two reports: **User Permissions Overview** and **User Permissions (detail)**.

Note: See "Run a Summary Report" on page 685 for more information about creating a Summary Report.

About the User Permissions Overview Report

MANAGEMENT CENTER USERS						
User Permissions Overview						
Username (Role Count)	Name	Network	Config	Jobs	Reports	Admin
JohnSmith (1)	John Smith	1	1	1	1	1
admin (1)	Management Center	1	1	1	1	1
Admin2 (1)	John Jones	1	1	1	1	1

The **User Permissions Overview** report lists the users, the number of assigned roles, and the associated number of permissions in each permission category. The permission categories are shown in the following table.

Network (Device Mgmt.)	Configuration (Policy & Config.)	Jobs	Reports	Administration
All Objects	All Objects	All Objects	All Objects	All Objects
Management Center	Management Center	Management Center	Management Center	Management Center
Device	Device Script	Backup Image	Statistics	Alert

Network (Device Mgmt.)	Configuration (Policy & Config.)	Jobs	Reports	Administration
Device Group	File	Scheduled Job		Attribution Definition
	Policy			Audit
	Tenant			Hierarchy
				Role
				Device
				Device Group
				Policy
				Device Script
				Session
				PKI
				(Data protection)
				Settings
				User
				User Group
				REST API

User Permission Overview Example

In this example, the user nance56 has 1 **Config** permission, 1 **Jobs** permission, and 2 **Admin** permissions:

User Permissions Overview

Username (Role Count)	Name	Network	Config	Jobs	Reports	Admin
JohnSmith (1)	John Smith	1	1	1	1	1
Admin2 (1)	John Jones	1	1	1	1	1
nance56 (1)	Nancy Howard		1	1		2
admin (1)	Management Center	1	1	1	1	1

This is because user nance56 has the following permissions:

Permission	Category
Device Script - All Operations	Configuration Administration

Permission	Category
Attribute Definition - All Operations	Administration
Scheduled Job - Add	Jobs

About the User Permissions Report

The Summary Report also includes a detailed breakdown by user. This is called the **User Permissions** report.

Nancy Howard nance56	Toronto CP Direct Inheritance	Device Script - All operations	None
		Attribute Definition - All operations	None
		Scheduled Job - Add	None
Management Center admin	administrator inherited from: Administrators		
	All objects - All operations		

For the release note: The Summary Report has been improved to show sub-sections and page numbers.

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

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

Observe the following prerequisites:

- The LDAPS server must support TLSv1.1 or higher for Management Center to successfully establish the connection for authentication.
- 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, consider a name you'll use to define it and log in to the Management Center command line interface to enter the following sequence of commands:

```
# configure
(config)# ssl
(config-ssl)# inline ca-certificate <CA Certificate name>
*** command will prompt for CA contents
(config-ssl)#
(config-ssl)# edit ccl browser-trusted
(config-ccl-browser-trusted)# add <CA Certificate name>
```

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.

Setting	Description	Input Value/Format
User must have permission	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.	false <input type="checkbox"/> true <input checked="" type="checkbox"/>
Role attribute	Specify the roles to assign to imported users. Use the same name that exists in LDAP, ensuring that the spelling and case are identical.	businessCategory
Display name attribute	Specify the format of user names.	displayName

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.
2. Enter the Primary Server Settings described in the following table.

Setting	Description	Input Value/Format
Is the authenticator enabled*	Enable LDAP authentication.	false <input type="checkbox"/> true <input checked="" type="checkbox"/>
LDAP URL*	The URL used to connect to the LDAP directory server. Example: ldap://localhost:10389/dc=example,dc=com LDAPS example ldaps://ldapserver1:3269/dc=example,dc=com	Specify the LDAP host, port, and root.
Login user	If required, enter the username used for browsing.	Specify the username.
Login password	If required, enter the password used for browsing.	Specify the password.

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.

Setting	Description	Input Value/Format
Is the authenticator enabled*	Enable LDAP authentication.	false <input type="checkbox"/> true <input checked="" type="checkbox"/>
LDAP URL*	The URL used to connect to the LDAP directory server.	Specify the LDAP host, port, and root. Example: ldap://localhost:10389/dc=example,dc=com
Login user	If required, enter the username used for browsing.	Specify the username.
Login password	If required, enter the password used for browsing.	Specify the password.

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.

Setting	Description	Input Value/Format
Ignore partial results on search	When set to true , ignores any partial results from LDAP searches. The default is false . When using this authenticator to connect to Active Directory, set this option to true .	false true <input type="checkbox"/>
Base DN for user search*	Specify where in the LDAP directory tree to initiate the username search.	Example: ou=users, o=organization
User search*	Specify the user search filter.	Example: (uid={0})

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, click **Save** and then **Activate**. Then, 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

Server Types	Configuration Interface
Apache DS	Apache Directory Studio™ user interface
Novell eDirectory	Novell ConsoleOne user interface

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.
2. Enter the General Active Directory LDAP Settings described in the following table..

Setting	Description	Input Value/Format
Sync the role membership	Specify whether to assign users to roles that match the Role Attribute setting. No roles are synchronized if the Role Attribute is not set.	false true ▾
Sync the group membership	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.	false true ▾
User must have permission	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.	false true ▾

Setting	Description	Input Value/Format
Role attribute	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.	Specify the department to which the role is assigned.
Display name attribute	Specify the format of user names.	displayName

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.
2. Enter the Primary Server Settings described in the following table.

Setting	Description	Input Value/Format
Is the authenticator enabled*	Enable AD authentication.	false true ▾
LDAP URL*	The host URL for LDAP authentication.	Example: ldap://localhost:389

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.

Setting	Description	Input Value/Format
Is the authenticator enabled*	Enable AD authentication.	false true ▾
LDAP URL*	The host URL for LDAP authentication.	Example: ldap://localhost:389

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, click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration. Then, 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.
- For role and group attributes to map appropriately to RADIUS attributes, you can either use the Blue Coat VSA custom dictionary file, or manually define attribute strings for attributes that are already configured in your RADIUS server.

- **Blue Coat VSA**

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.

- **Manual attribute definition**

If the RADIUS server in your organization has defined attributes that you would prefer to use, you can choose to define them instead of installing the Blue Coat VSA. Define the attributes for role membership and group membership in

Administration > Settings > RADIUS. If these fields are not populated with a custom attribute name, Management Center will assume that the Blue Coat VSA is in use.

With the group and role attributes defined, Management Center will apply the appropriate roles and/or group membership permissions as users authenticate 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.

RADIUS Settings	Description	Input Value/Format
Is the authenticator enabled*	Enable RADIUS authentication.	false true ▾
Sync the role membership	Specify whether to assign users to roles that match the Blue-Coat-Role VSA or custom attribute.	false true ▾
Role Membership Attribute	Define a custom attribute from your RADIUS configuration to use for role membership. Note: if left blank, Management Center assumes the Blue Coat VSA Dictionary is in use.	string
Sync the group membership	Specify whether to assign users to roles that match the Blue-Coat-Group VSA or custom attribute.	false true ▾
Group Membership Attribute	Define a custom attribute from your RADIUS configuration to use for group membership. Note: if left blank, Management Center assumes the Blue Coat VSA Dictionary is in use.	string

RADIUS Settings	Description	Input Value/Format
User must have permission	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.	false true <input type="button" value="▼"/>

Configure Secondary RADIUS Server

You can also configure a **Secondary RADIUS Server** to take over in case the Primary RADIUS Server fails. The settings under **Secondary RADIUS Server** are specific to the secondary server only.

Secondary RADIUS Server Settings	Description	Input Value/Format
RADIUS IP Address*	The IP Address of the RADIUS server.	default: localhost
Authentication Port*	Port number	<input type="button" value="▼"/>
Accounting Port*	Port number	<input type="button" value="▼"/>
	Note: Even though the Accounting Port is a required setting, Management Center does not supply accounting (or other) data to RADIUS.	
Connect Timeout (seconds)*	Connect retries is the number of times we attempt to connect to the given server before deciding to fail over to the next authentication server. For example, if RADIUS server 1 is set to a Connect Time-out of 10 seconds and 2 Connect Retries, we will try once to connect for 10 seconds and, when/if that attempt fails, we will try one more time (for 10 seconds) to connect. If both attempts fail, we will move on to the next authentication server (e.g., RADIUS 2, LDAP 1, LDAP 2...). But they are not locked out from any of those servers. Upon their next login, we will go through the exact same sequence of authentication servers until one succeeds.	<input type="button" value="▼"/>
Connect Retries:*	The number of attempts the RADIUS server allows before locking you out.	<input type="button" value="▼"/>
Shared Secret:*	Specific RADIUS key or password	Example: RADIUS PASSWORD

Supported RADIUS Servers

Server Types	Configuration Interface	Example User Credentials and Attributes
Steelbelted Note: You must create a RADIUS client for every device that accesses the RADIUS server.	Windows XP VM Note: Restart Windows services after making any modifications.	user1/1resu mcuser1/1resu (FirstName=MC1, LastName=User1) mcuser2/2resu (Role=Role_administrator) mcuser3/3resu (Group=MCAdministrator) mcuser4/4resu (No vendor-specific attributes defined) Important: The group and role attribute values should match the Blue-Coat-Group and Blue-Coat-Role VSAs, respectively.
Safeword	Windows XP VM	user1/password shown on token user2/2resu (fixed password)
RSA	Web - Use Internet Explorer 11 Linux VM	Configure users with a hardware or software token.

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, click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration. Then, 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 and User Groups using Existing Directory Service

You can use your existing directory service to authenticate users that you have previously added to Management Center. Management Center supports integration with Active Directory and LDAP. Authenticating users against LDAP and Active Directory LDAP simplifies user and user

group management because both of those directory services have the concept of group and role membership and can display existing usernames in the Audit Log and metadata.

Management Center supports *authenticating* users from LDAP, Active Directory LDAP and RADIUS directory services.

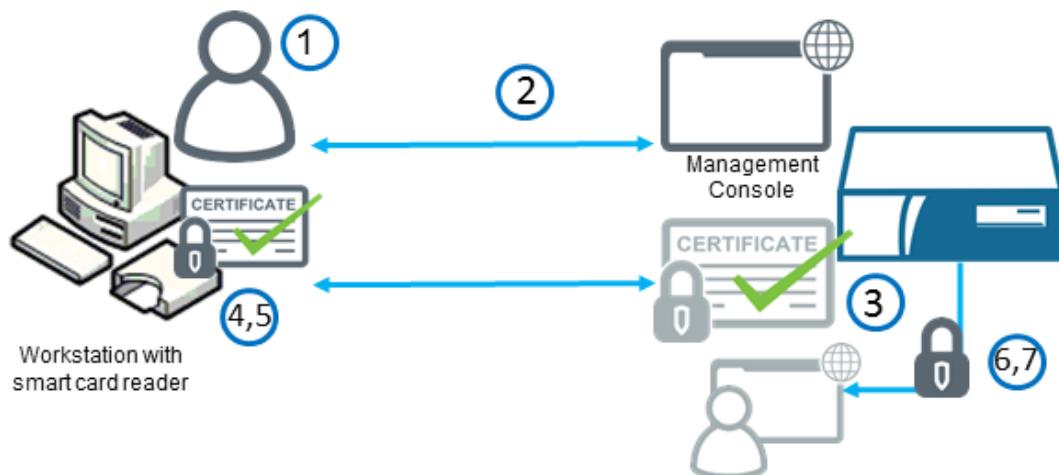
- "Authenticate Users Against LDAP" on page 531
- "Authenticate Users Against Active Directory LDAP" on page 535
- "Authenticate Users Against RADIUS" on page 538

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.



Management Center Configuration & Management

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.

```
# configure
(config)# ssl
(config-ssl)# inline ca-certificate <CA Certificate name>
*** command will prompt for CA contents
(config-ssl)#
(config-ssl)# edit ccl client-authentication
(config-ccl-client-authentication)# add <CA Certificate name>
```

If the device is in FIPS mode, run the following commands instead:

```
# configure
(config)# ssl
(config-ssl)# inline fips ca-certificate <CA Certificate name>
*** command will prompt for CA contents
(config-ssl)#
(config-ssl)# edit ccl client-authentication
(config-ccl-client-authentication)# add <CA Certificate name>
```

2. Verify that the certificate was installed in the CA Certificate List (CCL) with the appropriate command:

```
(config)# ssl view ccl client-authentication
```

See # ssl 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:

```
(config)# security client-authentication set-mandatory
```

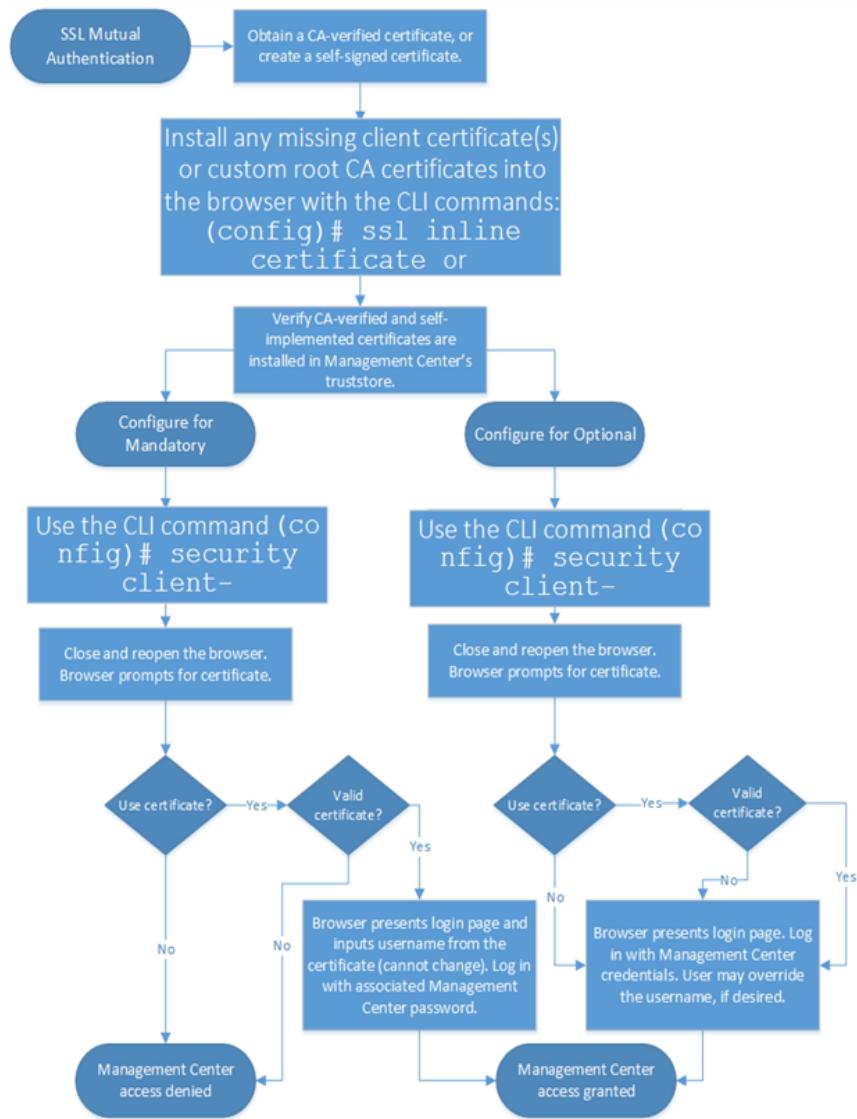
Management Center Configuration & Management

```
(config)# security client-authentication set-optional
```

See # security for more information on the client-authentication commands.

5. Import the client-authentication certificate with its CA chain into the browser. This is the same CA chain you installed in Step 1.

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

Updated for Management Center 2.0.1.1, 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:

```
(config)# security client-authentication password-requirement disable  
(config)# security 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" on page 548 and `# ssl` for more information.

Note: 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)

HSTS protocol support is included to allow web browsers interact with servers using 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`

Note: 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.

Warning: 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

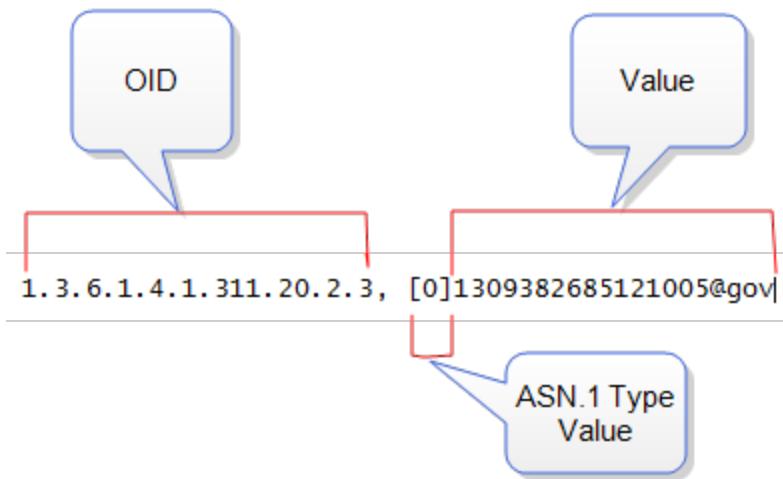
Management Center can search the certificate Subject Alternative Name (SAN) data so that it can be matched against a regular expression to validate the certificate and user. SAN is a X.509 extension that allows data to be associated with a security certificate using a subjectAltName field. SAN data can 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:



The subjectAltName data is compared to a regex set by the `security client-authentication set-regex` command, which is used to extract the portion of the value to use

Management Center Configuration & Management

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 542 for more information.

For example:

```
#security client-authentication set-regex  
"'^1\\\\\\3\\\\\\6\\\\\\1\\\\\\4\\\\\\1\\\\\\311\\\\\\20\\\\\\2\\\\\\3,\\\\\\s\\\\\\[0\\\\\\]  
(.*?)@'"
```

Note: Refer to # security 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 " on the next page
- "Delete a User" on page 552

View User Information

To view user information, expand the **Overview** section.



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.)

Role/Permission ↑	Filter	Inheritance	Actions
administrator	All objects - All op... Report - View	direct assignment All Reporters - All Databases	

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**.

Edit User: John Smith

[Basic Info](#) [Assign Roles](#)

Username: Test2

Password: [Change password](#) [Expire password](#)

Password expired on: 11/29/16 3:56 PM UTC

First Name:	John
Last Name:	Smith
Email:	test@mail.com
Phone:	(555) 555-5555
Mobile:	(555) 555-5555
Description:	New administrator in XYZ, California <small>988 of 1024 characters left</small>

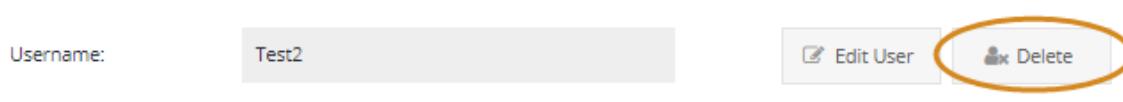
Save **Cancel**

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.

Warning: 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.

Situation	Topic
User knows his/her password and wants to change it	"Change Your Password" on the next page
User forgot his/her password	"Reset Password" on page 556
Admin wants to automate the password resetting process	"Automate Password Reset Process" on page 837
Admin needs to manually change a user's password because user forgot answer to security question or password reset process isn't automated	"Manually Reset a User's Web Console Password" on page 558
Admin wants to expire a user's web console password.	"Expire a User's Web Console Password" on page 558
Admin forgot admin account password	"Reset or Restore Admin Account Passwords" on page 560
Admin wants to change a device password	"Reset or Restore Admin Account Passwords" on page 560

Change Your Password

You can change the password that you use to log into the web console.

Note: 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.



Note: 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.

Tip: 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. The password reset process has the following restrictions:

- It is only good for the web console; it cannot be used for the CLI console.
- It only works for local users; it cannot be used by LDAP or RADIUS users.

Prerequisites

This capability requires that the administrator has enabled the Management Center password reset feature and that users have created a security password. For more information, see "Automate Password Reset Process" on page 837.

How to Reset Password

Tip: 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**.

The screenshot shows the Symantec Management Center login interface. At the top, a message reads: "Please sign in with your Symantec Management Center account credentials." Below this are two input fields: "Username" and "Password". To the right of the "Password" field is a blue "Reset Password" link. At the bottom of the form is a blue "log in" button.

2. Enter your **Username** and click **Next**.

Reset Password: Validate User

Validate User Security Question

Reset Password for User

User: *

Cancel Back Next

You then receive a notification that your password reset request was received.

3. Check your email to find the password reset message.
4. Click the password reset link included in the email. The system displays the **Reset Password** dialog.

Reset Password for Admin2

Security Question

Question: In what city or town was your first job?

Answer: *

New Password

New Password: *

Password Strength: 0%

Retype New Password: *

Change Password

5. Enter the answer to the Security Question, using the exact spelling and upper/lowercase you entered when defining it.
6. Enter a new password, then retype the new password.
7. Click **Change Password**.

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 837.) 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.

Note: 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.

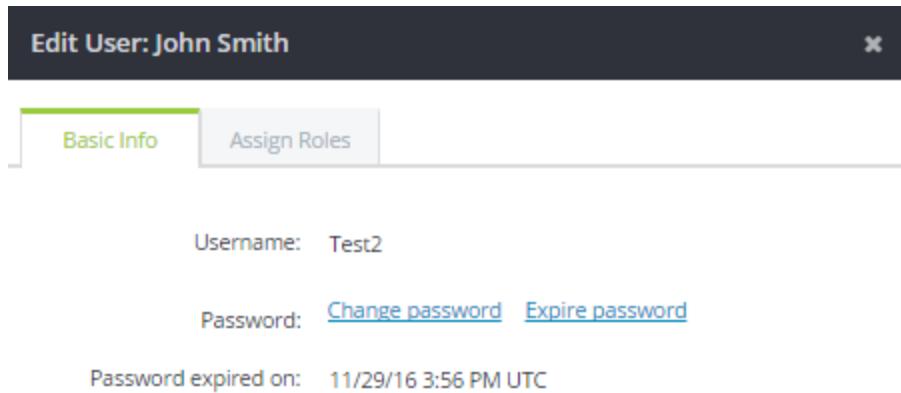
Expire a User's Web Console Password

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.

Note: You cannot expire the password for users authenticated against LDAP, Active Directory, or RADIUS (authenticated users have the following icon: ).

- From the **Basic Info** tab, click **Expire password**. The system displays the expiration time and date.



Edit User: John Smith

Basic Info Assign Roles

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

Management Center 2.1.x

In Management Center 2.1.x or later, the UI and CLI password for the "admin" account are shared. You can change the admin password using the following methods:

- Using the [authentication-password](#) command.
- Using the user interface options:

In the web console banner, click  and select your username.



- With the reset admin account password using the Initial Configuration Wizard via the serial console.

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 563
- "Configure Hierarchy for Devices and Device Groups" on page 103

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.

Note: Groups *cannot* be members of other groups.

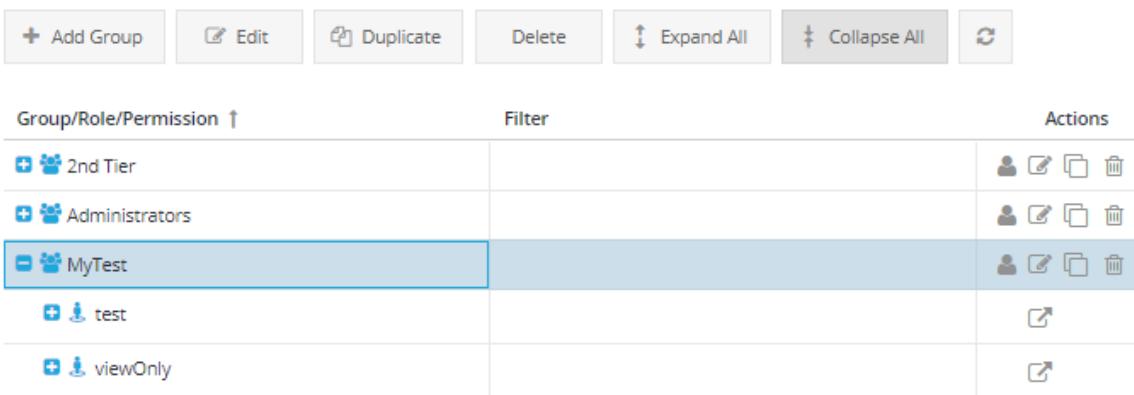
1. Select **Administration > Groups**.
2. From the **Groups** section, click **Add Group**. The web console displays the Add Group wizard.
3. In the **Add Group: Basic Info** page, enter the group's information. An asterisk denotes fields that are mandatory. Enter a Name for your group. This group name displays on the dashboard and other areas in the web console.

Tip: 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).

Tip: 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 567.
8. Click **Finish**. The system displays the the group that you just created in the left pane.



The screenshot shows a user interface for managing groups. At the top, there is a toolbar with buttons for 'Add Group', 'Edit', 'Duplicate', 'Delete', 'Expand All', 'Collapse All', and a refresh icon. Below the toolbar is a table with three columns: 'Group/Role/Permission', 'Filter', and 'Actions'. The 'Actions' column contains icons for edit, delete, and other management tasks. The table lists five entries:

Group/Role/Permission	Filter	Actions
2nd Tier		
Administrators		
MyTest		
test		
viewOnly		

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.

Management Center Configuration & Management

Group	Administrators		
Role	administrator		
Permissions	All objects - All operations Report - View	None	All Reporters - All Databases

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

Group/Role/Permission ↑	Filter	Actions
2nd Tier		
viewOnly		
Administrators		
MyTest		
Testing		

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**.

Note: Deleting a group does not delete any associated members or permissions. They are only disassociated from that group.

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.

User Sessions

User Access

Disable multiple active sessions per user

Disable user login to Management Center (does not affect super admin)

Sessions

Started On	User	Client ...	Last Request Time	Session ID
2017-01-17 15:28:14	[REDACTED]	[REDACTED]	2017-01-17 15:50:1...	[REDACTED]

Define Roles

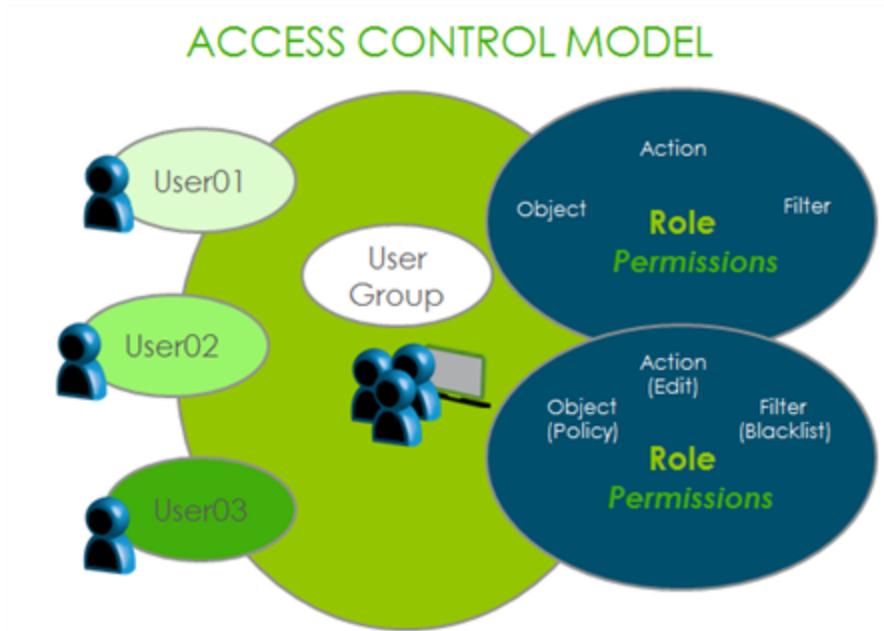
Roles are not necessarily associated with jobs or job titles; rather, each role should contain the permissions required to perform a specific task or set of tasks. Managing roles based on tasks is easier than managing permissions attached to features or functions. Because multiple users in organizations 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 570 and "Duplicate an Existing Role" on page 569.

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.



Tip: 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.

Tip: 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.

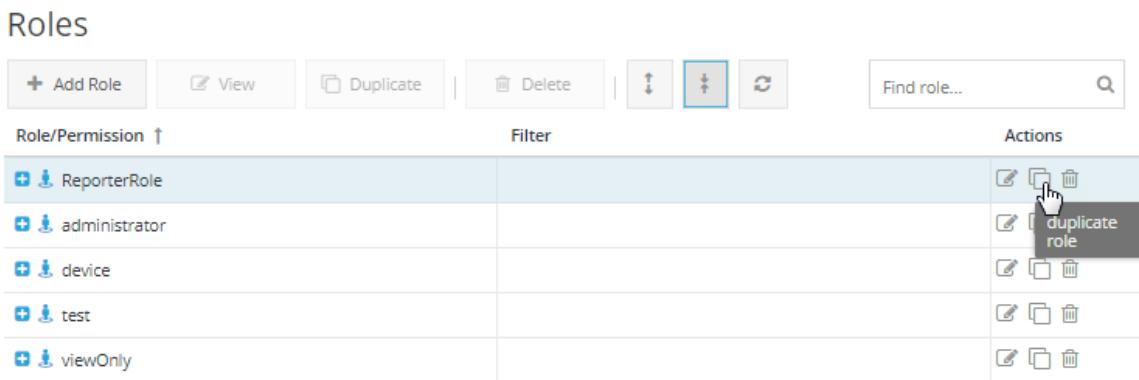
4. Click **Next**.
5. In the **Add Role: Permissions** dialog, click **Add Permission**.
6. From the **Object** drop-down list, select **All objects** or a specific object.
7. From the **Action** drop-down list, select **All operations** or one or more individual actions.
8. (Optional) In the **Filter** drop-down list, select a filter to apply to both the action and the object.
See "Grant Permissions" on page 572 for information on objects, actions, and filters.
9. To add more permissions, repeat steps 6 through 8.
10. Optional: [Add Reporter permissions](#).
11. Click **Finish**.

For information about managing roles, see "Edit an Existing Role" on page 570 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.



The screenshot shows a table titled 'Roles' with the following columns: 'Role/Permission ↑', 'Filter', and 'Actions'. The 'Actions' column contains icons for Edit, View, Delete, and Duplicate. A mouse cursor is hovering over the 'Duplicate' icon for the 'viewOnly' role, which is highlighted with a gray background. The table lists the following roles:

Role/Permission ↑	Filter	Actions
ReportRole		
administrator		
device		
test		
viewOnly		

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 572 for instructions.

- 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](#)

Note: 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.

Roles

Add Role	View	Duplicate	Delete	Actions
ReporterRole				
administrator				
All objects - All operations	None			
Report - View	All Reporters - All Databases			
device				
test				
viewOnly				

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 499. 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 575.
5. Add or remove an existing permission:
 - To add a permission, click **Add Permission**. See steps 7 through 10 in "Define Roles" on page 567 for instructions.

- To remove a permission, select it and click **Remove Permission**. The permission is removed from the list.
6. Click **Save**.

Note: 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 566.

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 575.

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.

Note: 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 567 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 570.

Update a User's Roles

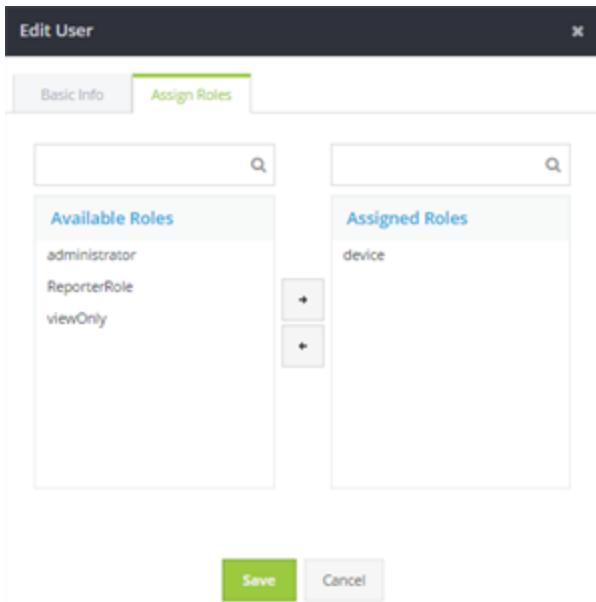
When a user has a new job or responsibilities within the organization, you might have to update their roles to ensure that they can perform their new tasks.

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:



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.

Note: 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 589 for information.

1. Perform one of the following:
 - Add a permission. See "Grant Permissions" on page 572.
 - Edit a permission. See "Edit an Existing Role" on page 570.
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" on page 513.
4. Click **Save**. The filter displays in the Filter field.

Restrict Access to Reporter Reports and Data

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. You can also restrict access at the dashboard level, allowing access to reports but filtering out data the role should not have access to.

1. Select **Administration > Roles**.
2. Select a role and click **Edit**.
3. Click the **Reporter Permissions** tab.
4. **Click Add Permission**.

The screenshot shows the 'Edit Role: test' dialog. The 'Reporter Permissions' tab is selected. Below it are three sections: 'Reporter-Database' containing 'All Reporters - All Databases', 'Restricted Fields' (empty), and 'Affected Reports' (empty). At the bottom are 'Save' and 'Cancel' buttons.

5. Select the Reporter database to apply permissions to.

The screenshot shows the 'Assign Reporter Database' interface. A dropdown menu is open, showing 'All Reporters - All Databases' as the selected option. Other options include 'Device - All Databases' and 'Device - ProxySG - WTL Office'. A note at the bottom states: '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.'

Note: 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. This action excludes reports that match the fields. (You can also allow access to reports while filtering out desired data. See step 9).

Select a report field to prevent this role from viewing the selected report information. Show screen.

Restricted Fields, Reports

Select restricted metrics (certain reports will be hidden)

Show Restricted Reports Restrict All Restrict None

<input type="checkbox"/> Action	<input type="checkbox"/> Category	<input type="checkbox"/> Client IP
<input type="checkbox"/> Day	<input type="checkbox"/> Day of Week	<input type="checkbox"/> Hour of Day
<input type="checkbox"/> Malware	<input type="checkbox"/> Method	<input type="checkbox"/> Month
<input type="checkbox"/> Protocol	<input type="checkbox"/> Risk Score	<input type="checkbox"/> Search Term
<input type="checkbox"/> Server IP	<input type="checkbox"/> Site	<input type="checkbox"/> User
<input type="checkbox"/> User Agent	<input type="checkbox"/> Verdict	<input type="checkbox"/> Web App Operation
<input type="checkbox"/> Web Application		

8. **To view the reports affected by your choices, select Show Restricted Reports.**

Restricted Reports by Field		
Restricted Fields ↑	Restricted Reports	Action
Action	Actions	
Day of Week	Bandwidth per Day of Week Cost per Day of Week Days of Week undefined	Allow
Month	Bandwidth per Month Cost per Month Months	Allow
Search Term	Search Terms	Allow
User	Blocked Requests by User Blocked Users Categories per User Cost per User Cost per User and Site Facebook Users	Allow

Close

When you are satisfied with your choices, click **Close**.

9. Restrict report data using a database filter. This action allows access to reports you have not restricted but removes data according to the fields specified in the filter. To begin, specify a database and then add one or more filter criteria.

Note: If you select All Selected Databases, the system does not provide a filter search and you must manually enter the filter criteria. Ensure that you are entering the criteria as it is worded in the report.

Here are several examples of filters you can create:

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.

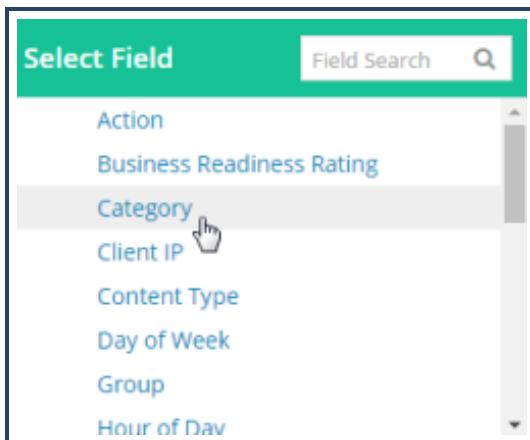
For each filter you want to add, follow the steps below.

Note: If users have report permission filters that apply to the role they're using to run the report, they will not be able to filter on any fields specified in those permission filters unless the Reporter is running 10.5 or higher.

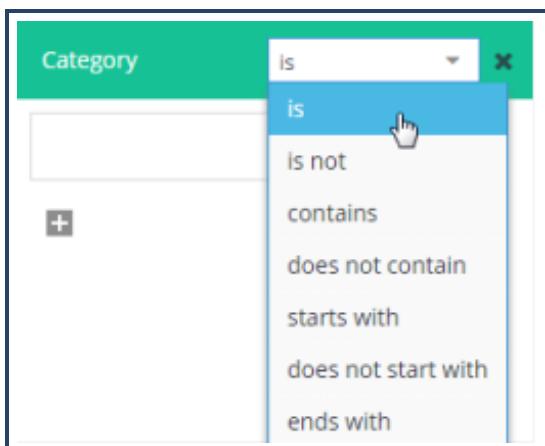
1. In the Filters section, click Add Filter.



2. Select a field.

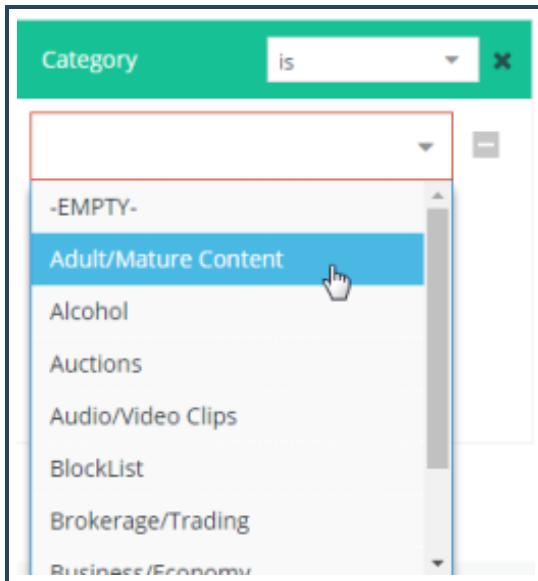


3. Select the appropriate operator. The available operators change depending on the selected field.



4. Select or enter a value.

Management Center Configuration & Management



10. Click **Finish**, then **Save**.

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.



Manage 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 describe devices, device groups, policy, and scripts. Attributes can also be used to filter on specific devices, device groups or objects.

About Attribute Inheritance

You can designate device and device group attributes as "inheritable." Attributes that are checked as inheritable can "inherit" their attributes from a parent device group.

Configure Device Group Inheritance

If you want a group to inherit an attribute's value, you must use a *device attribute*. (Group attributes are used only to add additional meta-data to a group.) To enable group inheritance, see "Enable Attribute Group Inheritance" on page 165. Group hierarchies can also affect inheritance. See "Configure Hierarchy for Devices and Device Groups" on page 103.

Work With Attributes

- "Add Attributes" on the next page
- "Edit Attributes" on page 587
- "Add Device Group Attributes" on page 164
- "Set User-Defined Device Attributes for Access Control" on page 589
- "Filter and Keyword Search" on page 594

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.

Add Attributes

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.**

Add Attribute

Display Name: *

Name: *

Type: * String

Format: * Text

Min Length: * 0

Max Length: * 50

Default Value:

Mandatory
 Inheritable
 Displayed as a default column

Description:

1024 of 1024 characters left

Save **Cancel**

Property	Description or Purpose
Display Name (*)	Name that displays throughout Management Center.
Name (*)	This is the name with no spaces.
Type (*)	Select the data type used for the attribute.
Tip: See "Hide Attribute Value" on page 590 for more information on the Encrypt attribute type.	
Format (*)	Select the format used for String attribute types. For example, Email or Phone .
Available Values (*)	Display, add, or delete available values for the Picklist attribute type.

Property	Description or Purpose
Min Value and Max Value (*)	Specify a minimum or maximum value for the String or Decimal attribute type. The system will not allow attribute values that do not meet or exceed these values.
Default Value	If the attribute has a default value, it is displayed here.
Mandatory	<ul style="list-style-type: none"> ■ All attributes that you check as mandatory will appear as options when you create a new policy, device, device group, or device script. When creating the new object, you must enter a value for the mandatory attribute. ■ Nothing changes to the existing devices, device groups, policy, or scripts when an attribute is marked mandatory. ■ All mandatory attributes can be filtered on when you "Filter by Attributes and Keyword Search" on page 256. ■ 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 312
Inheritable	This attribute applies to devices and devices groups. Attributes that are checked as inheritable can "inherit" their attributes from a parent device group.
Displayed as a default column	When enabled, the attribute displays as a column in the Policy Object grid, Script Object grid, or Network dashboard. Even if this option is not enabled, you can still display the attribute by right-clicking the column header, selecting Columns and selecting the attribute to display. See "Customize the Network View" on page 54.
Description	Give a useful description of this attribute to distinguish it from the others when viewing all of the attributes in a list.

4. Click **Save**.

Note: You are able to search for specific objects based on the attributes you define. See "Filter by Attributes and Keyword Search" on page 256.

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.

Property	Description or Purpose
Display Name (*)	Name that displays throughout Management Center.
Name (*)	This is the name with no spaces.
Type (*)	The format in which users must enter or select attribute values.
Available Values(*)	The Available Values depend on the Type you selected.
Default Value	If this attribute has a default value, it is displayed here.
Mandatory	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 "Filter by Attributes and Keyword Search" on page 256.
Inheritable	This attribute applies to devices and devices groups. Attributes that are checked as inheritable can "inherit" their attributes from a parent device group.

Management Center Configuration & Management

Property	Description or Purpose
Displayed as a default column	When enabled, the attribute displays as a column in the Policy Object grid, Script Object grid, or Network dashboard. Even if this option is not enabled, you can still display the attribute by right-clicking the column header, selecting Columns and selecting the attribute to display. See "Customize the Network View" on page 54.
Description	Give a useful description of this attribute to distinguish it from the others when viewing all of the attributes in a list.

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 103.
 - **Attributes** - Customized Location and Rack attributes or new custom attributes (or metadata) that administrators can create. See "Add Attributes" on page 584.
1. Collect statistics for the device by clicking the check box. See "View Statistics Monitoring Reports" on page 732.
 2. Use the up/down arrows to specify a Bandwidth Cost. "Set Bandwidth Cost for Reports" on page 756.

Note: 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.

Tip: 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 584 and "Edit Attributes" on page 587.

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 513.

Hide Attribute Value

There may be times when you do not want the value of an attribute to be shown in policy or scripts. For example, the attribute might contain a device password that should be kept confidential. Management Center provides an **Encrypt** attribute type for these situations.

The encrypted data is stored on Management Center. It is decrypted only when sending to the device.

Encrypted Attribute Feature Limitations

When using encrypted attributes, be aware that the attribute might be visible in some situations. For example:

- If you include the encrypted attribute in a script and do not structure the script properly, or you include the attribute in a place the device does not expect, the target device can "echo" the plain text value of the attribute in its response.
- If you attempt to install policy that includes an encrypted attribute and the policy installation fails because of a syntax error with the attribute, the target device provides the plain text value of the attribute in the resulting error message.
- If you install the policy to the target and then compare the policy versions, the value of the attribute will be visible in the comparison that shows the policy currently installed on the device.

Because of this, use discretion when assigning permissions for executing policy or scripts.

Add Encrypted Attributes

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.

4. Define the properties of the attribute that you are creating. To hide the value, set the Type to Encrypt. An asterisk denotes fields that are mandatory.

Add Attribute

Display Name:	*	GSM
Name:	*	GSM
Type:	*	Encrypt
Format:	*	Alphanumeric
Min Length:	*	0
Max Length:	*	50
Default Value:	*****	
<input type="checkbox"/> Mandatory		
<input checked="" type="checkbox"/> Inheritable		
<input type="checkbox"/> Displayed as a default column		
Description:	1024 of 1024 characters left	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

You'll notice that you can't even view the value while entering it in the **Default Value**. To ensure the accuracy of your entry, you might want to enter the text elsewhere and cut and paste it into this field.

Note: The **Encrypt** attribute type has the same options as the **String** type. However, it is not meant for long, multi-line strings and does not include an expanded editor.

Note: See "Add Attributes" on page 584 for a description of these properties.

5. Click **Save**.

Verifying Encrypted Attributes

After you've added the attribute, you should see a message indicating the value is *****MASKED*****.

Device Attributes

Name	Display Name	Type	Default Value
Location	Location	String	
Rack	Rack	String	
SG4_PW	SG4_PW	Encrypt	***MASKED***

If you subsequently add the attribute to policy or to a script, you cannot view the value in previews.

```
▲ default
<Proxy>
condition=blacklisted_categories DENY
${device.attributes.SG4_PW}
```

Preview

```
1 <Proxy>
2 condition=blacklisted_categories DENY
3 ***MASKED***
```

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.

Tip: 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).

Note: 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.

Note: 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 "0:0:0:0:0:1"

Tip: 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

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.

Name	Type	Description
localhost_access.log	WEB-ACCESS	<p>Tracks user requests to the Management Center UI.</p> <p>These logs roll over weekly for a maximum of 4 weeks.</p>
log.log	WEB	<p>Primary Management Center log.</p> <p>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.</p>
debug.log	DEBUG	<p>This log provides diagnostics information to help with debugging.</p> <p>The log only displays if a user enables debug diagnostics (Administration > Settings > Diagnostics).</p> <p>The DEBUG logs roll over when it reaches 10 MB and maintains a maximum of 9 history logs for a total of 1 GB.</p>
journal.txt	PDM	<p>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.</p> <p>These logs roll over weekly for a maximum of 4 weeks.</p>
device.log	SYSTEM	<p>Internal CLP OS log.</p> <p>These logs are very small and roll over every day for a maximum of 30 days.</p>

Name	Type	Description
clp_services.log	SYSTEM	<p>Internal CLP OS log.</p> <p>These logs are very small and roll over every day for a maximum of 30 days.</p>

Other Logs

Other logs include the following:

- Debug logs for each type of device. For example, cas.log.
- Rollover logs. Their formats are similar to the following:
 - *name.zip*
 - *name.log-data*

Log Types

The following table describes the log types.

Type	Description
WEB	Logs related to Management Center and its operation.
WEB-ACCESS	Logs that track user requests to Management Center web UI.
DEBUG	As the name implies, these are debugging logs.
SYSTEM	Internal core OS logs.
PDM	Performance Data processing logs. These correspond to anything related to the appstat processing of PDM logs from the ProxySG or other systems.

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.

Note: Scheduling a job and running an operation require different permissions. See "Reference: Understanding Job Permissions" on page 517.

1. Plan the job:
 - Determine which operation you want to create a job for. See "Job Operations" on page 648.
 - 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 637.
2. Create the job. See "Add a Job" below.
3. Monitor scheduled jobs, and run unscheduled jobs as needed. See "Monitor Jobs" on page 640.
4. Monitor jobs as they are running. See "View Current Jobs" on page 642.
5. View job history. See [Job History](#).

Add a Job

This page describes how to add a job using the **Jobs > Scheduled Jobs > New Job** page.

Note: You can also perform [operations](#) on individual device, [share jobs](#) with another Management Center, or organize jobs in [folders](#).

Composite Jobs

[Multistep Device Job](#)

[Multistep Job](#)

Device Management

[Backup Device](#)

[Change Monitoring State](#)

[Collect Certificates](#)

[Collect SysInfo](#)

[Compare Config](#)

[Export Backups](#)

[Factory Restore Device](#)

[Install System Image](#)

[Reactivate Statistics Monitoring](#)

[Restart Device](#)

[Save Config](#)

[Set Boot Image](#)

Policy and Configuration

[Check Consistency](#)

[Execute Script](#)

[Import External Policy](#)

[Install Policy](#)

[Remove Unused Policy](#)

[Synchronize Devices](#)

Reports

[Reporter Report](#)

[SWG-VR Data Collection](#)

[Statistics Monitoring Report](#)

[Schedule Summary Report Job](#)

System Management

[Backup Management Center](#)

[Schedule File Transfer](#)

Add Job That Includes Multiple Jobs (Multistep Job)

A Multistep Job is a job that includes other jobs you have previously created. The jobs are run in sequence on the target devices specified in each job. This means that you could run a job on a Content Analysis device and a different job on a ProxySG device. You cannot assign target devices while creating a Multistep Job.

If one of the jobs fails, you can continue to execute the rest of the jobs or configure the Multistep Job to abort.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Multistep Job**.
3. **Child Jobs:**
 - Select the jobs to add to the execution list, then click **OK**.
 - Use **Remove**, **Move Up**, and **Move Down** to edit the available jobs and their execution order.

- 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.

Note: Only single jobs are available to embed into a multistep job. To include several job operations in a single job, see "Add Job That Includes Multiple Operations (Multistep Device)" on the facing page.

4. Job Results:

- Optional—Click **Email results** and select the condition. Then, enter the email(s) of the recipient(s).

5. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. Name:

- Verify or change the name and add an optional description.

Add Job That Includes Multiple Operations (Multistep Device)

The Multistep Device Job (**Jobs > Scheduled Jobs > New Job > Multistep Device Job**) enables you to create a job that runs one or more operations on each target device. This is in contrast to the [Multistep Job](#), which is a job that contains other discrete jobs.

Tip: Use the Multistep Device Job when you want to run operations on multiple devices of the same type. Though a Multistep Device Job can have disparate device targets, all of the operations in the job must be supported by those device types.

Using the Multistep Device Job, you can specify the behavior to occur if a job operation encounters errors. If an operation fails, you have the option to force the job to continue on that device or specify a global recovery action.

Behavior

All operations are run in sequence on each target device. All of the selected operations must be able to be performed on the target device type. For example, if one of the job operations is to collect Sysinfo, you cannot add a Content Analysis (CA) device target because Sysinfo is supported only for ProxySG devices. The system filters out devices that do not support one or more operations in the job. Therefore, if you have mixed device targets, ensure you only add operations that are supported by those devices.

If an operation is marked **Continue on Error**, the job will continue to run even if that operation fails. If you specify a **Recovery** action, that action will be invoked when any operation in the job fails unless the operation is marked **Continue on Error**.

Add Multistep Device Job

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Multistep Device Job**.
3. **Operations:**
 - Click **Select Operation** to add a job operation. Click **Add another operation** to add additional job operations.
 - See "Add a Job" on page 600 for additional information about each option.
 - Use **Remove**, **Move Up**, and **Move Down** to edit the available jobs and their execution order.
 - For each operation, decide whether to continue on error. Click the gear icon and select **Continue on Error**.
 - If you add an **Install Policy** job, specify whether to always install the latest version or a specific version.

Tip: If you've added a lot of operations, save the job and then edit it. When you bring up the editor, all operations will be collapsed, allowing you to view them more easily.

4. Recovery:

- Optional—Specify one or more actions to take if one of the operations fails. For example, you can choose to collect Sysinfo for a ProxySG appliance if an operation fails.

This is a global setting that is used when an operation fails on any of the targets. However, the **Recovery** action will not occur if an operation is marked **Continue on Error**.

5. Targets:

- Select the **Devices** or **Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

6. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

7. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the next page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

8. Name:

- Verify or change the name and add an optional description.

9. Click **Save**.

Example

John Smith's company has several devices, including ProxySG, Content Analysis (CA), and

Malware Analysis (MA) appliances. He creates a Multistep Device Job that includes the following operations:

- Backup
- Install Policy
- Collect Sysinfo
- Restart

John wants the operations to continue even if the backup fails, so he clicks the gear icon in the Backup operation and selects **Continue on Error**.

He has also selected **Monitor/Unmonitor** for the **Recovery** operation, and has configured that option to deactivate the target device if an operation fails.

John continues the job configuration and notices that the **Targets** list does not display his CA and MA appliances. This is because those devices do not support the **Sysinfo** operation.

John completes the job configuration and saves and runs the job. As the job executes, John watches the status of each operations as it runs. The backup operation fails but the job continues to run because he had marked that operation **Continue on Error**. The rest of the operations run successfully. Even though the backup operation failed, the **Recovery** action was never invoked because the Backup operation was marked **Continue on Error**. He remembers that the **Recovery** action only occurs for operations that fail and that are not marked **Continue on Error**.

Collect Sysinfo

The **Collect Sysinfo** job 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 **Jobs > Archived Files** as a zip file.

Tip: This job requires that **Email Results** or **Generate Archive** is selected to save the result.

1. Select **Jobs > Scheduled Jobs > New Job** and click **Collect Sysinfo**.
2. **Targets:**

- Select the **Devices** or **Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

3. Job Results:

- Click **Email results** and select the condition. Then, enter the email(s) of the recipient(s).

4. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- Device added to Management Center
- Device added to Group
- Device removed from Group

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

5. **Name:**

- Verify or change the name and add an optional description.

6. Click **Save**.

Restore Device to Factory Defaults

This job executes a partial reset to factory defaults; the network settings are not lost and the connection to the device CLI is preserved. This job is supported only on the following devices:

- ProxySG appliance
- Advanced Secure Gateway

Factory Restore Device Job

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Factory Restore Device**.
3. **Configuration:**

- Select this option to wait for the device to restart before reporting job success.

4. Targets:

- Select the **Devices or Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

5. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).

6. Schedule:

Note: Symantec recommends that you only run ad-hoc jobs for this option. Do not schedule a factory restore job or trigger it with an event.

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job

- **Periodic**—runs the job every *x* number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. Name:

- Verify or change the name and add an optional description.

8. Click **Save**.

Schedule Device Restart

If you need to reboot a managed device, use the following procedure to restart it. You can also restart a device from the Network page (**Network** > *select device* > **Operations**).

Note: See also, "Restart a Device" on page 95.

1. Select **Jobs > Add > New Job**.

2. On the **Add New Job** page, select **Restart Device**.

2. **Configuration:**

- Select this option to wait for the device to restart before reporting job success.

3. **Targets:**

- Select the **Devices** or **Groups** tab.
- Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
- Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
- If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
- All selected targets appear in **Selected Targets**.

4. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).

5. **Schedule:**

- Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job

- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. Name:

- Verify or change the name and add an optional description.

7. Click **Save**.

Save Device Configurations

The **Jobs > Save Config** job saves the configuration settings of a managed device. You can use the **Save Config** job to create a "golden" configuration to be used for comparison with other devices (**Jobs > Compare Config**). The job results are saved to the archive (**Jobs > Archived Files**).

The resulting configuration is saved in JSON format and should only be used with the **Compare Config** job to identify configuration differences. See "Compare Device Configurations" on page 96 for more information.

Supported Devices

The **Save Config** job supports the following devices:

- ProxySG appliance
- Advanced Secure Gateway
- Content Analysis
- SSL Visibility 4.x
- Malware Analysis

Save a Device Configuration

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Save Config**.

Configuration:

- Select the device type.
- Enter the JSON paths to include or exclude, or select individual configuration sections. Use hard returns to enter multiple JSON paths.

If you are not familiar with the JSON paths available in your device configuration, select all of the sections. Then, run the job and view the saved configuration file to determine if additional filtering is required. JSON paths are entered using standard JSON path expressions. For example, enter `$.Policy` to specify the Policy node at the root level.

The JSON paths you enter override in the **Paths to Include** section overwrite any of the selected categories. For example, if you enter `$.Auth` and have selected **Tenants**, **Policy**

Slots, and **PKI** in the **Sections to Compare**, only the **Auth** configuration will be saved. All categories are ignored.

If you enter one or more JSON paths in the **Paths to Exclude** section, the checkboxes in **Sections to Compare** are used, with the exception of any specified in the **Paths to Exclude**.

3. Targets:

Select the devices or groups for which you want to save configurations. The selected devices must be running the same system image as the source device.

- Select the **Devices** or **Groups** 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**.

4. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the next page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time

Management Center Configuration & Management

- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

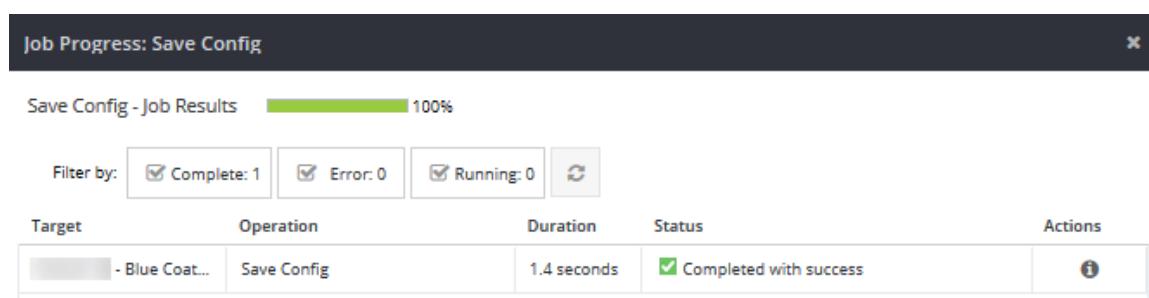
Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. Name:

- Verify or change the name and add an optional description.

7. Click **Save**.

The system displays the job progress.



View Job Results

To view the job results:

1. Select **Jobs > Archived Files**.
2. Select the job and click **Download**.
3. Locate the JSON file downloaded by your browser and view it using a text editor.

Schedule Reporter Reports

The reports scheduling feature enables you to create scheduled jobs. Some complex reports may take several hours to execute and you can schedule these reports to run during non-business hours. You can also use these features to email a report to users who cannot log into Management Center. Or you could schedule a monthly report that emails the results to interested stakeholders.

This feature creates a scheduled job whose results can be viewed in the **Jobs > Job History** page. All scheduled job reports are saved to the Management Center file archive for later viewing.

- Schedule reports from any of the following pages:
- **Reports > Reporter**: Select a job and click **Operations > Schedule**.
- **Reports > Reporter > ReportName**: Run a report and save it if necessary. Click **Actions > Schedule**.
- **Jobs > Scheduled Jobs > New Job**: Select **Reporter Report**.

Note: For additional information about these fields, see "Create a Custom Reporter Report" on page 708.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Reporter Report**.
3. **Configuration**:
 - **Database**: Select the Reporter database to use.
 - **Report period**: Specify the date range.
 - **Format**: Select the format, PDF, HTML, or CSV.

Note: By default, the reports have a Symantec logo. You can [replace that with your logo.](#)

- **Page Orientation:** For PDF, select the orientation, **Portrait** or **Landscape**. (This is not applicable to HTML or CSV.).
- **Report Rows:** Select the number of rows you want included in the offline report.
- **Description:** Enter a meaningful description to help you identify or find this job later.

4. Reports:

- Select the reports to run. For more information about the reports, see "Reference: Report Descriptions" on page 691.

5. Job Results:

- (Optional)—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).

6. Schedule:

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time

- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. Name:

- Verify or change the name and add an optional description.

8. Click **Save**.

Note: To run a report in the background for later viewing, see "Run a Reporter Report in the Background (Or to Archive)" on page 689. To run a report immediately, see "View a Reporter Report" on page 674.

Schedule SWG-VR Data Collection

The SWG-VR data collection is used to capture specific information associated with the Value Reporting service offered by Symantec. This job captures specific information from the ProxySG appliances attached to a Reporter instance and returns a payload suitable for emailing to your SE for analysis. Consult with your SE for more information on this service. This job saves the report as an archived file (**Jobs > Archived Files**).

Note: This operation is not supported in Multistep Device Jobs.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **SWG-VR Data Collection**.
3. **Reporter:**
 - Specify the Reporter to collect the data from. Select **Registered** if the device is managed by Management Center or **Unregistered Reporter** to specify the connection details for another Reporter instance.

Note: Use **Not Registered** if using Reporter 9.x or higher.
Manually enter the credentials to connect.

4. **Job Results:**
 - (Optional)—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).
5. **Schedule:**

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time

- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. Name:

- Verify or change the name and add an optional description.

7. Click **Save**.

Schedule Statistics Monitoring Reports

Use this procedure to create a job to schedule or run one or more statistics monitoring reports. For more information about the reports see "Reference: Statistics Monitoring Reports in Management Center" on page 736.

Note: You can also schedule or run statistics monitoring reports from the Statistics Monitoring page. See "View Statistics Monitoring Reports" on page 732.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Statistics Monitoring Report**.
3. **Configuration:**
 - **Report period:** Specify the date range.
 - **Format:** Select the format, PDF, HTML, or CSV.

Note: By default, the reports have a Symantec logo. You can [replace that with your logo](#).

- **Page Orientation:** For PDF, select the orientation, **Portrait** or **Landscape**. (This is not applicable to HTML or CSV.).
4. **Reports:**

- Select the reports to run. For more information about the reports, see "Reference: Statistics Monitoring Reports in Management Center" on page 736.

5. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).

6. **Schedule:**

Choose to trigger job execution using a "Schedule" below or an "Event" on the facing page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job

- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. Name:

- Verify or change the name and add an optional description.

8. Click **Save**.

Statistics monitoring reports are saved to **Jobs > Archived Files**. You can also download the report from the Job Progress dialog.

Schedule Summary Report Job

Management Center enables you to run a Summary Report that provides value-specific information on various security planning, monitoring, and compliance of corporate KPIs.

Use the Summary Report to drill down into the database to find specific information based on the inventory, health, user activity, license state, data from statistics monitoring, and/or device details necessary.

Note: This operation is not supported in Multistep Device Jobs. See also "Run a Summary Report" on page 685.

1. Select **Jobs > Add > New Job**.

2. On the **Add New Job** page, select **Summary Report**.

3. **Report Details:**

- Cover Title: Provide a title for the Summary Report.
- Page Header: Provide an optional page header for the report.
- Report Period: Specify the time period.

Note: By default, the reports have a Symantec logo. You can [replace that with your logo](#).

4. **Report Content:**

- Sections: Specify the report segments to include. For more information, see "Run a Summary Report" on page 685.
- Database: Select the database from which to run the report. The database is only required for some sections and is inaccessible for the others.

5. **Archived File:**

- Change the filename of the archived PDF, if wanted. This is automatically populated by what you enter for the Cover Title.

6. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address (s) of the recipient(s).

7. **Schedule:**

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

8. Name:

- Verify or change the name and add an optional description.

9. Click **Save**.

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 Management Center" on page 811.

Important Backup Notes

Backups are not compatible or transferable between FIPS and Non-FIPS mode, for the following reasons:

- Encryption differences between FIPS/Non-FIPS mode.
- Non-FIPS backup cannot be restored to FIPS appliance without omitting certain backup portions.

Backup Requirements

Backing up the Management Center configuration requires specific permissions. See the topic Understanding Job Permissions in the Management Center Configuration and Management Guide.

Additionally, sensitive data in the backup will be encrypted with an encryption key. As of Management Center 2.0, this encryption prevents anyone from accessing the contents of backup files outside of Management Center.

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.

Note: This operation is not supported in Multistep Device Jobs.

1. Select **Jobs > Add > New Job**.

2. On the **Add New Job** page, select **Backup Management Center**.

3. **Configuration:**

- 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. - 1 or more characters, alphanumeric.
 - **Username**
 - **Password**
- (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.

4. **Job Results:**

- (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. **Schedule:**

Choose to trigger job execution using a "Schedule" below or an "Event" on the next page.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job

- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. Name:

- Verify or change the name and add an optional description.

7. Click **Save**.

Caution: 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 Command Line Interface (CLI)" on page 873.
2. Enter privileged mode. See Privileged Mode Commands.
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 ..
Completed backup, Wed Apr 3 11:01:33 CMT 2018.
```

Schedule File Transfer

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.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **File Transfer**.
3. **Configuration:**
 - **Server URL:** Enter the URL of the file. Supported protocols include http/https.
 - **File Type:** Specify the file type.
 - **If the file already exists:** Choose what to do if the file already exists.
4. **Job Results:**
 - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).
5. **Schedule:**

Choose to trigger job execution using a "Schedule" below or an "Event" below.

Schedule

Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.

- **Immediate**—automatically runs the job after it is created
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
- **Run Once Only**—specify the date and time to run the job
- **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date
- **Daily**—runs the job every day at the specified time
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day

See also "Job Scheduling Options" on page 637.

Event

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See note below.

Note: If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. Name:

- Verify or change the name and add an optional description.

7. Click **Save**.

Share a Job With Another Management Center Appliance (Export/Import)

In some cases, you might want to share jobs you have created with another Management Center. You can do this by exporting the job(s) from the source Management Center and importing the job(s) on the target Management Center.

Exported jobs are saved in JSON format to allow another Management Center to import the job(s).

Important Export/Import Notes

- Symantec strongly recommends that you sync the Management Center "source" appliance's shared objects, policy and script objects, source devices, and so on, with all other Management Center appliances you are sharing jobs with. This is because job imports can fail if shared objects or source devices do not exist on the target Management Center appliance.
- Job data is exported by reference. The operation does not export full objects, for example, an entire script or policy. The system includes sufficient information to match an object with its counterpart on the target device, if it exists. If the counterpart does not exist, the import might fail. See previous bullet.
- Exported policy and script objects must have a reference ID. If they do not, they will fail to export.
- The jobs listed below may require a passphrase if they include sensitive data. For example, if a SWG-VR job contains a registered Reporter, it will not require a passphrase. But if the job contains an unregistered Reporter, a passphrase is required. The passphrase must be provided upon import so the data can be decrypted and re-encrypted by the target Management Center.
 - **SWG-VR**
 - **Import External Policy**
 - **Backup Management Center**
 - **Export Backups**

If you forget a passphrase, you will need to export the jobs again.

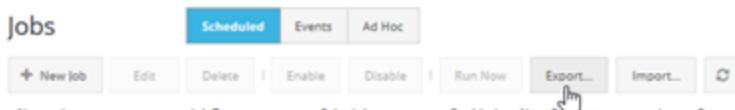
- Reporter Jobs with Role Permissions—If a report job has a server-database-role selection, you must verify the role name and associated permission. Management Center does not check the role permissions when importing or exporting. It imports/exports the Reporter device information, database name, and role name only.
- **Multistep Device Job**—If any step fails to export, the entire job will fail to export.
- **Multistep Job:**
 - If any subjob fails to export, the subjobs will still be exported—even if the Multistep Job fails. This also applies to imported Multistep Jobs.
 - If a **Multistep Job** is selected without selecting its subjobs for export or import, Management Center still tries to export/import all subjobs in the Multistep Job.
- **Execute Script**—If any script cannot be found, the Job will fail.

Step 1: Export Management Center Job

Exporting one or more jobs is the first step in sharing the job with another Management Center appliance. When you export the job, the system saves it as a JSON file on your local client. To export one or more Management Center jobs:

1. Review the "Important Export/Import Notes" on the previous page.
2. Select **Jobs** and click **Export**.

Note: If you select jobs in the Jobs list before clicking **Export**, those jobs will already be selected in the Export wizard.



3. In the Export Jobs window, select the jobs you want to export. If any job requires a passphrase, you will see a text box to enter the passphrase.

4. Enter the passphrase(s) if required and click **Next**.
5. Review the Export Results and click **Download**.

Note: If a job exports with errors, it is not included in the JSON file. Jobs exported with warnings are retained.

Step 2: Import Management Center Job

After you have exported jobs from the source Management Center appliance, you can import them onto a different Management Center appliance.

1. Review the "Important Export/Import Notes" on page 632.
2. Select **Jobs** and click **Import**.



3. In the Import Job File window, drag and drop the exported JSON files or click **Browse** to select them.
4. If any of the imported jobs requires a passphrase, enter it and click **Next**.
5. The system runs a simulated import to determine if the jobs can be successfully imported.
6. In the Choose Jobs window, review the results of the **Success** tab.
If a job with the same name already exists, the system prompts you to update an existing job or to create a new job.
7. Review the results in the **Error** tab, to determine if you can fix the problems.

The system displays the number of errors. Click the + symbol to expand the error description. Record the errors, and if necessary, exit the Import to fix the problems.

Errors can be caused for a number of reasons, including an incorrect passphrase. For example, if a job lists source devices that are not present on the Management Center,

you will have to add those devices before the import will succeed. If target devices are missing, the import will succeed if there is at least one valid target. See "Important Export/Import Notes" on page 632 for more information.,

8. After reviewing the errors and making the appropriate changes, ensure that **Import Job** is selected for each job you want to import and click **Next**. The system now imports the selected jobs.
9. Review the results of the import and click **Finish**.

Reference: How Objects are Referenced

The following list describes the exported data that is used to look up objects on the target device. It is not a comprehensive list of everything exported.

Job	Exported Data	Notes
Device	<ul style="list-style-type: none"> ■ Name (for informational purposes only, not used for lookup) ■ Serial number ■ Type ■ IP Address ■ Port 	
Device Group	<ul style="list-style-type: none"> ■ Hierarchy name ■ Group path from the selected group up to the base group 	The system matches this against the full path and hierarchy on the target device.

Job	Exported Data	Notes
Policy	<ul style="list-style-type: none"> ■ Name ■ Reference ID ■ Content type ■ Version ■ Targets (A list of objects containing a device group and/or a device export) 	The policy job is matched against the reference ID, content type, and if applicable, the version. Targets are matched according to their contents. If a target contains both a device and device group, then it will be matched against the device within the device group on the target.
Report	<ul style="list-style-type: none"> ■ Name (informational purposes only) ■ Canned ID 	The system matches this against the canned ID. Custom reports are not supported at this time.
Script	<ul style="list-style-type: none"> ■ Name (informational purposes only) ■ Reference ID ■ Device type ■ Version 	The system matches this against the same data (version may or may not apply) on the target 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.

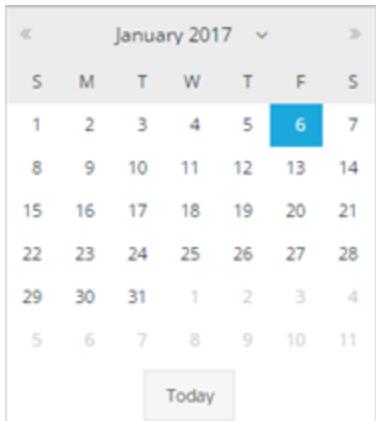
Run Once Only

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.

Tip: 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 next 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**.
3. Make your changes.
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 645. To view all scheduled jobs, see "Monitor Jobs" on page 640. To cancel a currently running job, see "Cancel a Currently Running Job" on page 644.

1. Select **Jobs > Current Jobs**. The top pane displays the following details:

Column	Description
Name	This is the name you gave the job when you created it. See "Add a Job" on page 600.
Status	This is the current status of the job. The status of a job changes from Running to Complete .
Progress	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.
Start Time	This shows the start time (in a 24-hour clock format) of the current job.
End Time	This shows the end time (in a 24-hour clock format) of the current job.
Description	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 "Backup", but without a good description it is difficult to see which devices are currently being backed up.

Note: 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

Management Center Configuration & Management

- **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 32.

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**.

Note: 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:

Status
Error: The operation has t

4. All jobs that you successfully cancel are obvious in the web console. Canceled jobs appear as such in the Status column.

Warning: 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 642. To view all scheduled jobs, see "Monitor Jobs" on page 640. 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:

Column	Description
Name	This is the name you gave the job when you created it. See "Add a Job" on page 600.
Status	This is the status of the job. More details are available about the job.
Progress	This progress bar is displays completed jobs, with the latest job that was run always on top.
Start Time	This shows the start time (in a 24-hour clock format) of the selected job.
End Time	The shows the end time (in a 24-hour clock format) of the selected job.
Description	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 "Backup", but without a good description it is difficult to tell the different backups that occurred.

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.

Warning: 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
 - Missed Execution
 - Prepared Running

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.

Tip: When the Job Progress window displays a currently running job that is taking a long time, you have the option to **Continue in Background**.

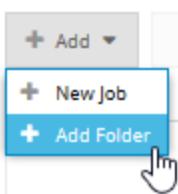
For more details on the use of color and status indicators, see "About Color-Coded Status Indicators" on page 32.

Note: You cannot delete a job from Job History, you can only "Cancel a Currently Running Job" on page 644.

Organize Jobs with Folders

To make it easier to find your policy, you can logically organize your jobs using folders.

1. Go to **Jobs > Jobs**.
2. Click **Add > Add Folder**.



Note: This system does not display the **Add Folder** option unless the **Folders** option is enabled.

- Provide a name and optional description and click **Save**.

The system displays the folder in the left pane. If you don't see the folder list, toggle the **Folders** option.

Policy Objects



- Drag and drop the job(s) you'd like to move to the folder.
- Optional—if you want to make the folder a sub-folder of another folder, drag and drop it to any folder (except itself).

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*

Operation	Description	Fields
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*
	<p>Note: 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.</p>	
	<p>Backup Description*</p>	
	<p>Include Private Data</p>	
	<p>Encrypt Backup</p>	

See also "Back Up Device Configuration Now" on page 174.

Management Center Configuration & Management

Operation	Description	Fields
Backup Management Center	Stores a backup of the Management Center configuration to the specified server on a defined schedule. This operation is not supported in Multistep Device Jobs. See also "Back Up the Management Center Configuration" on page 627.	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. 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 "Enable Device Health and Statistics Monitoring" on page 155.	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 .

Operation	Description	Fields
Check Consistency	<p>Checks whether the policy installed on selected devices matches the reference policy.</p> <p>This operation is not supported in Multistep Device Jobs.</p> <p>See also "Check Consistency between Policy and Devices" on page 483.</p>	<p>Policy* - Click  to select the reference policy to use for comparison.</p> <p>Select policy version* - Select the radio button for either The latest policy version or specify a previous Version.</p>
Collect Sysinfo	<p>Extracts the Sysinfo data from the selected ProxySG appliances and outputs it to a file.</p> <p>If the job executes successfully, the files are saved to Jobs > Archived Files as a zip file.</p>	<p>During job creation, ensure that Email Results or Generate Archive are selected.</p>
Execute a Script	<p>Runs the designated script on the selected target ProxySG appliances on a defined schedule.</p> <p>See also "Execute Scripts" on page 251.</p>	<p>Device Script* - Click  to select the script to execute</p>

Management Center Configuration & Management

Operation	Description	Fields
Export Backups	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.	<p>Export to Server - Select the check box.</p> <p>Server URL* - Supported protocols include scp, ftp/ftps, and http/https.</p>
	<p>Note: 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.</p>	
	See also "Export Device Backups" on page 191.	
	<p>Note: Management Center supports the following key exchange algorithms for SSH/SCP connections: DHGex, DHG, and Curve25519.</p> <p>If a user attempts to export a backup to a server via SCP and the target server does not support at least one of those key exchange algorithms, the export may fail with the message A connection could not be established or The secure handshake failed during key exchange. This also applies to other Management Center operations that use SSH/SCP.</p>	<p>Encryption</p> <p>Phrase* - 1 or more characters, alphanumeric.</p> <p>User name</p> <p>Password</p> <p>Prune Backups - Select this check box if you want to remove the backup from the backup slot when you export the backup.</p> <p>Retention Count* - Enter the number of backups to keep.</p> <p>Prune Pinned - Select this check box if you want to prune backups that have been pinned (or saved).</p>

Operation	Description	Fields
File Transfer	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.	<p>Server URL* - Enter the URL of the file. Supported protocols include http/https.</p> <p>File Type - Specify the file type.</p> <p>If the file already exists - Choose what to do if the file already exists.</p>
Import External Policy	<p>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.</p> <p>This operation is not supported in Multistep Device Jobs.</p> <p>See "Import External Policy " on page 465.</p>	<p>Import from URL* - Supported protocols include scp, ftp/ftps, and http/https. The filename must be the ID assigned to the target policy.</p> <p>Username</p> <p>Password</p>
Install Policy	<p>Runs the designated policy on the selected target ProxySG appliances on a defined schedule.</p> <p>See "Install Policy" on page 451.</p>	<p>Policies* - Click  to select the policies to install.</p> <p>Force Installation - Select this check box to override any warnings.</p>

Management Center Configuration & Management

Operation	Description	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 .	System Image - Select the image to install. The file will only be listed here if it has been uploaded to Management Center (Configuration > Files).
Remove Unused Policy	Removes tenant policy when there is no policy assigned to the tenant on the appliance. This operation is not supported in Multistep Device Jobs. See Remove Unused Tenant Policy .	<i>No additional fields.</i>
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 > Archived Files). This operation is not supported in Multistep Device Jobs.	Registered Not Registered * - Use Not Registered if using Reporter 9.x or higher. You can manually enter the credentials to connect. Reporter (*) - Select the Reporter device to run the report on. Database (*) - Select the database from which to run the report.

Operation	Description	Fields
Summary Report	<p>Runs a summary report. This saves the report as an archived file (Jobs > Archived Files). This operation is not supported in Multistep Device Jobs.</p> <p>See also "Run a Summary Report" on page 685.</p>	<p>Cover Title* - Add a title for the cover page of the report.</p> <p>Sections - Select the sections you want to add to the report on.</p> <p>Database (*) - Select the database from which to run the report. The database is only required for some sections and is inaccessible for the others.</p> <p>Filename (*) - Change the filename of the archived PDF, if wanted. This is automatically populated by what you enter for the Cover Title.</p> <p>Description - Add a description of the scheduled report.</p>

Management Center Configuration & Management

Operation	Description	Fields
Synchronize Devices	<p>Synchronizes configuration settings from one device (the source) to one or more similar devices running the same or later OS versions.</p> <p>Management Center supports synchronization of the following device types: SSL Visibility, Content Analysis, and Malware Analysis.</p> <p>See also "Synchronize Devices" on page 109.</p>	<p>Source Device* - Select the device whose settings you want to copy to other devices.</p> <p>What to synchronize (*) - Varies by source device.</p>

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 732

For descriptions of each report, refer to "Reference: Statistics Monitoring Reports in Management Center" on page 736.

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 659

For descriptions of each of these reports, see "Reference: Report Descriptions" on page 691.

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 166.
2. Decide which Devices report to view (such as Traffic Mix or Traffic Statistics). For descriptions of each report, see "Device Performance Reports" on page 736.
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 166.
2. Decide which WAN Optimization report to view. For descriptions of each report, see "WAN Optimization Reports" on page 737.
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 next 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 691.
4. View the report. See "View a Reporter Report" on page 674.

Integrate Reporter into Management Center

Reporter Enterprise Server 10.1.x is required to access and view Reporter reports and dashboards.

Prerequisites

- Configure your Reporter Enterprise Server to receive logs from one or more ProxySG appliances. Refer to [Upload Access Logs From ProxySG Appliance](#) and [Upload Access Logs to the Reporter Server](#) for more information.
- 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.
3. "View a Reporter Report" on page 674.

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.

Device	Go To...
Advanced Secure Gateway	"About Public Key or Credential Authentication for ProxySG or Advanced Secure Gateway" below
ProxySG appliance	"About Host Key Validation" on the next page "Add a ProxySG or Advanced Secure Gateway using Credential Authentication" on page 662 "Add a ProxySG or Advanced Secure Gateway using Public Key Authentication" on page 664
Content Analysis	"Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility" on page 667
Malware Analysis	"Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility" on page 667
PacketShaper	"Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility" on page 667
Reporter	"Add a Reporter" on page 665
Security Analytics	"Add a Security Analytics" on page 669
SSL Visibility	"Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility" on page 667
Web Security Service	"Add Web Security Service (WSS)" on page 671

Tip: Configure how often devices are polled. See Set the Device Polling Interval.

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.

Note: 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.

Note: 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-keykey-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-1f <(ssh-keyscan device_ip2>/dev/null)
```

The system displays the host key.

- Do the following from the device's serial connection:

- Enter the following command:

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

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

- 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 160 for information on pre-deployment devices.
 - Select **ReadWrite** or **Read Only**.
 - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 117 for more information.

- Specify whether to collect statistics for the device. See "View Statistics Monitoring Reports" on page 732.

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).
- Select the SSL context to use for TLS communication.

Operation:

- The default setting is **Global Default**. When **Global Default** is selected, the system uses the SSL context configured in the [Device Communications](#) settings.
- If you select a different SSL context (not **Global Default**), that context overrides the SSL context defined in the Device Communication setting.
- If no SSL context is set in the **Device Communication** setting, the system uses the **system-defined: default** SSL context when in FIPS mode, and none otherwise.

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**.

Caution: 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 584.
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 160 for information on pre-deployment devices.
 - Select **ReadWrite** or **Read Only**.
 - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 117 for more information.
 - Specify whether to collect statistics for the device. See "View Statistics Monitoring Reports" on page 732.
 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).
 - Select the SSL context to use for TLS communication.
- Operation:

- The default setting is **Global Default**. When **Global Default** is selected, the system uses the SSL context configured in the [Device Communications](#) settings.
- If you select a different SSL context (not **Global Default**), that context overrides the SSL context defined in the Device Communication setting.
- If no SSL context is set in the **Device Communication** setting, the system uses the **system-defined: default** SSL context when in FIPS mode, and none otherwise.

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**.

Caution: 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 584.
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

Note: 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 160 for information on pre-deployment devices.
 - Select **ReadWrite** or **Read Only**.
 - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 117 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`.
 - Optional—Your enable password. The enable password is required for SSH connections like running scripts, and so on. If you add the enable password, you must open port 22 or device registration will fail.
 - Select the SSL context to use for TLS communication.

Operation:

- The default setting is **Global Default**. When **Global Default** is selected, the system uses the SSL context configured in the [Device Communications](#) settings.
- If you select a different SSL context (not **Global Default**), that context overrides the SSL context defined in the Device Communication setting.
- If no SSL context is set in the **Device Communication** setting, the system uses the **system-defined: default** SSL context when in FIPS mode, and none otherwise.

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**.

Caution: 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. Optional—Verify or change the **Device Name**.
9. Optional—Input any applicable attributes. See "Add Attributes" on page 584.
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

Note: 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 160 for information on pre-deployment devices.
 - Select **ReadWrite** or **Read Only**.
 - Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 117 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.
 - Optional, for CA and SSLV only: The enable password. You must include the enable password only if you want to run scripts on the device.
 - Optional—Your enable password. The enable password is required for SSH connections like running scripts, and so on. If you add the enable password, you must open port 22 or device registration will fail.
 - Select the SSL context to use for TLS communication.
- Operation:
- The default setting is **Global Default**. When **Global Default** is selected, the system uses the SSL context configured in the [Device Communications](#) settings.

- If you select a different SSL context (not **Global Default**), that context overrides the SSL context defined in the Device Communication setting.
 - If no SSL context is set in the **Device Communication** setting, the system uses the **system-defined: default** SSL context when in FIPS mode, and none otherwise.
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**.

Caution: 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**
10. Optional—Input any applicable attributes. See "Add Attributes" on page 584.
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 160 for information on pre-deployment devices.

- Select **ReadWrite** or **Read Only**.
- Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 117 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.
- Enter the [Security Analytics device API key](#).
- Select the SSL context to use for TLS communication.

Operation:

- The default setting is **Global Default**. When **Global Default** is selected, the system uses the SSL context configured in the [Device Communications](#) settings.
- If you select a different SSL context (not **Global Default**), that context overrides the SSL context defined in the Device Communication setting.
- If no SSL context is set in the **Device Communication** setting, the system uses the **system-defined: default** SSL context when in FIPS mode, and none otherwise.

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**.

Caution: 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**

9. Optional—Input any applicable attributes. See "Add Attributes" on page 584.

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)

To add a WSS, you must first create an integration token on the WSS portal. Then use that token to add the WSS to Management Center.

You use WSS with Management Center to create [Universal Policy Enforcement \(UPE\) rules](#).

Note: The following steps require that you have not yet set up and configured your WSS portal account. If you have already set up your portal account, contact [Symantec support](#) for assistance.

Step 1: Create WSS Integration Token

To create the token, do the following:

1. To create the token, log into your WSS portal and enter **Service** mode. Select **Account Maintenance > Integrations**.
2. Click **New Integration**. The portal displays the **New Integration** dialog.
3. Select the **Integration Type**, depending on your solution. The portal displays the integration page per the device type.

The exception is CASB Integration; selecting this type adds the drop-down to the Integrations page. From you here, you tenant the CloudSOC.

Refer to the [WSS documentation](#) for more information.

Step 2: Add WSS in Management Center

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Select **Add > Add Device**. The system displays the **Add Device** wizard.
4. Select **Web Security Service**.

5. Specify the **Modes**:

- Select **Existing device** if your WSS account is configured, or **Unavailable** (pre-deployment) if the service is not configured or is unreachable. See "About Pre-Deployed and Deactivated Devices" on page 160 for information on pre-deployment devices.
- Select **ReadWrite** or **Read Only**.
- Specify whether to monitor the health of the device. See "Put Device in Read-Only Mode" on page 117 for more information.

6. In **Connection**, do the following:

- a. Select the **Cloud Network** to connect to, Production or Pre-Production.

Note: If you are participating in a beta program, click **Analyze in Pre-Production**.

- b. Click **Connect**.

7. In the **Registration Required** field, enter the Integration Token you created in "Step 1: Create WSS Integration Token" on the previous page and click **Register**.

Caution: 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**.

9. Optional—Input any applicable attributes. See "Add Attributes" on page 584.

10. Click **Save**.

Note: If you use the Management Center [failover feature](#) and the primary fails, you must reconnect to the WSS on the secondary. Though WSS devices are propagated to the secondary, it will be viewed by the WSS instance as a different appliance requiring

registration. To reconnect to the WSS, go to **Network > device > Edit Connection Parameters**.

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

Next Steps

What do you want to do next?	Refer to this topic
Ensure that all devices belong to a hierarchy and group.	"Ensure Devices Belong to Device Groups" on page 169
Check information specific to the selected device.	"Monitor Device Health " on page 147
Check device metrics.	"View System Metrics" on page 161
Troubleshoot device connection	"Can't Connect to Device After Upgrading to 2.x" on page 856

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.**

The screenshot shows the 'Reports Home' interface. At the top, there are buttons for 'New Report', 'New Group', and 'Operations'. On the right, a sidebar displays user information: 'RP-V50 - ProxyS' (Role: administrator), 'RP-V50 - ProxySG - WTL', and 'Office'. Below this, two report categories are listed: 'Security' and 'User Behavior'. The 'Security' category contains links for: Potential Malware Infected Clients, Blocked Users, Blocked Requests by User Agent, Malware Detected Names, Threat Sites Blocked, and Trend of Risky Requests. The 'User Behavior' category contains links for: Blocked Requests by Site, Blocked Requests by Category, Blocked Requests by User, Filtering Verdict Trend by Day, Sites, and Categories.

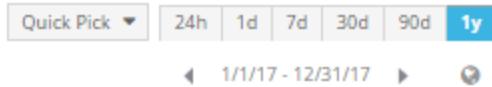
Note: If the database you want is not available, see "Determine Why A Reporter Database Does Not Display" on page 731.

Reporter has the following report categories:

Management Center Configuration & Management

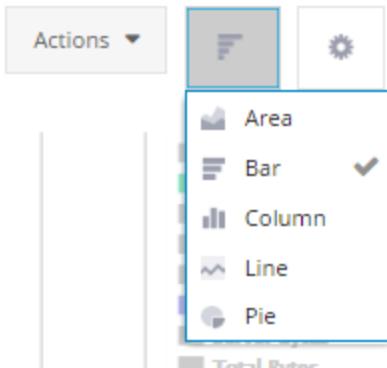
- Security
- User Behavior
- Log Detail
- Bandwidth Usage
- Web Applications

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**

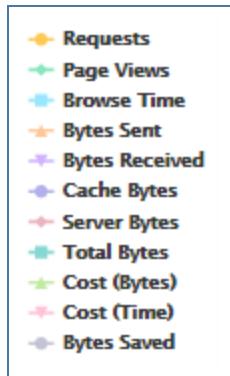


Graph types include:

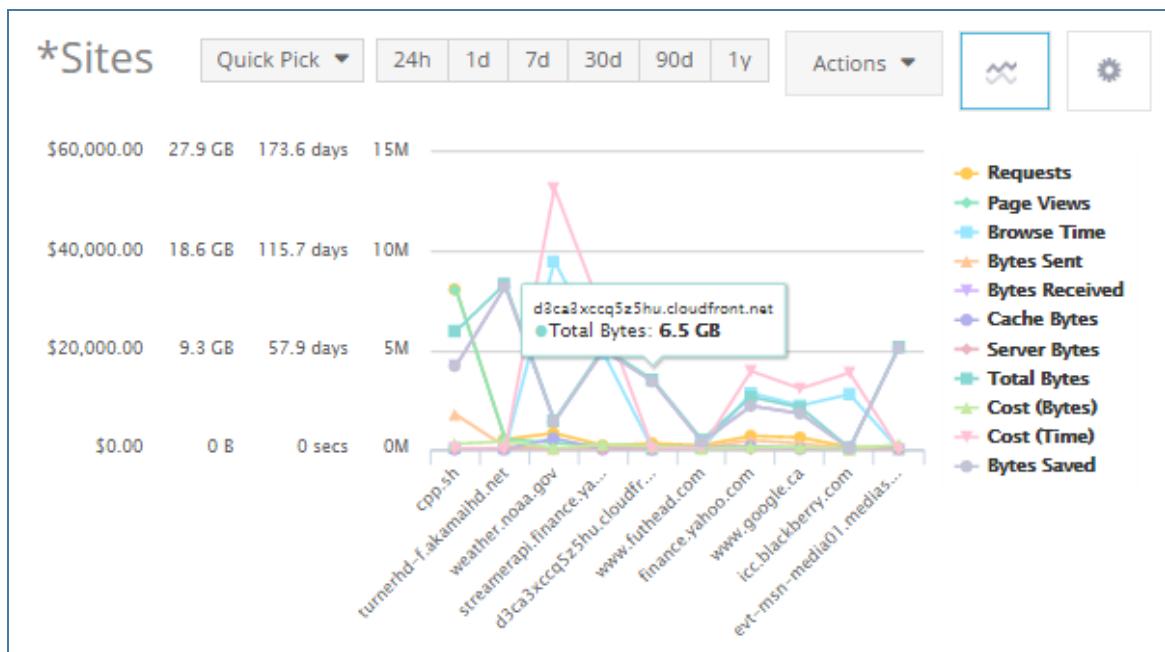
- **Area** - An area graph displays graphically quantitative data. It is based on the line chart. The area between axis and line are commonly emphasized with colors and textures. Commonly used area graphs compare one area with two or more areas.
- **Bar** - A bar graph presents grouped data with rectangular 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:

Management Center Configuration & Management



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. You can also [share the report](#) with other users.

Save As ×

Name: * Cost per User and Site

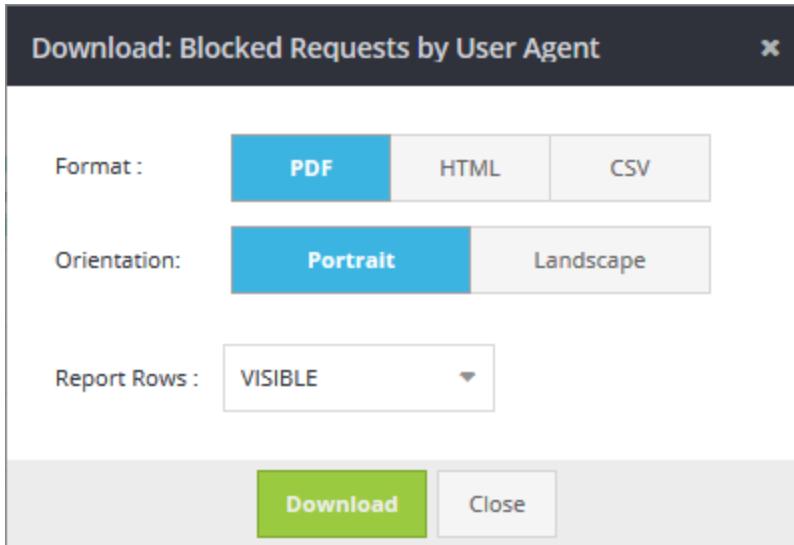
Description: This report has been filtered to show only requests to two specific domains.
948 of 1024 characters left

Group: * Custom Reports ▼

Save Cancel

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.

Note: By default, the reports have a Symantec logo. You can [replace that with your logo](#).



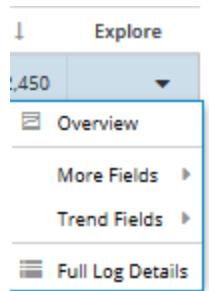
- a. Select the format, **PDF**, **HTML**, or **CSV**.
 - b. For PDF, select the orientation, **Portrait** or **Landscape**. (This is not applicable to HTML or CSV.)
 - c. Select the number of rows you want included in the offline report. Leave the default value, **Visible**, if you would like the report 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.

The screenshot shows the 'Reports Home' section of the Management Center. At the top, there's a 'Reporter' section with a house icon and the text 'Reporter Based'. Below it, 'Database: searchtest' is listed. A list of reports is displayed in a grid:

- Users per Risk Score** (highlighted with a green border)
- Trend of Discovered Client IPs
- Bandwidth per Hour of Day
- *Trend of Blocked Users
- *Trend of Blocked Requests

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 three ways to drill down in a report:

- Highlight the entry in the table and click the arrow in the **Explore** column.



- 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.
- Right-click any field in the table at the bottom of a report to display a list of fields.

Management Center Configuration & Management

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.

The screenshot shows a data grid interface with a context menu open over a row. The data grid columns include 'Category' and 'Action'. The context menu, which is the focus of the image, is titled 'More Fields' and lists various data fields: Action, Business Readiness Rating, Client IP, Content Type, Day of Week, Group, Hour of Day, Malware, Method, Port, Protocol, Proxy IP, Risk Score, Search Term, Server IP, Status, User, User Agent, Web App Operation, and Web Application. The 'Site' option in the main menu is highlighted.

Action
Business Readiness Rating
Client IP
Content Type
Day of Week
Group
Hour of Day
Malware
Method
Port
Protocol
Proxy IP
Risk Score
Search Term
Server IP
Status
User
User Agent
Web App Operation
Web Application

14. (Optional) Generate an 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.

Site	Categories	Page Views ↓	Browse Time
[REDACTED]	News/Media, none, Network...	21,533	5.8 days
www.cnn.com	News/Media, none, Audio/...	21,511	3.3 days
[REDACTED]	File Storage/Sharing, Techn...	20,324	5.4 days
[REDACTED]	Web Ads/Analytics, Search	10,700	6.7 days

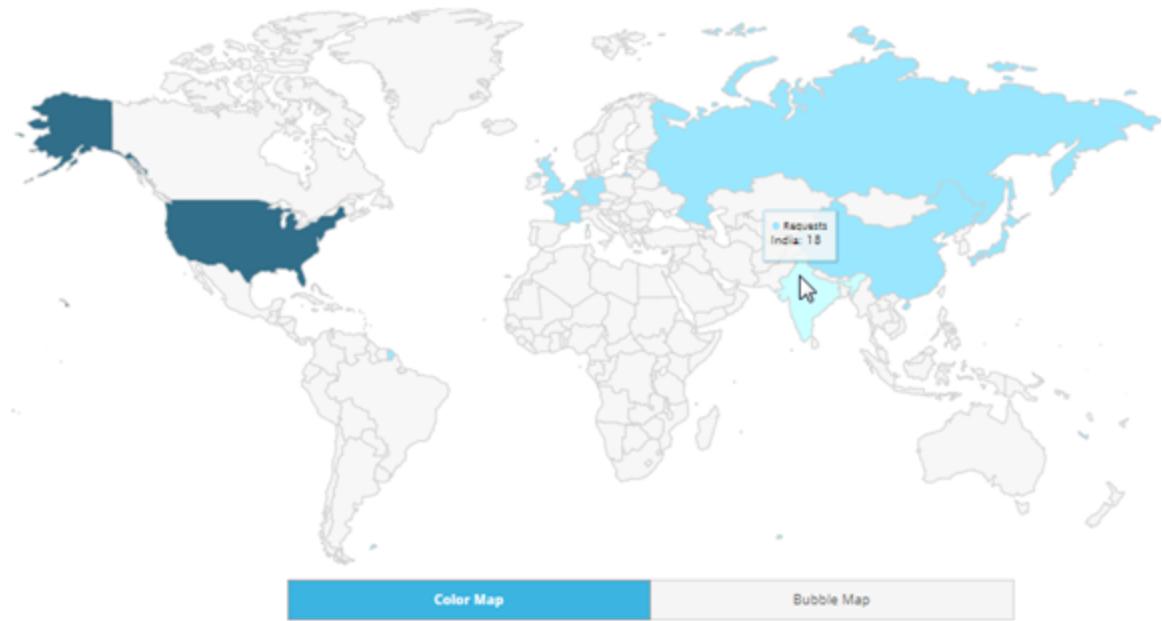
15. (Optional) [Filter or change the report criteria.](#)

Create Geovisual Reporter Reports

The Color Map, Bubble Map, and Pie Map reports (**Reports > Reporter > New Report**) provide a geographically-based view of report data. Currently, you can create these reports only by grouping by **Destination Country**. Hover the cursor over the colored map areas to view relevant information.

Note: To view these reports, you must select a database that contains access logs generated by a ProxySG with an Advanced Web Security license.

Color Map



Bubble Map



Geo Pie Map



Create GeoVisual Maps

1. Select **Reports > Reporter**.
2. Select a Reporter database. To view these reports, you must select a database that contains access logs generated by a ProxySG with an Advanced Web Security license.



3. Click **New Report**. The six-step report designer displays in the left pane, and the report preview displays in the right pane.
4. In **Grouping Level**, select **One Level** for Color or Bubble maps. Select **Two Level** for Geo Pie maps.
5. In **Group By**, select **Destination Country**. For two-level reports, **Destination Country** must be specified for the 1st level.
6. Select the chart type.



For two-level reports, the system displays the following:



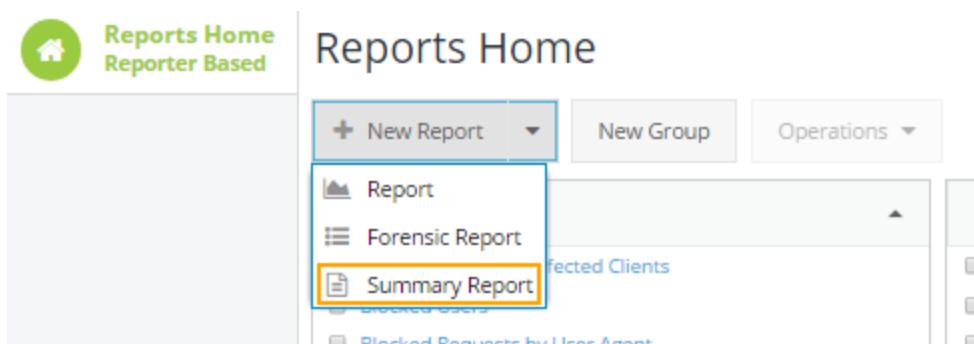
7. Select the desired time frame, columns, and filters. See "Create a Custom Reporter Report" on page 708 for more information.
8. Click **Run Report**.

Run a Summary Report

Management Center enables you to run a Summary Report (**Reports > Reporter > New Report > Summary Report**) that provides value-specific information on various security planning, monitoring, and compliance of corporate KPIs.

Use the Summary Report feature to drill down into the database to find specific information based on the inventory, health, user activity, license state, data from statistics monitoring, and/or device details necessary.

1. **Select Summary Report from the New Report menu.**



2. Add and select the information and sections for the report.

Report Content	Notes	Description
Protection	Requires Reporter 10.x appliance	Provides a summary of Protection Metrics, Top Sites and Categories, Traffic Composition, Traffic Composition for Potential Security Risk, and Blocked Traffic.
Network Activity	Requires Reporter 10.x appliance	Provides a summary of Network Activity Metrics, Network Traffic Top 5s, and Traffic Trend.

Report Content	Notes	Description
Device Inventory	Requires Management Center only	Provides a summary of health status, device types, license state and expiry, and ProxySG appliance license components.
User accounts	Requires Management Center only	Provides a summary of Management Center user accounts and their roles and permissions. For more information, see "View All Users and Associated Roles and Permissions" on page 527.
Device Performance	Requires statistics monitoring service	Provides a summary of Services, Trend of Services, CPU, and Memory.
WAN optimization	Requires statistics monitoring service	Provides a summary of Bandwidth Savings and Effective Bandwidth.

Note: The database is required (and available) only for reports that include specific section(s).

3. Click **Run Report**. When the job is finished, the system provides a link to the report in PDF format.

Note: By default, the reports have a Symantec logo. You can [replace that with your logo](#).

4. Click **Download** to save the file locally.

You can also access the PDF report by going to the archive in **Configuration > Jobs > Archived Files**.

Tip: Alternately, you can click **Create Job...** to run the report as a job.

Management Center saves the reports under the Jobs tab, on the Archived Files page. The total amount of space allocated to the archive is 10% of the available disk space.

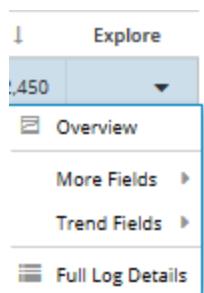
Use the filters to sort through the archived reports. You can sort by:

- Filename
- Extension (example: PDF)
- Created By
- Source

View Reporter Report Details

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 three ways to drill down in a report:

- Highlight the entry in the table and click the arrow in the **Explore** column.



- 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. 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.

Site	Categories	Page Views ↓	Browse Time
[REDACTED]	News/Media, none, Network...	21,533	5.8 days
www.cnn.com	News/Media, none, Audio/...	21,511	3.3 days
[REDACTED]	File Storage/Sharing, Techn...	20,324	5.4 days
[REDACTED]	Web Ads/Analytics, Search	10,700	6.7 days

- 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.

The screenshot shows a list of log entries on the left and a detailed view on the right. A context menu is open over the entry 'proxy_client_Allow' at index 0, specifically over the 'More Fields' option. The menu lists various fields:

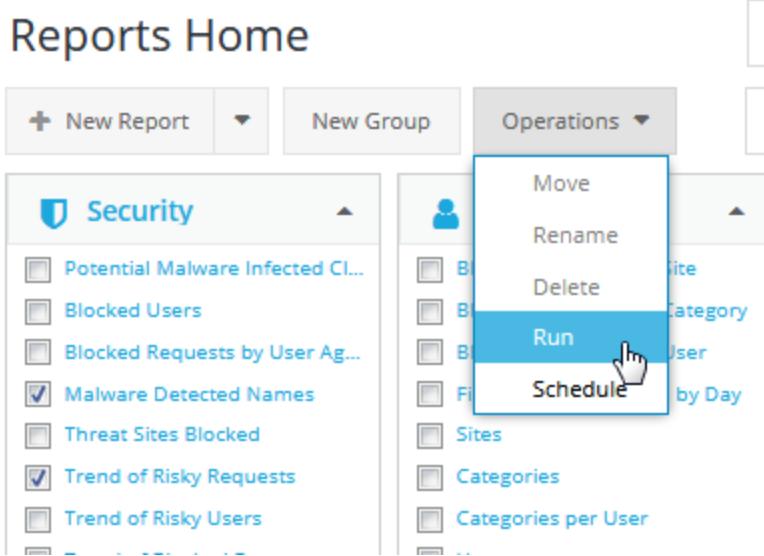
- Action
- Business Readiness Rating
- Client IP
- Content Type
- Day of Week
- Group
- Hour of Day
- Malware
- Method
- Port
- Protocol
- Proxy IP
- Risk Score
- Search Term
- Server IP
- Status
- User
- User Agent
- Web App Operation
- Web Application

Run a Reporter Report in the Background (Or to Archive)

This topic describes how to create a report that can be run and archived to **Jobs > Archived Files**. You can also choose to run the report in the background. Though this operation does not create a scheduled job object, the results can be viewed in the **Jobs > Job History** page and are saved to **Jobs > Archived Files** for later viewing.

Note: This operation creates an ad hoc job. You cannot email the results of this type of job. If you want to email results, select **Create Job** in the Schedule Reports: Reports dialog. See "Schedule Reporter Reports" on page 618.

1. Select **Reports > Reporter**.
2. Select a Reporter database to use for the reports.
3. Select the check box next to one or more reports and click **Operations > Run**.



4. In the Schedule Reports: Reports dialog, select any other reports to run.
5. In the Schedule Settings dialog, specify any other reports to schedule.

- a. Select the database from which you want to schedule the report.
 - b. Select the time span for the report.
 - c. Select a report format: PDF, HTML, or CSV.
 - d. Select the page orientation.
 - e. Select the number of report rows.
 - f. Optional: Add a description.
6. Click **Run Now**. The system runs the report.
7. Click **Continue in Background** button at the bottom of the Job Progress: Run Report dialog to continue running the report for later viewing. When the report completes, the system provides a notification that includes a link to view the report.

The Job Progress dialog shows the status of the job. If the job is successful, click the **Download** link next to the report to view it. You can also access the files by navigating to **Jobs > Archived Files**.

Reference: Report Descriptions

The following report groups are available if you have [integrated Reporter 10.1.x](#) or later with Management Center:

Note: Some reports require Reporter versions later than 10.1.2.x. These requirements are noted in the report description.

- 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 674 for details.

Note: 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.

Report	Description of Default Graph
Potentially Infected Clients - Unified	To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database.
	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 <i>Unified</i> reports.
	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.
Potential Malware Infected Clients	To view this report, you must add a Reporter appliance running 10.1.3.x or later. 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.
Malware Detected Names	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. Note: This report will be blank if user name data isn't available in the Reporter log file.
Blocked Users	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. Note: This report will be blank if user name data isn't available in the Reporter log file.
Blocked Request by User Agent	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.
Threat Sites Blocked	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.
Trend of Risky Requests	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 <i>normal requests range</i> , 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.

Management Center Configuration & Management

Report	Description of Default Graph
Trend of Risky Users	Displays a line graph that shows the number of users making requests to URLs of risky categories (Spyware , Suspicious , Phishing , or Malicious) over the specified time period. The graph contains a shaded area that represents the <i>normal count range</i> , 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. Note: User drill-downs are blank if user name data isn't available in the Reporter log file.
Trend of Blocked Requests	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 <i>normal requests range</i> , 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.
Trend of Blocked Users	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 "normal count range," 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. Note: User drill-downs are blank if user name data isn't available in the Reporter log file.
Trend of Risky Clients	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 "normal count range," 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.
Threats	To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a bar chart that provides details for the number of threats discovered by each detection method (Sandboxing, File Reputation, Anti-virus, WebPulse).

Report	Description of Default Graph
Threats - Unified	<p>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database.</p>
	<p>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 <i>Unified</i> reports.</p>
	<p>Displays an area, bar, column, or pie chart that provides details for the number of threats discovered by each detection method (sandboxing, file reputation, predictive analysis score, anti-virus, WebPulse).</p>
	<p>Note: If Malware Analysis processing results in a detonation, the Malware Analysis sends that result to the Content Analysis, which notifies the SGOS proxy device. The SGOS proxy device caches the result and blocks subsequent requests that match. However, the log entries for these cache block actions do not contain the sandboxing vendor or score. Because of this, you might not see the Malware Analysis benefits reflected in the reports. For example, the SGOS proxy device might block 20 requests that match a cached result; the Malware Analysis is credited with only one result (the one that resulted in the cache entry). However, when the SGOS proxy device receives a clear cache action (for example, when new AV patterns are loaded), the Malware Analysis action re-occurs on the next request.</p>
Trend of Threats	<p>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</p> <p>Displays a column chart that shows the trend over time for each detection method (Sandboxing, File Reputation, Anti-virus, Web Pulse).</p>
Trend of Threats - Unified	<p>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database.</p> <p>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 <i>Unified</i> reports.</p>
	<p>Displays an area, bar, column, or pie chart that shows the trend over time for each detection method (sandboxing, file reputation, predictive analysis score, anti-virus, WebPulse).</p>
Threats - WAF	<p>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later.</p> <p>Displays an area, bar, column, or pie chart that shows the number of threats by category (attack family or anti-virus). Each colored section represents a threat type and corresponding number of incidents.</p>

Management Center Configuration & Management

Report	Description of Default Graph
Trend of Threats - WAF	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 trend over time for anti-virus and attack family threats.
Actions	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 action-related data. This data includes requests, page views, browse time, cost (time), cost (bytes), total bytes, bytes sent, bytes received, cache bytes, server bytes, bytes saved.
Methods	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.
Attack Families	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 <code>x-bluecoat-waf-attack-family</code> log field. Each slice represents an attack type. The chart displays only the top ten attack types.
Attack Families Per Country	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 <code>x-bluecoat-waf-attack-family</code> or <code>x-virus-id</code> does not include "-".
Sandboxing Risk Score	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.
Trend of Sandboxing	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.
Trend of Predictive Analysis	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.

Report	Description of Default Graph
Trend of File Reputation	<p>To view this report, you must add a Reporter appliance running 10.1.4.x or later.</p> <p>Displays an area, bar, column, or pie chart that shows the trend over time for each file reputation score.</p>
File Risk Score	<p>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</p> <p>Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</p>
File Risk Score	<p>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</p> <p>Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</p>
URL Threat	<p>To view this report, you must add a Reporter appliance running 10.1.5.4 or later.</p> <p>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.</p>
Risky Sites per Country	<p>To view this report, you must add a Reporter appliance running 10.1.5.4 or later.</p> <p>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.</p>
Risky Clients per Country	<p>To view this report, you must add a Reporter appliance running 10.1.5.4 or later.</p> <p>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.</p>
Attack Families by Site	<p>To view this report, you must add a WAF database from a Reporter appliance running 10.1.5.4 or later.</p> <p>Two-level report that displays each protected web site and the corresponding number of requests per attack type. 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.</p>
Allowed - No WAF Detection	<p>To view this report, you must add a WAF database from a Reporter appliance running 10.1.5.4 or later.</p> <p>Can be used to on a non-production system to test WAF policy. After you set up your WAF policy, you can send malicious traffic through your test device to see if the policy is working; this report lists the requests that were allowed to pass without being detected.</p>

User Behavior

Management Center Configuration & Management

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.

Report	Description of Default Graph
Blocked Requests by Site	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.
Blocked Requests by Category	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.
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.
Client IPs	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.
User Agent Families	In releases prior to 2.4.1.1, you must add a WAF database from a Reporter appliance running 10.1.3.x or later to view this report. In 2.4.1.1 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.

Report	Description of Default Graph
Countries	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).
Protocols	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.
Days	Displays an area graph that shows the number of web requests for each day in the selected time period.
Days of Week	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.
Hours of Day	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.
Months	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.
Trend of Discovered Users	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.

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.

Report	Description of Default Graph
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.

Management Center Configuration & Management

Report	Description of Default Graph
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.

Report	Description of Default Graph
Full Log Details	<p>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</p> <p>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.</p>
Blocked Log Details	<p>To view this report, you must add a Reporter appliance running 10.1.3.x or later.</p> <p>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.</p>

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.

Report	Description of Default Graph
Web Applications	<p>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.</p>
Web Applications by Users	<p>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.</p>
Web Applications by Client IPs	<p>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.</p>
Blocked Web Applications	<p>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.</p>
Trend of Active Web Applications	<p>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.</p>
Trend of Web Application Traffic	<p>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.</p>

Management Center Configuration & Management

Report	Description of Default Graph
Web Application Operations	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.
Users of Risky Applications	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. Note: This report will be blank if user name data isn't available in the Reporter log file.
Web Applications per Risk	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.
Tips:	
<ul style="list-style-type: none">■ Sort the values in the Web Application column to alter the pie chart to show the corresponding data.■ You may want to turn off the Other overlay, if this segment has a significant number of requests.	
Users Per Risk Score	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.
Risk Distribution	Displays a pie chart that shows the percentage of requests at each risk level. Each slice represents a risk level.
Risk Distribution Per User	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.
Trend of Risk Distribution	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.
Social Media Activity	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.
Social Media Applications	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.

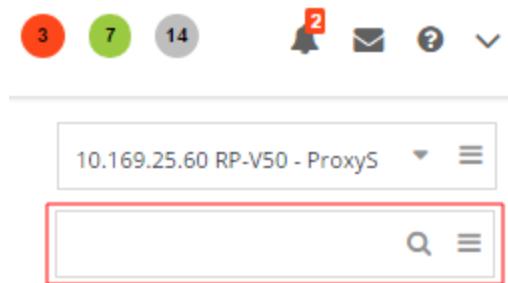
Report	Description of Default Graph
Facebook Users	Displays a bar graph that shows the number of Facebook requests by each user. The names of the users with the most Facebook requests appear at the top of the report. This report allows you to see who the most active Facebook users are.
	Note: This report will be blank if user name data isn't available in the Reporter log file.
Facebook Categories	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.
Mail Activity	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.
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).

Search for Specific Report Data (Search and Forensic Report)

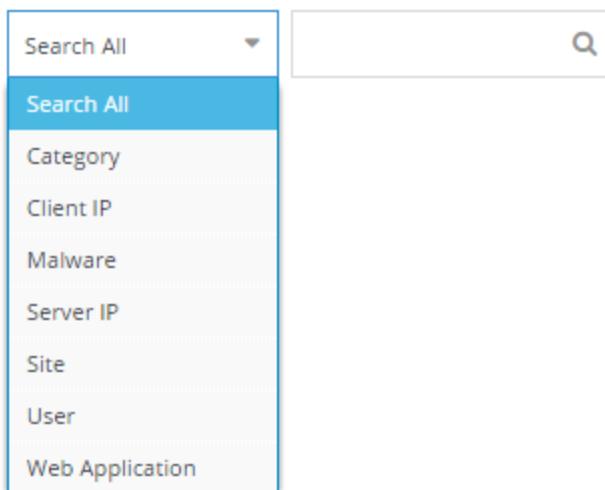
Management Center enables you to search for specific report data using a simple search or by executing a forensic report.

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.**

The screenshot shows the Symantec Management Center homepage. On the left, there's a sidebar with links for 'Reports Home' (Reporter Based), 'Reporter: RP-V50', 'Database: ProxySG - WTL Office', and a search bar containing 'Search: "violence"'. The main content area has a title 'Searching Categories' with the subtitle 'Results for "violence"'. It shows a list of categories under 'Violence/Hate/Racism' with the first item selected. Navigation controls like '<<', '<', 'Page 1', and '>' are visible at the bottom.

- 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.

The screenshot shows the 'Reports Home' page. At the top, there's a green banner with a house icon and the text 'Reports Home Reporter Based'. Below it, a navigation bar includes 'New Report' (with a dropdown arrow), 'New Group', and 'Operations'. A dropdown menu for 'New Report' is open, showing three options: 'Report' (selected), 'Forensic Report' (highlighted with an orange border), and 'Summary Report'. Other items like 'Blocked Clients' and 'Blocked Users' are visible in the background.

- Select **Forensic Report** from the New Report menu. The system opens the Run Forensic Report window.

Management Center Configuration & Management

Run Forensic Report ×

Source

User: All Users

Client IP: All Client IPs

Destination

Category: All Categories

Site: All Sites

What

Verdict: All Verdicts

When

Date: Quick Pick ▾ 24h 1d **7d** 30d 90d 1y

Run Report Cancel

2. Select (or enter) the search criteria from the available data or enter a transaction ID.
3. **Select a time duration.**

Run Forensic Report

Source

User: All Users

Client IP: All Client IPs

Destination

Category: All Categories

Site: All Sites

What

Verdict: **virus_detected**

When

Date: Quick Pick **7d** 24h 1d 7d 30d 90d 1y

Run Report Cancel

- Click Run Report. The system displays the search results in the Full Log Details report.

Details for virus_detected
Verdict is "virus_detected"

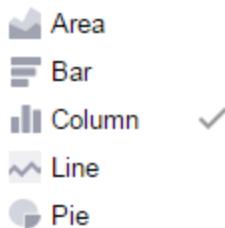
Date and Time	Client IP	Status	User
Jun 22, 2015 8:29:19 PM	[REDACTED]	200	No Us
http://www.eicar.org/download/eicar.com.txt Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML like Gecko) Ch			

- 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 clicking the down arrow in the **Explore** column (or by selecting a line the column portion in the report and right-clicking) 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 is available when you are drilling down in a report:

The screenshot shows a list of fields on the left and a dropdown menu on the right. The list includes: Action, Business Readiness Rating, Client IP, Content Type, Day of Week, Destination Country, Group, Hour of Day, Malware, Method, Port, Proxy IP, Risk Score, Search Term, Server IP, Status, URL Threat Level, User, User Agent, User Agent Family, Web App Operation, and Web Application. The dropdown menu, titled 'More Fields', contains: Overview, Category, Site, Verdict, More Fields (selected), Trend Fields, and Full Log Details. A cursor points to the 'More Fields' option.

Create a Custom Reporter 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.

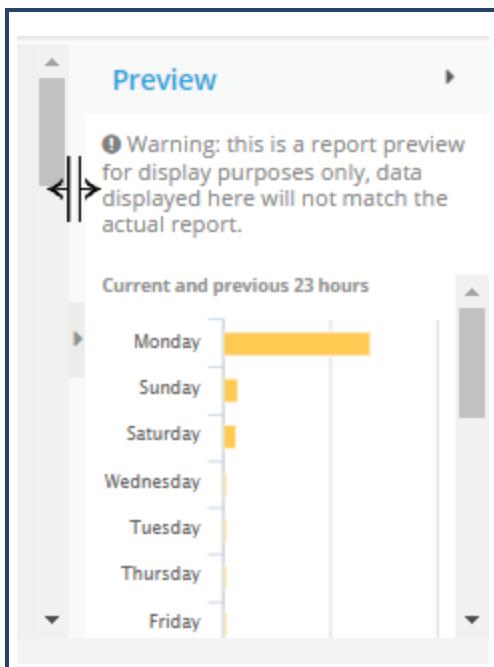
Once you have finished designing the report, you can save it for future use and run it at any time.

Step 1: Create the Report

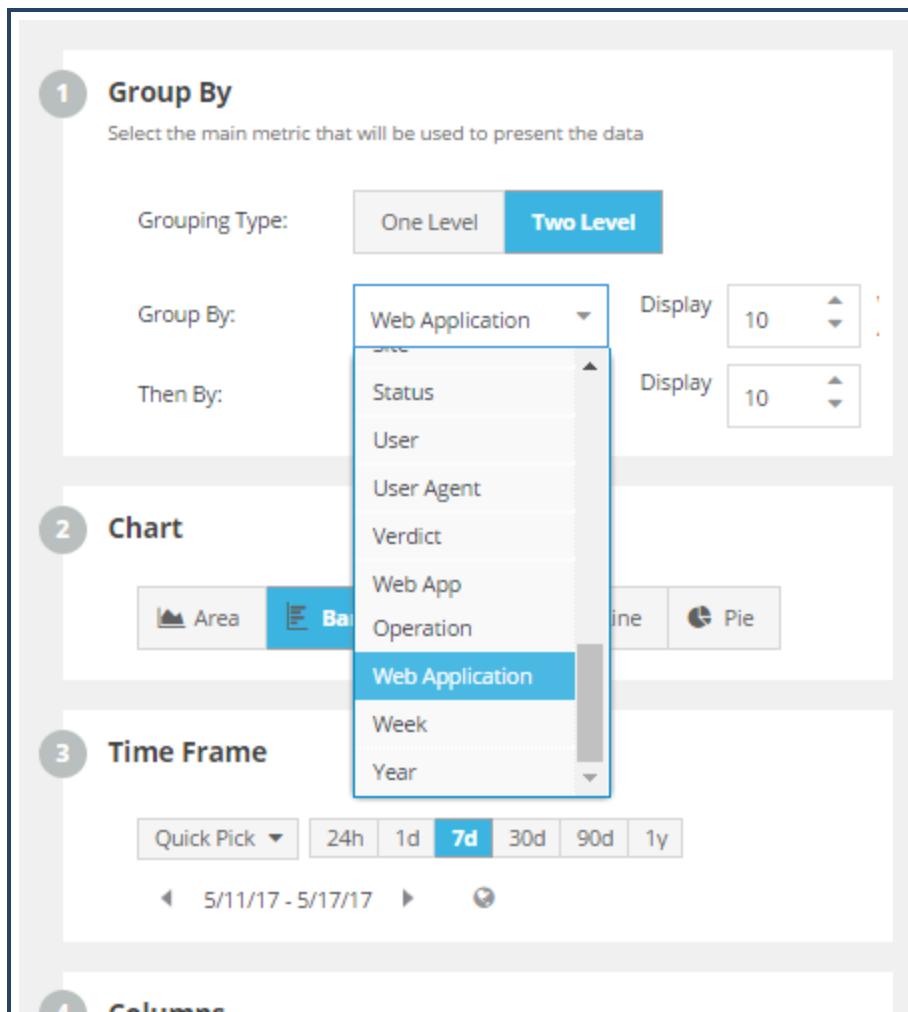
1. Select **Reports > Reporter**.
2. Select a Reporter database.



3. Click **New Report**. The six-step report designer displays in the left pane, and the report preview displays in the right pane.
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.

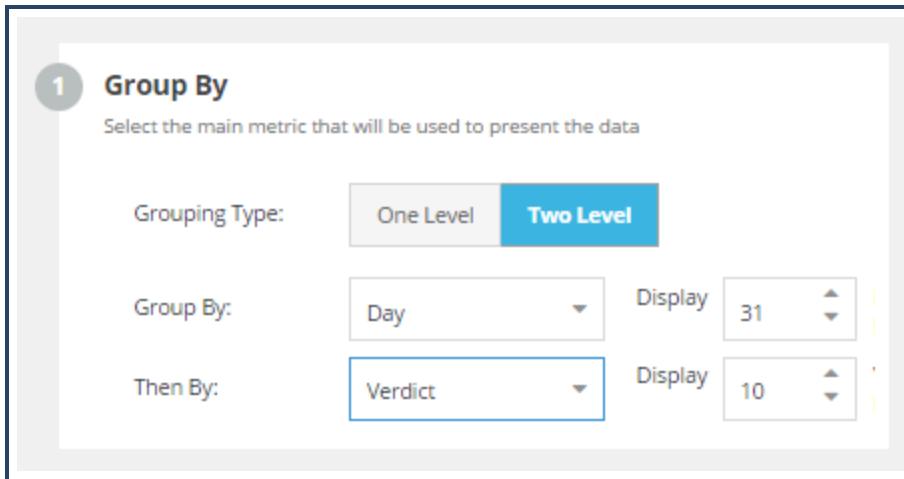


Note: If a Reporter administrator had created custom log fields in Reporter 10.x, these fields will be displayed in the list along with the standard built-in fields.

6. In the **Display** field, specify the number of items to display in the chart.

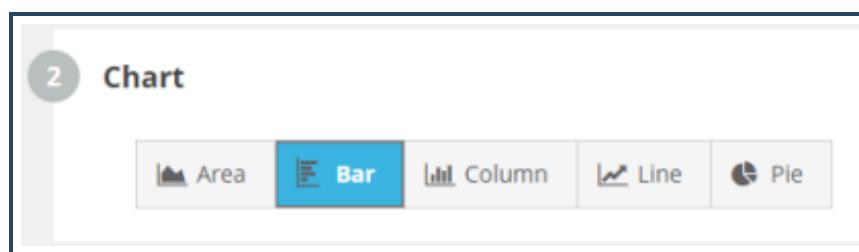
7. If you want to report on two metrics:

- Select **Two Level** for the **Group Type**. An additional row displays so that you can choose a second metric.



- In the **Then By** drop-down, select the secondary metric to report on.
 - 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

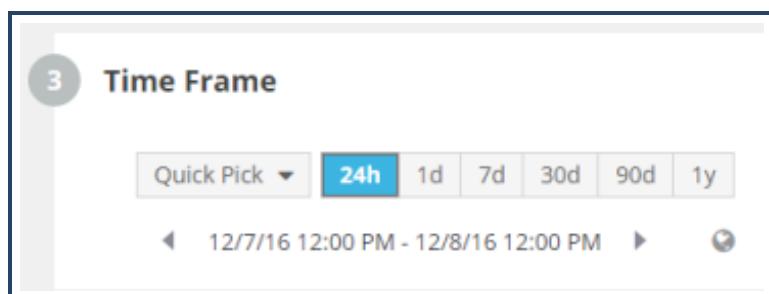
to the values that they represent. The bars are plotted horizontally and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped bar graphs display bars clustered in groups of more than one bar graph.

- **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.
- **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.

Note: 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

The screenshot shows the 'Columns' configuration screen. At the top left, there is a circular icon with the number '4'. Below it, the word 'Columns' is displayed. The main area is titled 'Display:' and contains a list of metrics with checkboxes. The checked metrics are 'Requests' and 'Total Bytes'. The unchecked metrics are 'Page Views', 'Browse Time', 'Bytes Sent', 'Bytes Received', 'Cache Bytes', 'Server Bytes', 'Cost (Bytes)', 'Cost (Time)', and 'Bytes Saved'. Below this section, there is a 'Sort By:' section with two dropdown menus. The first dropdown is set to 'Requests' and the second is set to 'Descending'.

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.

Preview

⚠ Warning: this is a report preview for display purposes only, data displayed here will not match the actual report.

Current and previous 23 hours

12/7/16 1:00 PM - 12/8/16 1:00 PM

A horizontal bar chart titled "Current and previous 23 hours" showing the total bytes transferred for various users. The x-axis represents bytes from 0 B to 190... MB. The y-axis lists users: No User, acr0q3e, abs0qwl, adf03ye, acg0b6w, acr0o7n, and abr0c5y. The bars are teal-colored.

User	Requests	Total Bytes ↓
[REDACTED]	27,529	179.1 MB
No User	2,726	26.8 MB
acr0q3e	2,476	21.6 MB
[REDACTED]	1,109	19.0 MB
abs0qwl	669	9.1 MB
adf03ye	1,999	3.1 MB
acg0b6w	465	1.7 MB
acr0o7n	462	1.6 MB
abr0c5y	499	867.2 KB
Report Totals:	275,290	1.7 GB

Note: 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 a report by setting up filters.

Here are several examples of filters you can create:

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.

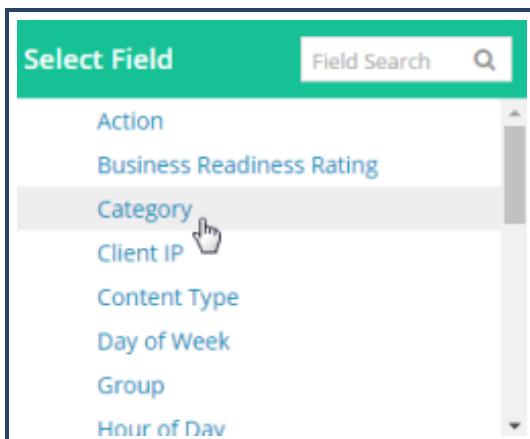
For each filter you want to add, follow the steps below.

Note: If users have report permission filters that apply to the role they're using to run the report, they will not be able to filter on any fields specified in those permission filters unless the Reporter is running 10.5 or higher.

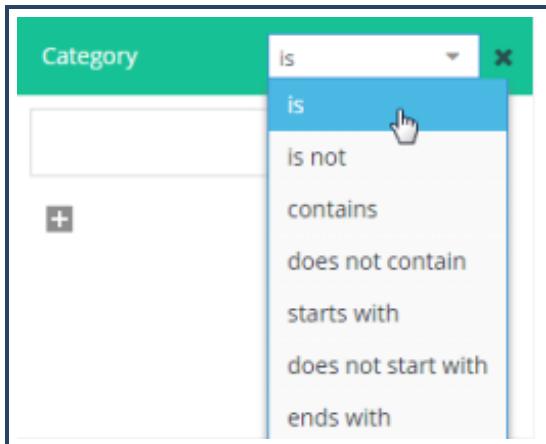
1. In the Filters section, click Add Filter.



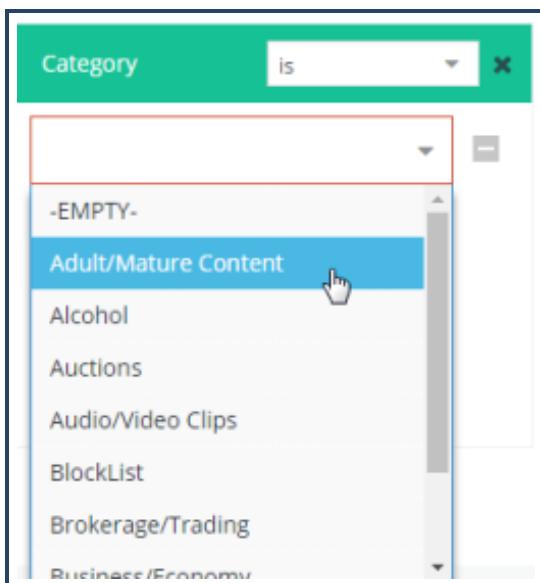
2. Select a field.



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.

The screenshot shows a 'SaveReport' dialog box. At the top left is a step indicator '6'. Below it is the title 'SaveReport'. There is a checked checkbox labeled 'Save report for running later'. A 'Name:' field contains the value 'User' with a yellow asterisk indicating it is required. A 'Description:' field is empty with the note '1024 of 1024 characters left'. A 'Group:' dropdown menu is set to 'Custom Reports'. At the bottom are three buttons: a green 'Save and Run' button, a standard 'Save' button, and a 'Cancel' button.

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 or [share the report](#) with other users. 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.

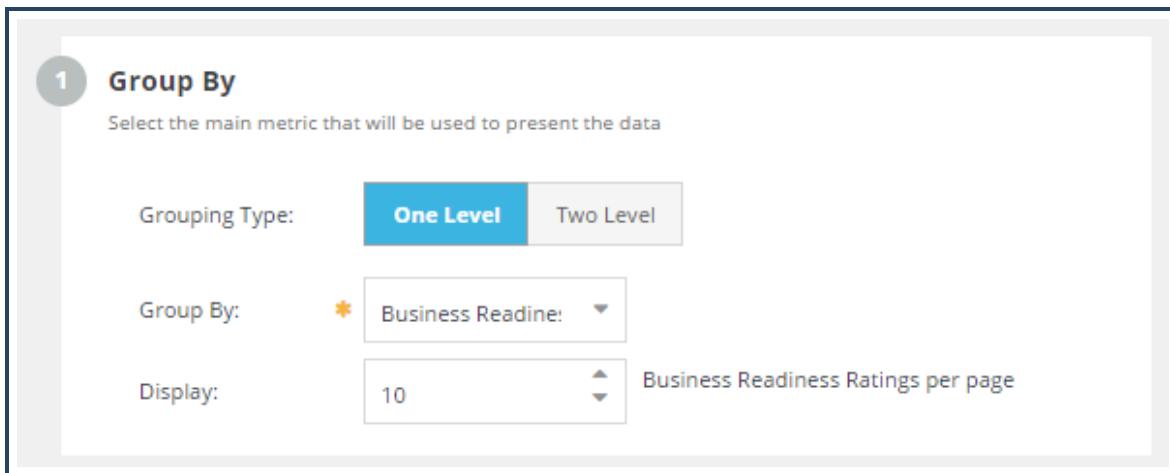
Edit Custom Reporter Reports

After designing and saving a custom report, you may want to tweak some of the settings.

Tip: For more information about any of these settings, see "Create a Custom Reporter Report" on page 708.

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.**



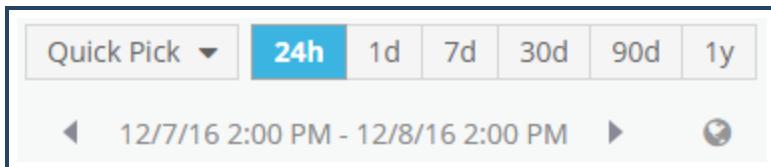
1 **Group By**
Select the main metric that will be used to present the data

Grouping Type: **One Level** Two Level

Group By: * Business Readine!

Display: 10 Business Readiness Ratings per page

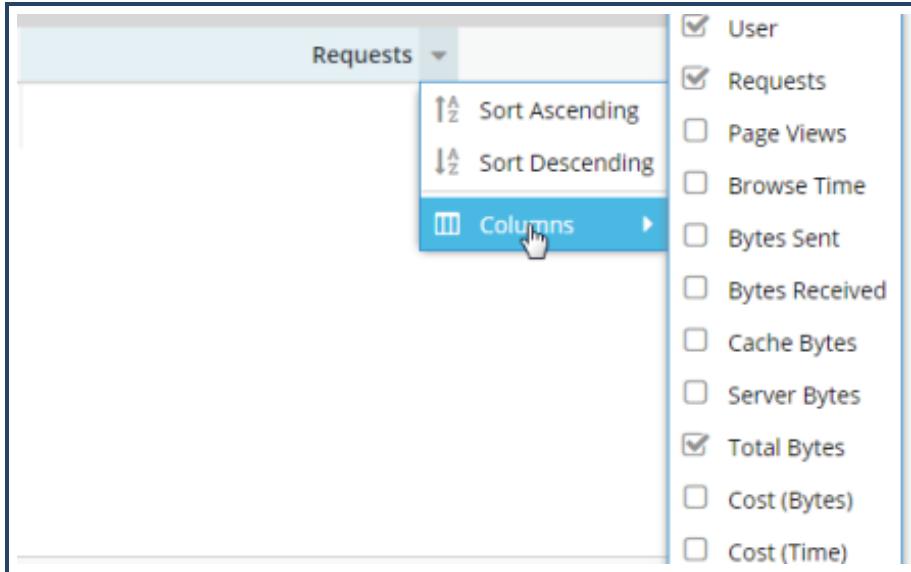
4. To modify the chart type, click the chart  icon and select the desired type.
5. The Time Frame can be changed using the time tool bar at the top of the report.



Quick Pick ▾ **24h** 1d 7d 30d 90d 1y

◀ 12/7/16 2:00 PM - 12/8/16 2:00 PM ▶ ⏴

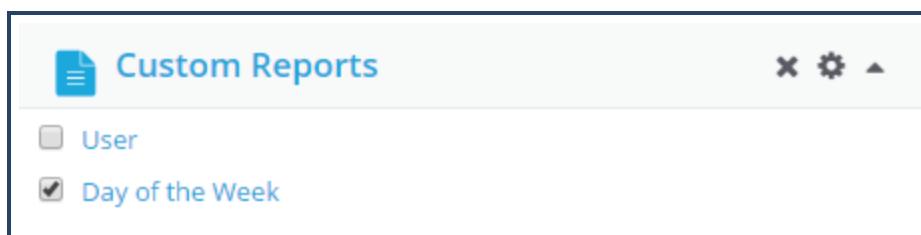
6. To modify the columns:
 - a. In the report table below the chart, hover the mouse on the right side of a column heading until you see the triangle, then click.



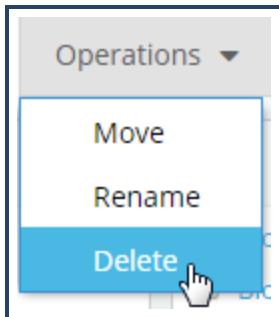
- b. Select **Columns**.
 - c. Select the columns you want to include in the report.
7. To save the custom report modifications, select **Actions > Save**.

Delete a Custom Report

1. Select **Reports > Reporter**.
2. Select the check box by each report name you want to delete.



3. Select **Operations > Delete**.



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.

Date Filters

When filtering by date, different time increments may display, depending on the type of date filter that you select. The list below describes each date filter and its associated time increments. User date filters for both reports and dashboards.

Filter	Time Increments	Description
Quick Pick	1 Day 7 Day 30 Day 90 Day YTD	Displays the time increment of data selected starting from the current date. For example: If you select 30 Day, the report displays 30 days of data from the current date.
Current	hour day week month year	Displays the current time increment of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the report displays a month of data for the current month of May.
Previous	hour day week month year	Displays the previous time increment of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the report displays a month of data for the previous month of April.

Filter	Time Increments	Description
Current and Previous	hour day week month year	Displays the current and previous time increment of data based on the beginning and ending cycle of that increment. For example: If you filter on the current and previous month, and the current month is May, the report displays two months of data for both April and May.
Before	Calendar picker	Displays an absolute date on a calendar. Displays all data for that report that exists in the database before the date chosen.
Since	Calendar picker	Displays an absolute date on a calendar. Displays all data for that report that exists in the database after the date chosen.
Custom	Calendar picker	Displays a calendar picker to choose the beginning and end of the data.
All Dates	No dates are filtered	Displays all data for all dates stored in the database. When choosing this option, all absolute dates disappear and no calendar picker is available.

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 Reporter Report" on page 708 for more information.

You can alter what is reported in the following ways:

- "Add Report Filters" below
- "Change the Report Grouping" on page 725
- "Customize Reporter Report Options" above

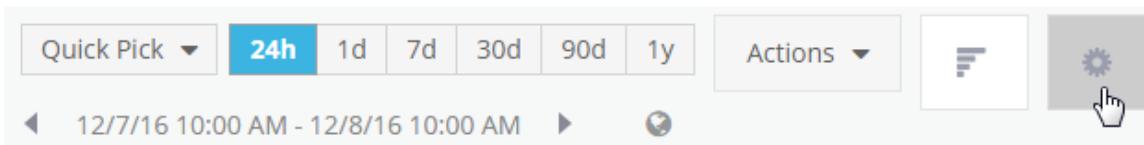
Add Report Filters

1. **Select a Reporter database.**

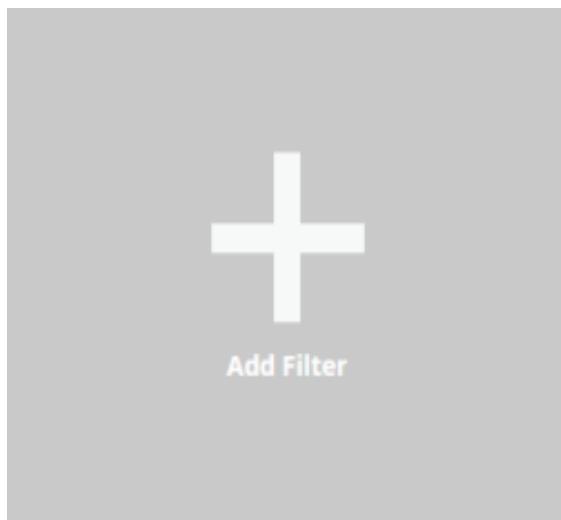
Management Center Configuration & Management



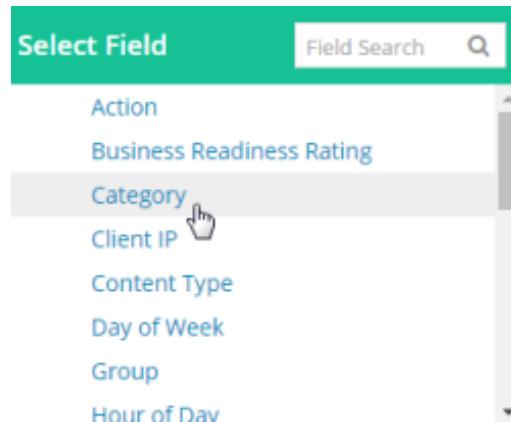
2. Select the desired report.
3. Optional—adjust the report settings (date range, format, and so on).
4. **To customize the report, select the gear icon in the upper right corner.**



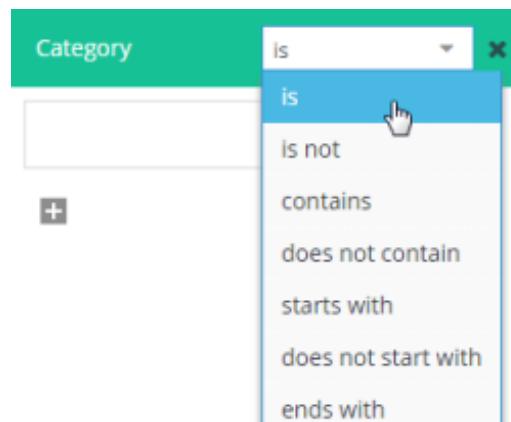
5. Add a filter.
 - a. **In the Filters section, click Add Filter.**



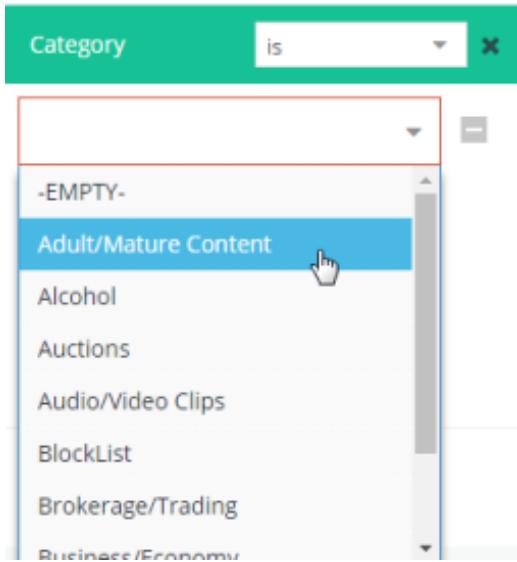
- b. **Select a field.**



- c. Select the appropriate operator. The available operators change depending on the selected action.



- d. Select or enter a value.



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

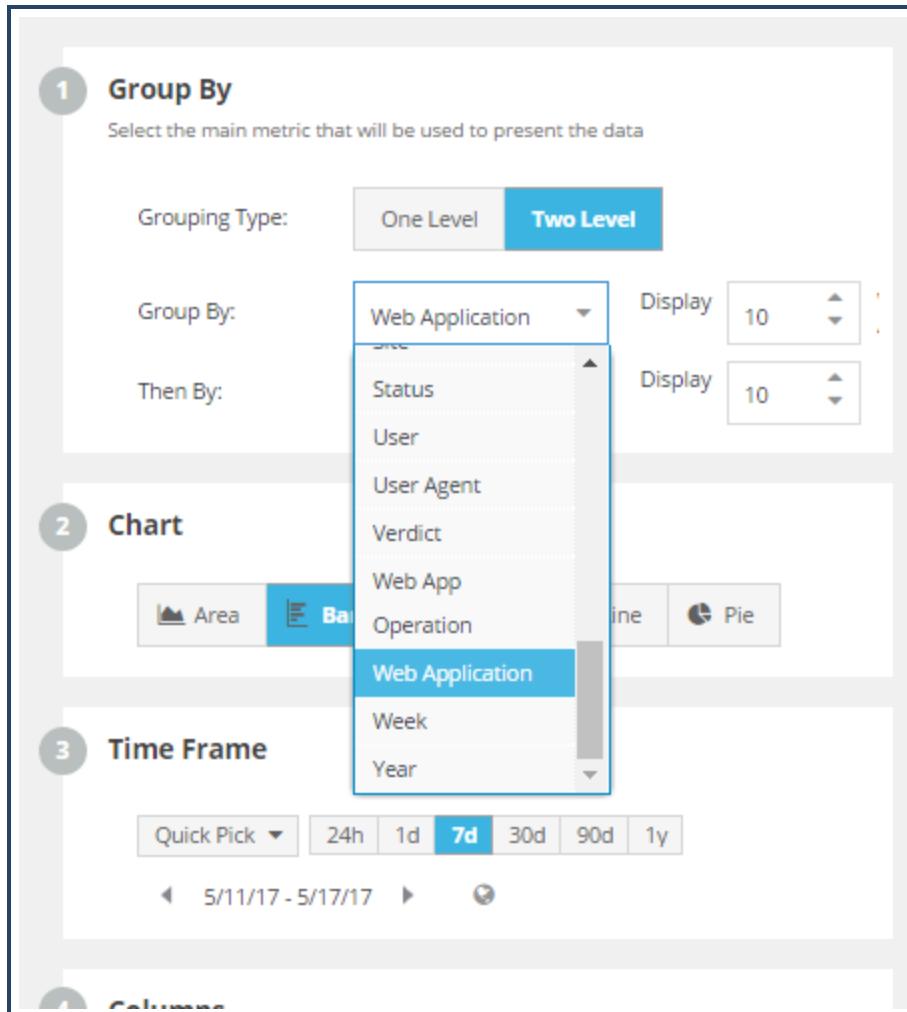
1. In the Group By section, change the Display value.

The screenshot shows a configuration interface for 'Group By'. At the top, there is a heading '1 Group By' with a note: 'Select the main metric that will be used to present the data'. Below this, there are three sections: 'Grouping Type' with a radio button for 'One Level' (which is highlighted in blue), 'Two Level' (disabled), 'Group By' with a required indicator (*), and 'Display' with a value of 10 and up/down arrows to adjust it.

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.



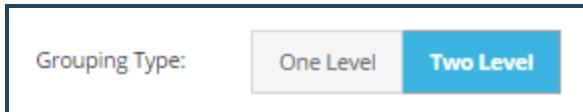
Note: If a Reporter administrator had created custom log fields in Reporter 10.x, these fields will be displayed in the list along with the standard built-in fields.

2. Change other options as desired.
3. Click **Run Report**.

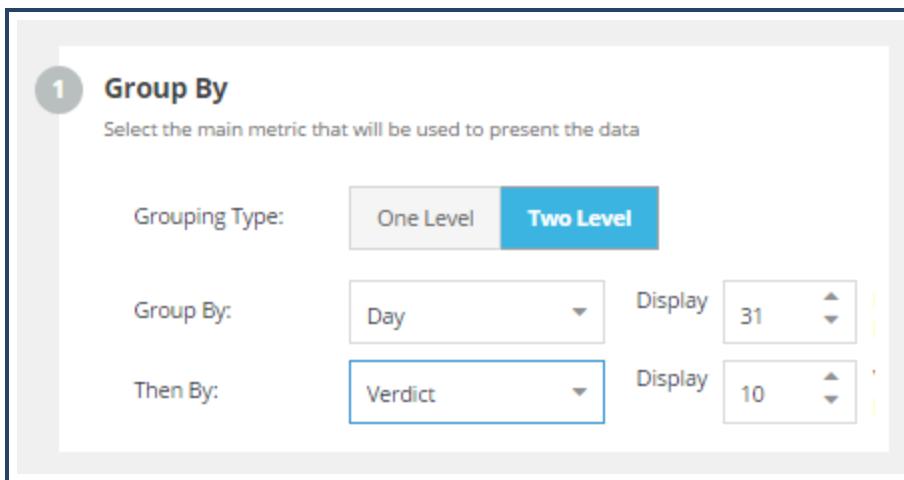
When you change the **Group By** field, a new report is generated and the name of the report is changed to match your selection. The previous report is still available in the left pane.

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.

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.
2. Click New Group. The New Report Group dialog opens.

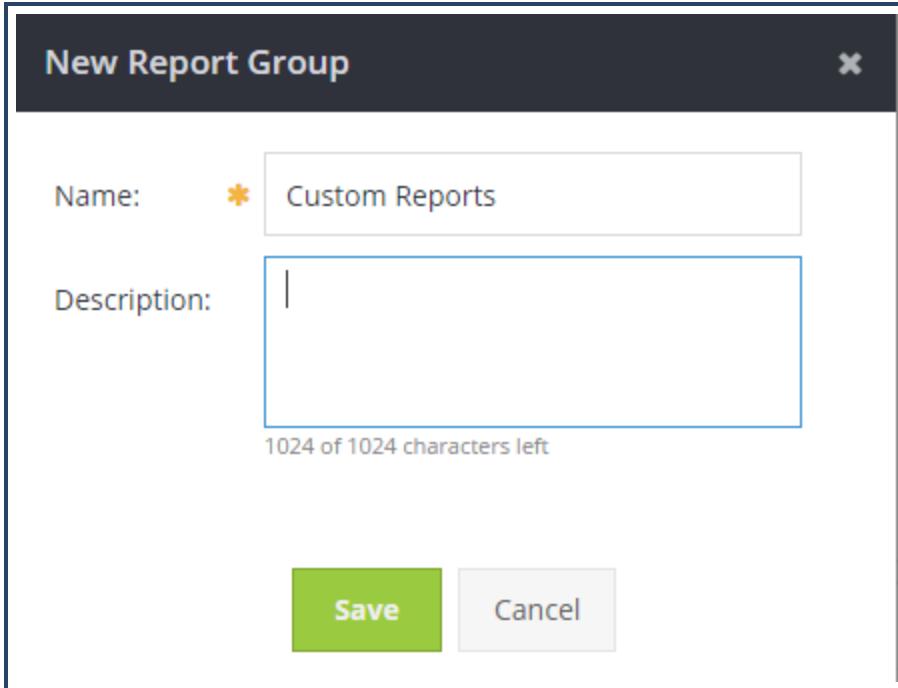
New Report Group X

Name: * Custom Reports

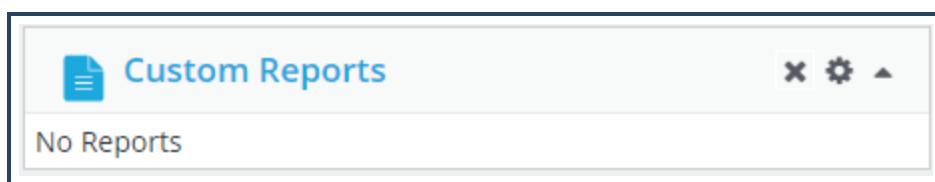
Description:

1024 of 1024 characters left

Save Cancel



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.

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.

- In the web console banner, click  and select your username.



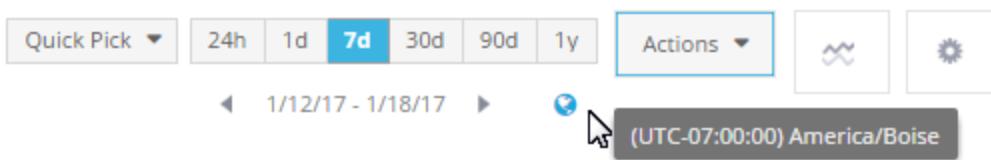
Note: The username for the standard Admin login is "Management Center."

- Select the Reporter Time Zone tab.

The screenshot shows a 'Profile' settings window. At the top, there are tabs for 'Profile', 'Change Password', 'Change Security Question', and 'Reporter Time Zone'. The 'Reporter Time Zone' tab is highlighted with a green border. Below the tabs, there is a dropdown menu labeled 'Time Zone: (UTC-07:00) America/Denver'. A note below the dropdown states: 'This time zone setting will affect all Reporter Reports, and Reporter based dashboard widgets on Reporter and Mixed dashboards'. At the bottom right of the window are 'Save' and 'Cancel' buttons.

- Select the new time zone.
- Click **Save**.
- When you open a Reporter report, verify your settings by opening a

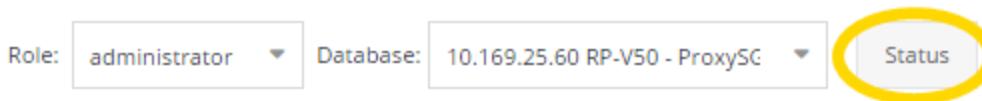
Reporter report and hovering over the time zone icon.



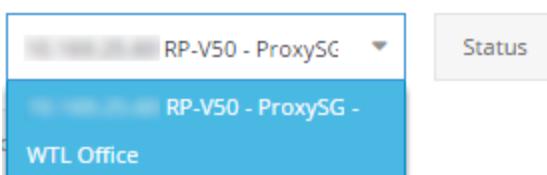
6. (Optional) Once set, you can change the time zone by clicking the time zone icon.

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.



1. Click **Reports > Reporter**.
2. **Click the Database: drop-down. The system displays the available databases.**



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		
Name	Status	Version / Type
 [REDACTED] RP-V50	 InternalServerException HTTP 500 Intern...	[REDACTED]
  [REDACTED] RP-V50	 Available	[REDACTED]

[Close](#)

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.

Caution: 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" on page 745 for more information.

Caution: 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" on page 115.

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 147.

Prerequisites

You can generate 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 660)

You can still manage ProxySG appliances that do not meet these requirements, but their statistics will be unavailable from **Statistics Monitoring**.

View Statistics Monitoring Reports

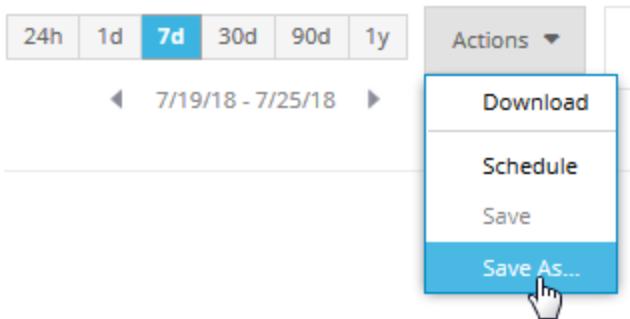
To view Statistics Monitoring reports:

1. Select **Reports > Statistics Monitoring**.
2. Select a report from **Device Performance** or **WAN Optimization**. See "Reference: Statistics Monitoring Reports in Management Center" on page 736 for descriptions.
3. From a dashboard widget, you can also "Display a Full Statistics Monitoring Report" on page 744.
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 741.
 - Add metrics to focus on specific data. See "Modify Options for Statistics Monitoring Reports" on page 739.
5. (Optional) Save the current report view in PDF, HTML, or CSV format for offline viewing. Click **Actions > Download**. The system displays the **Download** dialog.

Note: By default, the reports have a Symantec logo. You can [replace that with your logo](#).

Save a Custom Statistics Monitoring Report and Assign to a Group

1. Select **Reports > Statistics Monitoring**.
2. Generate a report by clicking the desired report link.
3. Optional—Modify the report to suit your requirements (date range, etc.).
4. Select **Actions > Save As**.



5. Name the report and provide an optional description.
6. Assign the report to an existing group or select **New Group** and follow the prompts.
7. Click **Save**.

Move, Rename, or Delete Statistics Monitoring Reports

You can only move, rename, or delete custom reports. If you select a custom report and a report residing within the **Device Performance** or **WAN Optimization** groups, these options will not be available.

1. Select **Reports > Statistics Monitoring**.
2. Select one or more reports and click **Operations**.
3. Select the desired operation.

Run Now or Schedule Report Execution

- Select **Reports > Statistics Monitoring**.
- Select one or more reports and click **Operations**.
- Select one or more reports and click **Run and Archive Now** or **Schedule**.
- Complete the job settings and run or save the job.

Troubleshooting Statistics Monitoring Reports

If the statistics monitoring dashboard shows an incorrect number of devices, see "Remove Orphan Device Count in Statistics Monitoring Dashboard" on page 746.

Reference: Statistics Monitoring Reports in Management Center

The following **Statistics Monitoring** reports are available in Management Center.

Device Performance Reports

Device reports show statistics on network traffic seen by a single ProxySG device, ProxySG appliances in a device group, or all ProxySG devices.

Report	Description	Report Format	Field	Overlays
CPU	Displays the percentage of CPU being used. By default, data shown in this report is an average of CPU usage across all devices.	Line graph		Memory, Users
Memory	Displays the percentage of memory being used. By default, data shown in this report is an average of memory usage across all devices.	Line graph		CPU, Users
Active Sessions	Provides an immediate picture of the client-server sessions and the associated proxies, services, bytes, savings, and other statistics.	Line graph		CPU, Memory
Interfaces	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.	Circle graph	Bytes Received, Bytes Sent, Packets Received, Packets Sent	

Management Center Configuration & Management

Report	Description	Report Format	Field	Overlays
Interfaces Detail	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.	Table chart		
Trend of Interfaces	Displays the trend of bytes or packets sent or received through ProxySG appliance network ports over the specified period of time.	Stack graph	Bytes Received, Bytes Sent, Packets Received, Packets Sent	
Devices	Displays a comparison of the traffic through specified ProxySG appliances measured in bytes.	Circle graph	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.	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.	Table chart		
Traffic Mix	Displays the distribution of traffic and bandwidth statistics.	Line graph, circle graph, and table chart		
Traffic Statistics	Displays the effective bandwidth, actual bandwidth, and bandwidth savings for different services.	Line graph and table chart		

WAN Optimization Reports

The **WAN Optimization** reports display statistics for ProxySG appliances with a Proxy or MACH5 Edition license.

Report	Description	Report Format Field	Overlays
Bandwidth Savings (bytes)	Displays bandwidth savings in bytes received from monitored devices.	Line graph	CPU, Memory, Users
Bandwidth Savings (cost)	Displays bandwidth savings expressed in terms of cost.	Line graph	CPU, Memory, Users
Bandwidth Savings (percent)	Displays bandwidth savings expressed as a percentage.	Line graph	CPU, Memory, Users
Bandwidth Gain	Displays bandwidth gains (including negative gains) for a specified interval.	Line graph	CPU, Memory, Users
Effective Bandwidth	Compares effective and actual bandwidth, measured in bytes.	Line graph	CPU, Memory, Users
Services	Compares specified services.	Circle graph	Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections
Services Detail	Displays bandwidth savings for different services in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain.	Table chart	
Trend of Services	Displays the trend of the specified service over a period of time.	Stack graph	Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections
Proxies	Breaks down the total number of server bytes through different proxies.	Circle graph	Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connection
Proxies Detail	Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain.	Table chart	

Report	Description	Report Format Field	Overlays
Trend of Proxies	Displays the trend of proxies versus the Server Bytes by default aggregated across all devices.	Stack graph	Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections
ADN History	Displays the number of optimized and unoptimized bytes for different peer IP addresses.	Line graph and table chart	

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.

Note: 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 736 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.**

The screenshot shows a 'Filters' dialog box with the following settings:

- Start Date:** 01/24/2017 (with a calendar icon)
- Interval:** 7 Days
- Filter:** No Filter
- Graph:** Mean Average
- Overlays:** CPU, Memory

At the bottom are 'Save' and 'Cancel' buttons.

5. Filter the report data using the options described in the following table.

Option	Description
Start Date	<p>The date and time from which report data begins.</p> <p>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.</p> <p>Specify the date in MM/DD/YY format, or click the calendar to pick a date.</p>
Interval	<p>The number of hours or days after the start date for which the report shows data.</p> <p>Note: 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.</p> <p>Select the interval from the drop-down list. Intervals can include 60 minutes, 24 hours, 7 days or 31 days.</p> <p>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.</p>
Filter	Select a filter from the drop-down list. If you select Device or Device Groups , use the to select multiple ProxySG devices or a single device group.

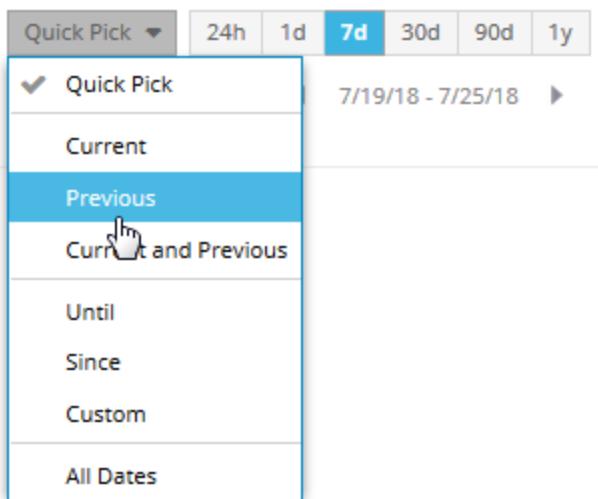
Option	Description
Graph (This option is not available for all reports)	Changes how the data is displayed. You can graph the data as the mean average for all devices (single data line) or as individual metrics for each device (one line per device). Hover the mouse cursor over a graph line to get additional information.
Field (This option is not available for all reports)	The source for which to show trending data. Select the specific item that you want to report on (by default, the first item in the drop-down list is displayed when you first open the report). The report displays the data for your selection.
Overlays (This option is not available for all reports)	Metrics that you can add to the report to help you interpret the data. You can add overlay(s) to the report. When you add overlays, the additional data displays in a legend at the bottom of the report. Use the legend to identify the appearance and color of each data type.
<p>The following is an example of the legend for the Bandwidth Savings (bytes) report:</p>  <ul style="list-style-type: none"> ● Bandwidth Savings ▲ CPU ■ Memory ★ Users 	

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 <>.



To view data from a broader or narrower time frame, select an interval from the **Quick Pick** 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.

Selected Date Range	Description	Report shows data for this period
Current Hour	The current hour.	09:00 - 10:00
Today	The current day.	October 15th
Current Week	The current calendar week, starting on Monday.	October 14th - October 20th
Current Month	The current calendar month, starting on the 1st.	October 1st - 31st
Yesterday	The previous day.	October 14th
Previous Week	The previous calendar week, starting on Monday.	October 7th - 13th
Previous Month	The previous calendar month, starting on the 1st.	September 1st - 30th
Last 7 Days	The period of time starting 7 days ago and ending today.	October 8th - October 15th
Last 31 Days	The period of time starting 31 days ago and ending today.	September 14th - October 15th

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" on page 721.

Note: 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 739.

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 Statistics Monitoring Report

Display a full report from a statistics monitoring widget.

1. Select **Dashboards > Statistics Monitoring**. The web console displays the Statistics Monitoring Dashboard.
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.

Note: 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

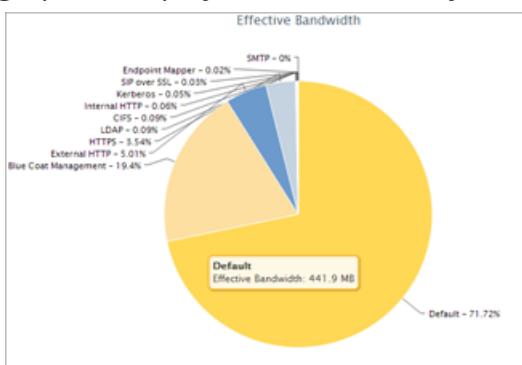
What do you want to accomplish?	Refer to this topic
Learn about different graph types.	"Statistics Monitoring Graph Types" on the next page
See the report for different dates or times.	"Change the Scope of a Statistics Monitoring Report" on page 741
Change the metrics and other data that display on the report.	"Modify Options for Statistics Monitoring Reports" on page 739
View descriptions of the Statistics Monitoring reports.	"Reference: Statistics Monitoring Reports in Management Center" on page 736
Schedule Statistics Monitoring reports.	"Schedule Statistics Monitoring Reports" on page 622

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.

Statistics Monitoring Over HTTPS

Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. Because of this change, the statistics monitoring for all ProxySG appliances will not function after upgrade to 1.7 or later (because port 9009 is blocked). To re-enable statistics monitoring on all monitored ProxySG appliances, you must do one of the following:

- Create a job on Management Center to enable statistics monitoring and manually select all target ProxySG appliances (**Jobs > Scheduled Jobs > New Job**).
- Deactivate, and then reactivate, all ProxySG appliances that previously had statistics monitoring enabled. Upon reactivation, statistics monitoring will be correctly configured. During that process Management Center does the following on the ProxySG appliance:
 - Uploads a new certificate required to enable the ProxySG appliance to trust the connection (**Configuration > SSL > CA Certificates**)
 - Creates a central management CCL that includes the new certificate (**Configuration > SSL > CA Certificates > CA Certificate Lists**)
 - Creates a new device profile that includes the CCL (**Configuration > SSL > Device Profiles**)

If you subsequently change the certificate by importing (`security ssl import external-certificate`) or generating (`security generate-ssl-certificate`) a new one, statistics monitoring will fail until you re-enable statistics monitoring using one of the procedures above.

Remove Orphan Device Count in Statistics Monitoring Dashboard

One or more "orphan" devices can be shown in the Statistics Monitoring Dashboard if the following is true:

- A user replaced a monitored device on the network with a different device that used the same IP address, without completing the **RMA Device** operation.

This caused Management Center to retain information about removed device in Statistics Monitoring Database. You can now remove these orphan devices using the following CLI command.

Syntax

```
# service-action purge-statistics-monitoring-orphans
```

After you execute the command, Management Center deletes the orphans and writes the results to syslog.

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 674
- "Customize Reporter Report Options" on page 722
- "Reporter Graph Types and Views" on page 707
- "Create Geovisual Reporter Reports" on page 682
- "Date Filters" on page 721
- "Search for Specific Report Data (Search and Forensic Report)" on page 702
- "Set Time Zone for Reporter Reports" on page 730

Statistics Monitoring

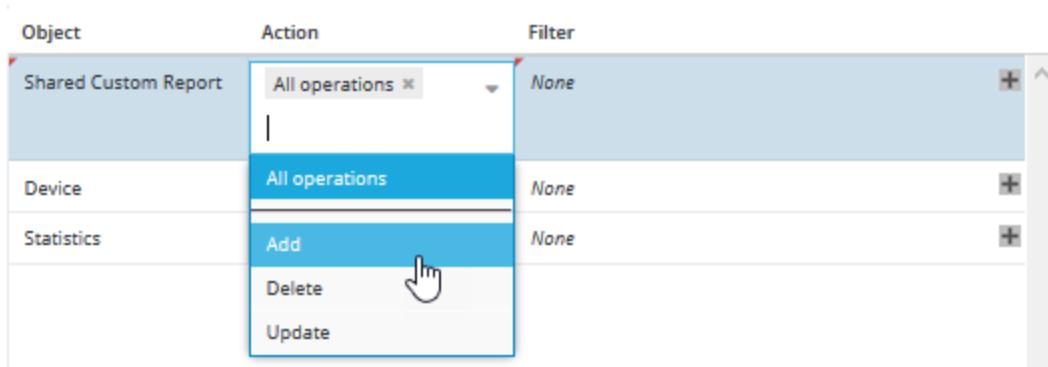
See the following for information about working with Statistics Monitoring reports:

- "View Statistics Monitoring Reports" on page 732
- "Change the Scope of a Statistics Monitoring Report" on page 741
- "Statistics Monitoring Graph Types" on page 745
- "Modify Options for Statistics Monitoring Reports" on page 739
- "Date Filters" on page 721

Create a Shared Statistics Monitoring or Reporter Custom Report

In 2.3 and later, Management Center provides a way for you to share custom reports with other users. Any user who previously had permission to view Reporter or Statistics Monitoring reports will be able to view the shared reports.

Though everyone with the correct permissions can view the reports, they cannot add, delete, or update them unless they have either the admin role or the **Shared Custom Report** permission with the appropriate action assigned to their role. To allow a user (or group or users) to perform one or more of those operations, edit their role (**Administration > Roles > Edit**) and assign the **Shared Custom Reports** permission along with the correct associated **Action**.



Note: After upgrade to 2.3, only the admin role has full permissions to add, delete, or update shared reports.

Allowed User Operations

The allowed operations for shared custom reports are as follows:

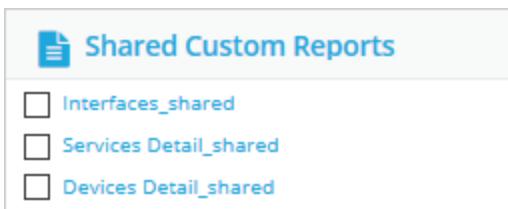
- Any user that can view statistics monitoring or Reporter reports can view shared custom reports.
- By default, users with the admin role can add, delete, or update shared custom reports.
- Other users can perform one or more of those operations, depending on the settings configured for their role.

- Even if a user does not have a delete or update permission, they can still perform those operations on reports they have created.
- Shared custom reports cannot be moved.

Find Shared Custom Reports

Two shared report groups are automatically created upon upgrade to Management Center 2.3. These groups are named as follows:

- Reporter: **Shared Custom Reporter Report**
- Statistics Monitoring: **Shared Custom Reports**



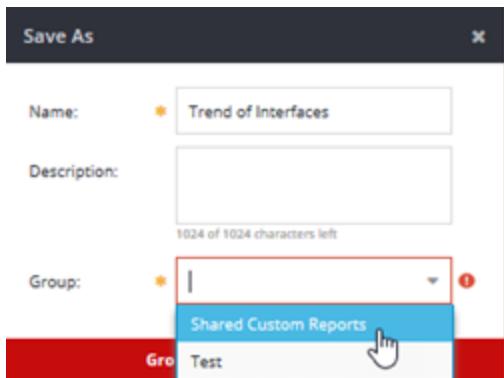
All shared custom reports are saved to one of these groups.

Create a Shared Custom Report

Users that have the **Share Custom Report Add** permission are able to create new shared custom reports.

1. If the user does not have the **Share Custom Report** permission, assign it to their role.
See "Define Roles " on page 567 and "Reference: Permissions Interdependencies" on page 499 for more information.
2. Create a custom report by editing one of the canned reports.
See "Create a Custom Reporter Report" on page 708 and "Modify Options for Statistics Monitoring Reports" on page 739 for more information.
3. When you are satisfied with your report, click **Save As**.
4. Edit the name of the report as desired.

5. In the **Save As** dialog, select **Groups > Shared Custom Reports**.



Add a Custom Logo to Downloaded Reports

By default, downloaded reports include the Symantec logo at the top of each report page. In Management Center 2.3 and later, you can add your corporate (or other) logo to your downloaded reports.

The new logo will be applied to the following reports:

- Reporter Reports
- Statistics Monitoring reports
- Summary reports

Logo Size

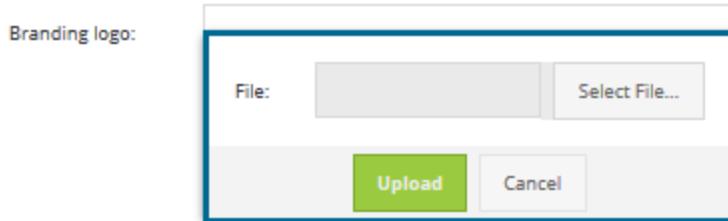
When adding a logo, ensure that the logo size is commensurate with the page header:

- Maximum width: 295 pixels
- Maximum height: 32.5 pixels

If your image is too big, the system should scale it to the proper size.

Procedure—Add Custom Logo to Reports

1. Select **Administration > Settings > Branding**.
2. Click inside the **Branding logo** text box. The system prompts you to browse for the file.



3. Click **Select File** and locate the custom logo.
4. Click **Upload**.
5. Click **Save**.

Remove Custom Logo

To remove a custom logo, select **Administration > Settings > Branding**. In the Branding log field, click **Remove**.

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.

Change Date Range for Reporter Widgets

To change the date for a Reporter widget, click the gear icon in the top-right corner of the widget.

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

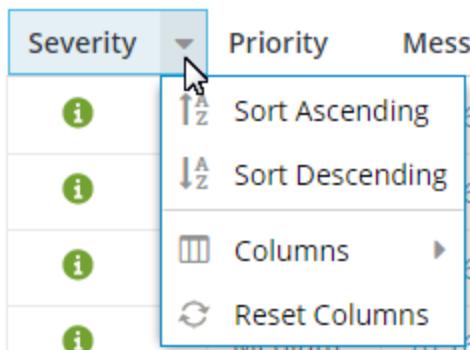
If you have multiple reports open, you can close a report other than the active one by clicking the **X** on the appropriate tab at the bottom of the screen.

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.

Severity	Priority	Message
i	Sort Ascending	[REDACTED] has failed to
i	Sort Descending	[REDACTED] has failed to
i	Columns	<input checked="" type="checkbox"/> Severity <input checked="" type="checkbox"/> Priority <input checked="" type="checkbox"/> Message <input type="checkbox"/> Count <input type="checkbox"/> Source <input checked="" type="checkbox"/> Category <input checked="" type="checkbox"/> State <input checked="" type="checkbox"/> Received <input checked="" type="checkbox"/> Acknowledged <input checked="" type="checkbox"/> Owner
i	Medium	[REDACTED]
i	Medium	[REDACTED]
i	Medium	[REDACTED]
!	High	Licen

Group Table Data

Select **Group by this field** to group the table data in accordance with that column heading.

Management Center Configuration & Management

A screenshot of a dropdown menu for column grouping in a table. The menu items are:

- Sort Ascending
- Sort Descending
- Columns (with a submenu option "Group by this field")
- Show in groups (unchecked)
- Reset Columns

The data is then grouped. In the example below, the Type column was grouped.

Name	Type	Description	Versi...	Last Edited
■ Type: WAF Application				
High Security	WAF Application		1.0	7/14/16 9:1
WAF App	WAF Application		1.1	12/7/16 9:5
■ Type: Universal VPM Policy				
UP_Test	Universal VPM P...		1.1	10/19/16 5
UP Test2	Universal VPM P...		1.0	11/2/16 9:1
■ Type: VPM				
TestVPM	VPM		1.1	8/18/16 4:3
VPM1	VPM		1.5	12/5/16 7:0
■ Type: Tenant Determination File				
Landlord Poli...	Tenant Determin...		1.0	7/5/16 7:25
■ Type: SSLV Lists				
SSLV Policy	SSLV Lists	policy for SSLV lists	1.0	12/9/16 7:5
testSSLVonline	SSLV Lists		1.1	12/7/16 11

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.

1. Select **Reports > Statistics Monitoring**.
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.

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.

1. Select **Administration > Settings**. Select **General**. General fields display on the right.
2. Enter a decimal value.
3. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

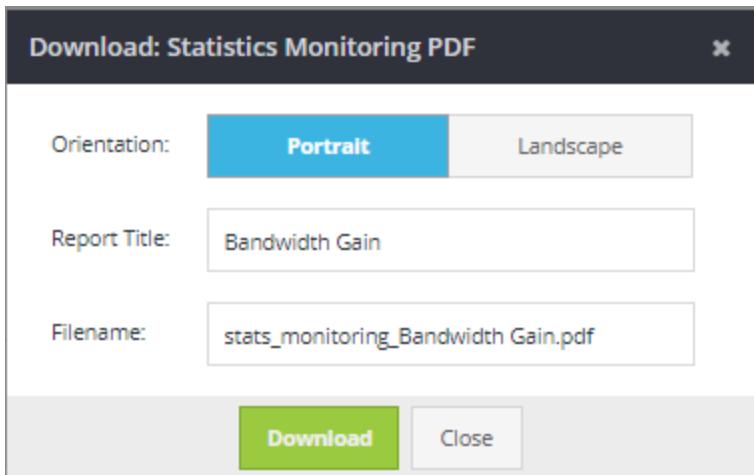
If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

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.

Management Center Configuration & Management



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.

Order ↑	Name	Type	Widget	Description
1, 2, 3, etc. The order is displayed from left to right on the dashboard tab beginning with 1 on the left.	The name of the dashboard as it appears on the Dashboard tab.	Reporter - displays only Reporter widgets on the dashboard. WAF Reporter - displays only WAF widgets on the dashboard Mixed - Can display data from all widgets on the dashboard. Statistics Monitoring - displays only Statistics Monitoring widgets on the dashboard.	Each dashboard can display multiple widgets. For a quick reference of what is displayed on each dashboard, view the widget count for each dashboard.	The description helps to differentiate the dashboard type, and the widgets within the dashboard.

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 [Integrate Reporter into Management Center](#).

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.

Note: 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.

Note: 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

The **Dashboards** section of Management Center enables you to get a quick view of your device health and statistics.

Dashboards

A *dashboard* provides a simplified view of data in *widgets*. Management Center displays the following default dashboards after users "Log into the Web Console" on page 35:

- Home Dashboard

The home dashboard displays when you log into the web console by default. The dashboard displays **Device Health** and **Top Problem Devices** widgets by default, but you can add and remove widgets to any dashboard.

- 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.

Note: 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.

For help with managing dashboards, see the following:

- "Manage Dashboards" on page 758
- "Change the Dashboard Layout or Refresh Rate" on page 765
- "Web Console Overview" on page 29
- "Display a Full Statistics Monitoring Report" on page 744
- "View Statistics Monitoring Reports" on page 732
- "Change the Scope of a Statistics Monitoring Report" on page 741

- "Schedule Statistics Monitoring Reports" on page 622
- "Monitor Device Health " on page 147
- "Enable Device Health and Statistics Monitoring" on page 155
- "View and Edit Device Information" on page 69

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 758.

For help with managing widgets, see the following:

- "Add a Widget to the Current Dashboard" below
- "Customize Report Widgets" on page 752
- "Add the Bookmarked Devices Widget" on page 764
- "Monitor Device Health " on page 147

Add a Widget to the Current Dashboard

1. Select the **Dashboards** tab.
2. Click **Add Widgets**.

Note: 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

Management Center Configuration & Management

Behavior, WAN Optimization, Web Applications. The right pane updates with the list of report widgets for the selected report type.

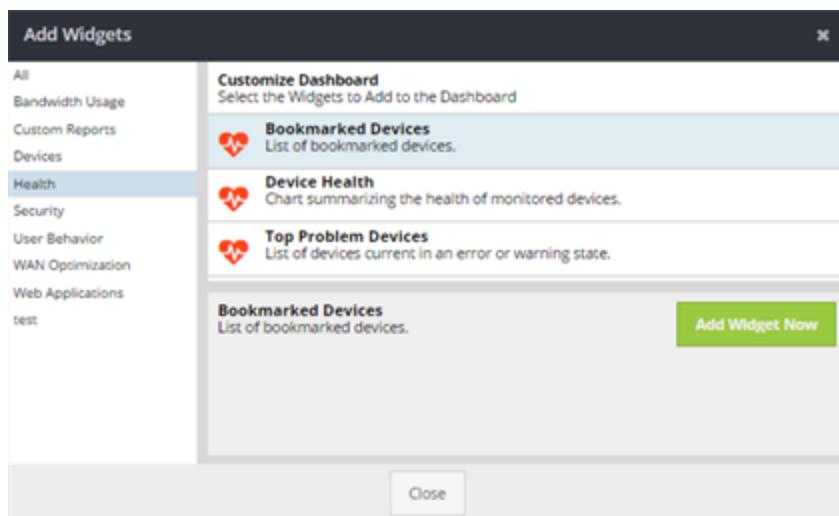
4. Select the report widget you want to add.
5. For Reporter widgets, select the **Database**, **Layout**, and **Date Filter**.
6. Click **Add Widget Now**.
7. Repeat steps 3 to 6 to add more widgets, and then click **Close**.

To customize the layout and widgets of your dashboard, see "Change the Dashboard Layout or Refresh Rate" on page 765.

Add the Bookmarked Devices Widget

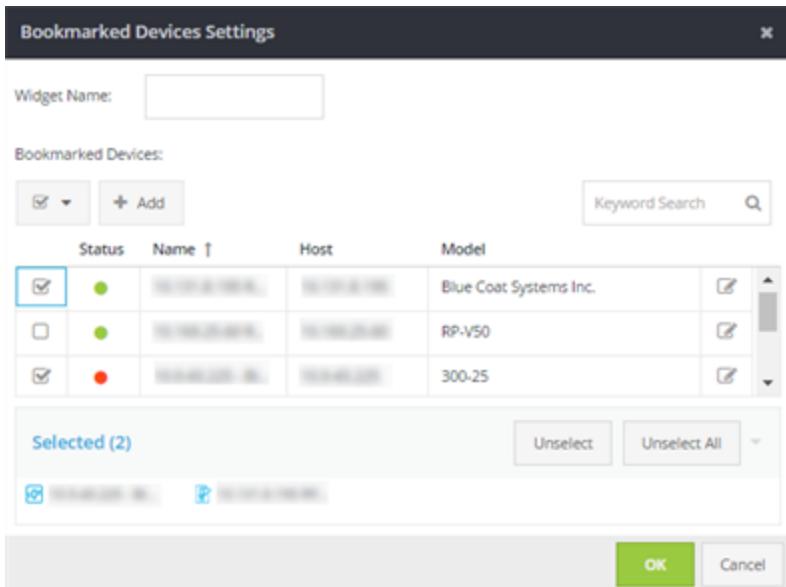
The Home dashboard displays the Device Health and the Top Problem Devices widgets by default after you log in. To add a widget specifically to view real-time data for favorite devices, add the **Bookmarked Devices** widget to a dashboard.

1. From the Home dashboard, select **Add Widgets**. The web console displays the Add Widgets wizard.
2. **Scroll to Health and select Bookmarked Devices.**

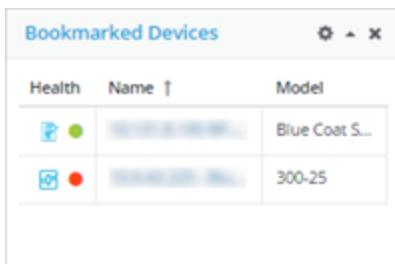


3. Select **Add Widget Now**. Click **Close**. The dashboard displays an empty widget.
4. **Select Add Devices. Give the widget a name and select the devices that you want to monitor in the dashboard.**

Management Center Configuration & Management



5. Select the devices that you want to "bookmark" as your favorite devices and click OK. The new widget displays the selected devices.



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:

- 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.

Administate Management Center

- "Define Management Center Settings" below
- "Configure General System Settings" on page 769
- "Upgrade Management Center" on page 811
- "Downgrade Management Center" on page 815
- "Back Up the Management Center Configuration" on page 627
- "Encrypt Sensitive System Data" on page 47
- "Restore a Management Center Backup Configuration" on page 817
- "Configure Management Center Failover" on page 818

Define Management Center Settings

Use the **Administration > Settings** page to modify Management Center device-specific settings, for example, diagnostic settings, SNMP, and authentication settings.

- [General](#)

Configure General Settings about managed devices, policy revisions and users and backups.

- [Alerts](#)

Configure alerts for device errors.

- [LDAP](#)

Authenticate users against LDAP.

- [Active Directory LDAP](#)

Authenticate users against Active Directory.

- [RADIUS](#)

Authenticate users against RADIUS.

- [SMTP Alerts](#)

Configure SMTP communication settings.

- [SNMP Alerts](#)

Configure SNMP communication settings.

- [HTTP Proxy](#)

Configure proxy settings.

- [Diagnostics](#)

Configure the Logging level for logs (collected from devices).

- [Housekeeping](#)

Configure auditing and job execution settings.

- [SNMP Settings](#)

Configure SNMP community settings.

- [Mail Settings](#)

Configure mail server settings.

- [Consent Banner](#)

Specify consent banner settings.

- [Hardware Monitor Settings](#)

Set hardware monitoring thresholds.

- [Device Communication](#)

Identify the hostname used in Management Center's HTTPS server certificate.

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.
3. Specify General settings.

Setting	Input Value/Format
Bandwidth Cost per GB*	<input type="text"/> See "Set Bandwidth Cost for Reports" on page 756
Device Polling Interval*	<input type="text"/> See Set the Device Polling Interval
Number of backup slots*	<input type="text"/> "Set the Number of Backup Slots" on page 195
Maximum number of policy revisions to store*	<input type="text"/> "Set the Maximum Number of Policy Versions to Store in Management Center" on page 475
Maximum number of script revisions to store*	<input type="text"/> Set the Maximum Number of Script Revisions to Store in Management Center
Inactivity timeout (minutes)*	<input type="text"/> Specifies the number of minutes before an inactive user is logged out. Users are warned 30 seconds before they are logged out.

Setting	Input Value/Format
Inactivity timeout exclusions	text: Enter comma-separated usernames The list of usernames that should be excluded from the Inactivity timeout setting.
Is Reset Password enabled?*	false true See "Reset Password" on page 556
Reset Password Email Subject*	text: Management Center Reset Password
Reset Password Email Message*	text: Enter the body text of the email that will be sent upon a user's request of a password reset. Click OK .

4. Click **Save** and then **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.

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.

Note: The audit log displays system, web-access and web logs, if configured. To access remote system logs, from the CLI enter # rsyslog-output.

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 below.
2. Inspect the data recorded for transactions. See "Audit Transactions" on page 846.
3. (Optional) "Customize the Audit Log" on page 849 to focus on specific transaction data.

Note: 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.

Audit Log Viewer

The screenshot shows the Audit Log Viewer interface. On the left is a table with columns: Operation Ti..., Operating User, Object Type, Operation Ty..., Info 1, and Info 2. The table contains 12 rows of audit log data. On the right is a 'Filters' panel with sections for Object (Role), Operation (- All -), User (- All -), and Record Type (EVENT). Buttons for 'Apply', 'Clear', and a gear icon are at the top of the filters panel.

Operation Ti...	Operating User	Object Type	Operation Ty...	Info 1	Info 2
2017-01-13 0...	SYSTEM	User	Update	Ad...	
2017-01-13 0...	SYSTEM	Authentication	Authenticated	Ad...	10....
2017-01-13 0...	SYSTEM	License	Validated		OK
2017-01-13 0...	SYSTEM	License	Validated		OK
2017-01-13 0...	SYSTEM	Device	Monitoring E...		
2017-01-13 0...	SYSTEM	Device	Monitoring E...		
2017-01-13 0...	SYSTEM	Device	Monitoring E...		
2017-01-13 0...	SYSTEM	License	Validated		OK
2017-01-13 0...	SYSTEM	Housekeepin...	Housekeepin...	4	
2017-01-13 0...	SYSTEM	Housekeepin...	Housekeepin...	File...	OK
2017-01-13 0...	SYSTEM	Housekeepin...	Housekeepin...	Ale...	OK

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.

CLI Shell Audit Log Notes

When users log into the CLI shell of a device or of Management Center, the following is logged:

- Session open, close, and failure
- User, host, port, browser IP address, and close reason (if applicable)
- **Info 3**, in the [Audit Log](#), is an internal identifier used to correlate open/closed events. The identifier is unique until Management Center reboots.

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.

Setting	Description	Input Value/Format
Enable*	Specify whether an explicit proxy is configured.	false true
HTTP Proxy IP or hostname	Specify the IP address or hostname of proxy server.	Example: <code>https://<IP_address></code>
HTTP Proxy Port	Specify the port for the proxy server.	Example: 8082
Username	If necessary, enter the username to authenticate to the proxy.	Example: <code>admin</code>
Password	If necessary, enter the password to authenticate to the proxy.	Example: <code>admin123</code>

3. Click **Save** and then **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 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.

Log Level	Description
DEBUG	Logs detailed informational events and is most useful when you are attempting to diagnose problems.
INFO	Logs high-level informational messages only.
WARN	Logs potentially harmful events.
ERROR	Logs all errors that do not cause the system to restart.

Log Level	Description
OFF	Disables logging. The Master Log cannot be disabled.
ALL	Logs everything. Applicable only to the Master Log.

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.

Management Center Configuration & Management

Diagnostics

Master Logging Level:

* INFO

General

Security Logging Level:

* OFF

Networking Logging Level:

* OFF

Device Management Logging Level:

* OFF

Device Plugins

Content Analysis Plugin:

* OFF

Malware Appliance Plugin:

* OFF

PacketShaper Plugin:

* OFF

Reporter Device Plugin:

* OFF

SG Device Plugin:

* OFF

SSLV Device Plugin:

* OFF

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.

Setting	Description	Input Value/Format
Run every n hours.* Default is 12.	The value represents (in hours) how often to run a full audit.	numeric using up and down arrows
Number of days of audit records to keep.* Default is 120.	The value represents the number of days that audit records are kept.	numeric using up and down arrows
Number of days of job execution records to keep.* Default is 120.	The value represents the number of days that job executions records are kept.	numeric using up and down arrows
Number of days of closed alert records to keep.* Default is 120.	The value represents the number of days that alerts are kept after being closed.	numeric using up and down arrows

4. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

Configure Mail Settings

The settings on the **Administration > Settings > Mail Settings** page are for configuring the server that Management Center uses to send alerts related to users of the system, for example, password resets.

Note: The options on this page do not enable alerts for managed devices. To receive monitored device event notifications via email, you

must configure [SMTP alerts](#). Management Center stores the settings so that SMTP alerts (emails) can be transmitted and received correctly.

1. Select **Administration > Settings**.
2. Select **Mail Settings**. Mail settings display on the right. An asterisk denotes fields that are mandatory.
3. Specify email settings.

Setting	Description	Input Value/Format
Mail Server*	The SMTP mail server to use for outgoing mail.	Example: smtp.organization.com
Mail Server Port*	The Port that the SMTP mail server uses.	Example: 25
From address*	The e-mail address from which e-mails are sent.	Example: bccm@organization.com
Username	The User name used to access the SMTP mail server.	Example: joe.admin
Passphrase	The password required to access the SMTP mail server	Example: admin123

4. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

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).

Tip: The MIBs are available on the [Downloads](#) page. Refer to the *Management Center Release Notes* for information on MIBs. See "Access Management Center Software Downloads and Documentation" on page 27 for more information about accessing Symantec downloads.

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. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration. See **Community** in "Configure SNMP Alerts" on page 131.

Management Center: SNMP Monitoring Best Practices

Systems and network administrators are challenged with ensuring the reliability, stability, and availability of mission-critical systems in the corporate network. SNMP has made that task easier by making devices simpler to monitor, maintain, and upgrade. The network administrator is alerted about situations that require administrative attention, but even the best of appliances will need closer monitoring and observation when problems arise either in the network or in the application.

Management Center offers specific features (SNMP elements), which allow close resource monitoring for day-to-day informational use. It also provides information that allows users to prioritize network needs and to focus and allocate resources to maximize reliability.

Administrators need to determine when their Management Center is utilizing resources outside of normal operation ranges or is approaching the resource capacity limits of the system so that they can take appropriate corrective action.

This document defines a set of metrics that help characterize load conditions on Management Center appliances running MC 2.x or later and identifies the SNMP sources of statistics that enable monitoring of these resources.

MIBs Used With Management Center

Management Center uses private and standard MIBs. This document does not describe all of these MIBs. The information in this document provides information only about the MIBs that provide the best data for monitoring Management Center resources.

Refer to Management Center MIB Files for more information about the MIBs and how to download them.

BLUECOAT-SG-SENSOR-MIB

The SENSOR-MIB monitors the values of the various environmental sensors present on the appliance.

Parameters that you can monitor with the SENSOR-MIB include:

- Bus Temperature
- CPU Temperature
- Fan
- CPU Fan
- Bus Voltage
- CPU Voltage
- Power Supply

The SENSOR-MIB trap variables and their values are described in the following table.

Trap Variable	Description	Value
deviceSensorName	The textual name of the sensor	---
deviceSensorUnits	The units of sensor measurements.	other(1) truthvalue(2) specialEnum(3) volts(4) celsius(5) rpm(6)

Trap Variable	Description	Value
deviceSensorValue	<p>Reports the most recent measurement seen by the sensor.</p> <p>Measurements are interpreted based on the deviceSensorUnits value.</p>	other(1) - a measure other than those listed below truthvalue(2) - true(1), false(2) specialEnum(3) - user defined enumerated values volts(4) - electrical potential as a fixed point number celsius(5) - temperature as a fixed point number rpm(6) - revolutions per minute in nonnegative numbers
deviceSensorCode	Interprets the deviceSensorValue.	ok(1) unknown(2) notInstalled(3) voltageLowWarning(4) voltageLowCritical(5) noPower(6) voltageHighWarning(7) voltageHighCritical(8) voltageHighSevere(9) temperatureHighWarning(10) temperatureHighCritical(11) temperatureHighSevere(12) fanSlowWarning(13) fanSlowCritical(14) fanStopped(15)
deviceSensorStatus	Indicates the operational status of the sensor.	ok(1) unavailable(2) nonoperational(3)

The error messages produced by the deviceSensorCode are described in the following table.

Message	Status
OK(1)	Normal

Management Center Configuration & Management

Message	Status
voltageLowCritical(5) noPower(6) voltageHighCritical(8) voltageHighSevere(9) temperatureHighCritical(11) temperatureHighSevere(12) fanSlowCritical(14) fanStopped(15)	Critical-Immediate attention is required.
unknown(2) notInstalled(3)	Minor
voltageLowWarning(4) voltageHighWarning(7) temperatureHighWarning(10) fanSlowWarning(13)	Warning

Listing SENSOR-MIB Values From the CLI

The Management Center CLI lists the current SENSOR-MIB values from the enable command level:

```
# enable
Password:
# show BLUECOAT-SG-SENSOR-MIB
```

DEVICE SENSOR INDEX	DEVICE TRAP ENABLED	DEVICE SENSOR UNITS	DEVICE SENSOR SCALE	DEVICE VALUE	DEVICE SENSOR CODE	DEVICE STATUS	DEVICE TIME STAMP	DEVICE SENSOR NAME
	DEVICE TRAP ENABLED	DEVICE SENSOR UNITS	DEVICE SENSOR SCALE	DEVICE VALUE	DEVICE SENSOR CODE	DEVICE STATUS	DEVICE TIME STAMP	DEVICE SENSOR NAME
	DEVICE TRAP ENABLED	DEVICE SENSOR UNITS	DEVICE SENSOR SCALE	DEVICE VALUE	DEVICE SENSOR CODE	DEVICE STATUS	DEVICE TIME STAMP	DEVICE SENSOR NAME
1	false	specialEnum	0	0	notInstalled	notInstalled	2677	PWR button1
2	false	specialEnum	0	0	ok	ok	2677	PSU 2 status1
3	false	specialEnum	0	16	noPower	ok	2677	PSU 1 status1
4	false	specialEnum	0	0	notInstalled	notInstalled	2677	CPU CATERR1
5	false	specialEnum	0	128	notInstalled	notInstalled	2677	CPU status1
6	false	specialEnum	0	0	notInstalled	notInstalled	2677	Chassis opened1
7	false	specialEnum	0	0	notInstalled	notInstalled	2677	BIOS2 Boot Fail1
8	false	specialEnum	0	0	notInstalled	notInstalled	2677	BIOS1 Boot Fail1
9	false	volts	0	0	notInstalled	notInstalled	2677	SSL VPTX
10	false	volts	0	0	notInstalled	notInstalled	2677	SSL PLL
11	false	volts	0	0	notInstalled	notInstalled	2677	SSL core
12	false	volts	-4	18228	ok	ok	2677	SAS IO
13	false	volts	-3	1048	ok	ok	2677	SAS core
14	false	volts	-3	1528	ok	ok	2677	PCH SAS
15	false	volts	-2	112	ok	ok	2677	PCH core
16	false	volts	-3	752	ok	ok	2677	Memory VT
17	false	volts	-3	1528	ok	ok	2677	Memory I/O
18	false	volts	-3	1064	ok	ok	2677	CPU VT
19	false	volts	-4	9212	ok	ok	2677	CPU sys agent
20	false	volts	-3	1813	ok	ok	2677	CPU PLL
21	false	volts	-4	9114	ok	ok	2677	CPU core

Management Center Configuration & Management

22	false	volts	-3	1264	ok	ok	2677	BMC PLL
23	false	volts	-3	1568	ok	ok	2677	BMC memory
24	false	volts	-3	3072	ok	ok	2677	Battery
25	false	volts	-4	50232	ok	ok	2677	+5V standby
26	false	volts	-4	50508	ok	ok	2677	+5V main bus
27	false	volts	-2	331	ok	ok	2677	+3.3V standby
28	false	volts	-3	3328	ok	ok	2677	+3.3V main bus
29	false	volts	-2	1196	ok	ok	2677	+12V main bus 2
30	false	volts	-2	1196	ok	ok	2677	+12V main bus 1
31	false	volts	-4	11172	ok	ok	2677	+1.1V standby
32	false	rpm	3	7	ok	ok	2677	Sys fan 6 rear
33	false	rpm	2	81	ok	ok	2677	Sys fan 6 front
34	false	rpm	3	7	ok	ok	2677	Sys fan 5 rear
35	false	rpm	3	8	ok	ok	2677	Sys fan 5 front
36	false	rpm	2	69	ok	ok	2677	Sys fan 4 rear
37	false	rpm	2	81	ok	ok	2677	Sys fan 4 front
38	false	rpm	3	7	ok	ok	2677	Sys fan 3 rear
39	false	rpm	2	81	ok	ok	2677	Sys fan 3 front
40	false	rpm	2	68	ok	ok	2677	Sys fan 2 rear
41	false	rpm	2	81	ok	ok	2677	Sys fan 2 front
42	false	rpm	2	69	ok	ok	2677	Sys fan 1 rear
43	false	rpm	2	81	ok	ok	2677	Sys fan 1 front
44	false	rpm	0	0	notInstalled	notInstalled	2677	DC PSU 2 fan R
45	false	rpm	0	0	notInstalled	notInstalled	2677	DC PSU 2 fan F
46	false	rpm	0	0	notInstalled	notInstalled	2677	DC PSU 1 fan R
47	false	rpm	0	0	notInstalled	notInstalled	2677	DC PSU 1 fan F
48	false	rpm	3	12	ok	ok	2677	AC PSU 2 fan
49	false	rpm	0	0	notInstalled	notInstalled	2677	AC PSU 1 fan
50	false	celsius	0	28	ok	ok	2677	System R temp
51	false	celsius	0	25	ok	ok	2677	System L temp
52	false	celsius	0	31	ok	ok	2677	System C temp
53	false	celsius	0	0	notInstalled	notInstalled	2677	SSL card temp
54	false	celsius	0	35	ok	ok	2677	SAS card temp
55	false	celsius	0	17	ok	ok	2677	PSU inlet temp
56	false	celsius	0	21	ok	ok	2677	PSU 2 core temp
57	false	celsius	0	0	notInstalled	notInstalled	2677	PSU 1 core temp
58	false	celsius	0	44	ok	ok	2677	PCH temp
59	false	celsius	1	2	ok	ok	2677	Midplane R temp
60	false	celsius	0	16	ok	ok	2677	Midplane L temp
61	false	celsius	0	17	ok	ok	2677	Midplane C temp
62	false	celsius	0	13	ok	ok	2677	Front panel temp
63	false	celsius	0	0	notInstalled	notInstalled	2677	DIMM C2 temp
64	false	celsius	0	0	notInstalled	notInstalled	2677	DIMM C1 temp
65	false	celsius	0	23	ok	ok	2677	DIMM B2 temp
66	false	celsius	0	23	ok	ok	2677	DIMM B1 temp
67	false	celsius	0	24	ok	ok	2677	DIMM A2 temp
68	false	celsius	0	24	ok	ok	2677	DIMM A1 temp
69	false	celsius	0	33	ok	ok	2677	CPU temp

HOST-RESOURCES-MIB

Management Center includes support for the HOST-RESOURCES-MIB, an internet standard that is detailed in RFC 2790: <https://tools.ietf.org/html/rfc2790>

<http://www.net-snmp.org/docs/mibs/host.html>

Management Center Configuration & Management

Management Center does not display all of the information available in the HOSTRESOURCES-MIB. The displayed information is limited to the following values:

- System up time
- Memory size
- CPU load per core

The following example shows the results of `snmpwalk` on an S-400 appliance:

```
HOST-RESOURCES-MIB::hrSystemUptime.0 = Timeticks: (263841) 0:43:58.41
HOST-RESOURCES-MIB::hrMemorySize.0 = INTEGER: 32791168 KBytes
HOST-RESOURCES-MIB::hrProcessorLoad.196608 = INTEGER: 20
HOST-RESOURCES-MIB::hrProcessorLoad.196609 = INTEGER: 12
HOST-RESOURCES-MIB::hrProcessorLoad.196610 = INTEGER: 12
HOST-RESOURCES-MIB::hrProcessorLoad.196611 = INTEGER: 4
HOST-RESOURCES-MIB::hrProcessorLoad.196612 = INTEGER: 3
HOST-RESOURCES-MIB::hrProcessorLoad.196613 = INTEGER: 1
HOST-RESOURCES-MIB::hrProcessorLoad.196614 = INTEGER: 1
HOST-RESOURCES-MIB::hrProcessorLoad.196615 = INTEGER: 1
```

You can also view this information from the Management Center CLI:

```
# show HOST-RESOURCES-MIB
HOST-RESOURCES-MIB hrSystem hrSystemUptime 456987
HOST-RESOURCES-MIB hrStorage hrMemorySize 32791168
HR          HR
DEVICE     PROCESSOR
INDEX      LOAD
-----
196608    20
196609    11
196610    12
196611    4
196612    1
196613    1
196614    1
196615    1
```

Interfaces Group MIB (IF-MIB)

Management Center includes support for the Interfaces Group MIB (also known as the IF-MIB), an internet standard detailed in RFC 2863: <https://tools.ietf.org/html/rfc2863>

<http://www.net-snmp.org/docs/mibs/interfaces.html>

As with the HOSTRESOURCES-MIB, Management Center limits the information that it displays. Consider the following example (note the 4 interfaces on the S-400 appliance):

```
bash-4.1# snmpwalk -v2c -c testsnmp localhost .1.3 | grep IF-MIB
IF-MIB::ifNumber.0 = INTEGER: 4
```

```
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifDescr.1 = STRING: 0:0
IF-MIB::ifDescr.2 = STRING: 1:0
IF-MIB::ifDescr.3 = STRING: 2:0
IF-MIB::ifDescr.4 = STRING: 2:1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 1500
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
IF-MIB::ifMtu.4 = INTEGER: 1500
IF-MIB::ifSpeed.1 = Gauge32: 1000000000
IF-MIB::ifSpeed.2 = Gauge32: 0
IF-MIB::ifSpeed.3 = Gauge32: 0
IF-MIB::ifSpeed.4 = Gauge32: 0
IF-MIB::ifPhysAddress.1 = STRING: 0:d0:83:9:69:26
IF-MIB::ifPhysAddress.2 = STRING: 0:d0:83:9:69:27
IF-MIB::ifPhysAddress.3 = STRING: 0:d0:83:9:69:28
IF-MIB::ifPhysAddress.4 = STRING: 0:d0:83:9:69:29
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifAdminStatus.3 = INTEGER: up(1)
IF-MIB::ifAdminStatus.4 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: down(2)
IF-MIB::ifOperStatus.3 = INTEGER: down(2)
IF-MIB::ifOperStatus.4 = INTEGER: down(2)
IF-MIB::ifLastChange.1 = Timeticks: (57013) 0:09:30.13
IF-MIB::ifLastChange.2 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.3 = Timeticks: (57013) 0:09:30.13
IF-MIB::ifLastChange.4 = Timeticks: (0) 0:00:00.00
IF-MIB::ifInOctets.1 = Counter32: 2702197
IF-MIB::ifInOctets.2 = Counter32: 0
IF-MIB::ifInOctets.3 = Counter32: 25283
IF-MIB::ifInOctets.4 = Counter32: 0
IF-MIB::ifInUcastPkts.1 = Counter32: 17871
IF-MIB::ifInUcastPkts.2 = Counter32: 0
IF-MIB::ifInUcastPkts.3 = Counter32: 227
IF-MIB::ifInUcastPkts.4 = Counter32: 0
IF-MIB::ifInNUcastPkts.1 = Counter32: 3026
IF-MIB::ifInNUcastPkts.2 = Counter32: 0
IF-MIB::ifInNUcastPkts.3 = Counter32: 48
```

Management Center Configuration & Management

```
IF-MIB::ifInNUcastPkts.4 = Counter32: 0
IF-MIB::ifInDiscards.1 = Counter32: 183
IF-MIB::ifInDiscards.2 = Counter32: 0
IF-MIB::ifInDiscards.3 = Counter32: 0
IF-MIB::ifInDiscards.4 = Counter32: 0
IF-MIB::ifInErrors.1 = Counter32: 0
IF-MIB::ifInErrors.2 = Counter32: 0
IF-MIB::ifInErrors.3 = Counter32: 0
IF-MIB::ifInErrors.4 = Counter32: 0
IF-MIB::ifInUnknownProtos.1 = Counter32: 0
IF-MIB::ifInUnknownProtos.2 = Counter32: 0
IF-MIB::ifInUnknownProtos.3 = Counter32: 0
IF-MIB::ifInUnknownProtos.4 = Counter32: 0
IF-MIB::ifOutOctets.1 = Counter32: 380710
IF-MIB::ifOutOctets.2 = Counter32: 0
IF-MIB::ifOutOctets.3 = Counter32: 468
IF-MIB::ifOutOctets.4 = Counter32: 0
IF-MIB::ifOutUcastPkts.1 = Counter32: 2555
IF-MIB::ifOutUcastPkts.2 = Counter32: 0
IF-MIB::ifOutUcastPkts.3 = Counter32: 6
IF-MIB::ifOutUcastPkts.4 = Counter32: 0
IF-MIB::ifOutNUcastPkts.1 = Counter32: 0
IF-MIB::ifOutNUcastPkts.2 = Counter32: 0
IF-MIB::ifOutNUcastPkts.3 = Counter32: 0
IF-MIB::ifOutNUcastPkts.4 = Counter32: 0
IF-MIB::ifOutDiscards.1 = Counter32: 0
IF-MIB::ifOutDiscards.2 = Counter32: 0
IF-MIB::ifOutDiscards.3 = Counter32: 0
IF-MIB::ifOutDiscards.4 = Counter32: 0
IF-MIB::ifOutErrors.1 = Counter32: 0
IF-MIB::ifOutErrors.2 = Counter32: 0
IF-MIB::ifOutErrors.3 = Counter32: 0
IF-MIB::ifOutErrors.4 = Counter32: 0
IF-MIB::ifOutQLen.1 = Gauge32: 0
IF-MIB::ifOutQLen.2 = Gauge32: 0
IF-MIB::ifOutQLen.3 = Gauge32: 0
IF-MIB::ifOutQLen.4 = Gauge32: 0
IF-MIB::ifSpecific.1 = OID: SNMPv2-SMI::zeroDotZero
IF-MIB::ifSpecific.2 = OID: SNMPv2-SMI::zeroDotZero
IF-MIB::ifSpecific.3 = OID: SNMPv2-SMI::zeroDotZero
IF-MIB::ifSpecific.4 = OID: SNMPv2-SMI::zeroDotZero
bash-4.1#
```

You can also view IF-MIB information from the Management Center CLI. The following output is from an S400 appliance:

```
# show IF-MIB
IF-MIB interfaces ifNumber 4
```

```
IF-MIB ifTable ifEntry 1
ifDescr          0:0
ifType           ethernetCsmacd
ifMtu            1500
ifSpeed          1000000000
ifPhysAddress   00:d0:83:09:69:26
ifAdminStatus    up
ifOperStatus     up
ifLastChange    57013
ifInOctets       2725695
ifInUcastPkts   18120
ifInNUcastPkts  3065
ifInDiscards    183
ifInErrors       0
ifInUnknownProtos 0
ifOutOctets      392678
ifOutUcastPkts  2609
ifOutNUcastPkts 0
ifOutDiscards   0
ifOutErrors     0
ifOutQLen        0
ifSpecific      0.0
IF-MIB ifTable ifEntry 2
ifDescr          1:0
ifType           ethernetCsmacd
ifMtu            1500
ifSpeed          0
ifPhysAddress   00:d0:83:09:69:27
ifAdminStatus    up
ifOperStatus     down
ifLastChange    0
ifInOctets       0
ifInUcastPkts   0
ifInNUcastPkts  0
ifInDiscards    0
ifInErrors       0
ifInUnknownProtos 0
ifOutOctets      0
ifOutUcastPkts  0
ifOutNUcastPkts 0
ifOutDiscards   0
ifOutErrors     0
ifOutQLen        0
ifSpecific      0.0
IF-MIB ifTable ifEntry 3
ifDescr          2:0
ifType           ethernetCsmacd
ifMtu            1500
ifSpeed          0
ifPhysAddress   00:d0:83:09:69:28
ifAdminStatus    up
ifOperStatus     down
ifLastChange    57013
ifInOctets       25283
ifInUcastPkts   227
ifInNUcastPkts  48
ifInDiscards    0
ifInErrors       0
```

Management Center Configuration & Management

```
ifInUnknownProtos 0
ifOutOctets      468
ifOutUcastPkts   6
ifOutNUcastPkts  0
ifOutDiscards    0
ifOutErrors      0
ifOutQLen        0
ifSpecific       0.0
IF-MIB ifTable ifEntry 4
ifDescr          2:1
ifType           ethernetCsmacd
ifMtu            1500
ifSpeed          0
ifPhysAddress   00:d0:83:09:69:29
ifAdminStatus    up
ifOperStatus     down
ifLastChange    0
ifInOctets      0
ifInUcastPkts   0
ifInNUcastPkts  0
ifInDiscards    0
ifInErrors      0
ifInUnknownProtos 0
ifOutOctets      0
ifOutUcastPkts   0
ifOutNUcastPkts  0
ifOutDiscards    0
ifOutErrors      0
ifOutQLen        0
ifSpecific       0.0
```

SNMPv2-MIB

Management Center uses a standard implementation of the SNMPv2-MIB, RFC 3418:

<https://tools.ietf.org/html/rfc3418>

The SNMPv2-MIB is the Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), the document that defines managed objects which describe the behavior of a Simple Network Management Protocol (SNMP) entity.

The following output is from a BASH shell `snmpwalk`:

```
bash-4.1# snmpwalk -v2c -c testsnmp localhost .1.3 | grep SNMPv2-MIB
SNMPv2-MIB::sysDescr.0 = STRING: Symantec Management Center
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.14501.6
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::snmpInPkts.0 = Counter32: 2198
SNMPv2-MIB::snmpInBadVersions.0 = Counter32: 0
```

```

SNMPv2-MIB::snmpInBadCommunityNames.0 = Counter32: 0
SNMPv2-MIB::snmpInBadCommunityUses.0 = Counter32: 0
SNMPv2-MIB::snmpInASNParseErrs.0 = Counter32: 0
SNMPv2-MIB::snmpEnableAuthenTraps.0 = INTEGER: disabled(2)
SNMPv2-MIB::snmpSilentDrops.0 = Counter32: 0
SNMPv2-MIB::snmpProxyDrops.0 = Counter32: 0
SNMPv2-MIB::snmpSetSerialNo.0 = INTEGER: 2103378064
bash-4.1#

```

You can display similar information from the Management Center CLI:

```

# show SNMPv2-MIB
SNMPv2-MIB system sysDescr "Symantec Management Center"
SNMPv2-MIB system sysObjectID 1.3.6.1.4.1.14501.6
SNMPv2-MIB system sysUpTime 831609
SNMPv2-MIB system sysServices 72
SNMPv2-MIB system sysORLastChange 0
SNMPv2-MIB snmp snmpInPkts 1400
SNMPv2-MIB snmp snmpInBadVersions 0
SNMPv2-MIB snmp snmpInBadCommunityNames 0
SNMPv2-MIB snmp snmpInBadCommunityUses 0
SNMPv2-MIB snmp snmpInASNParseErrs 0
SNMPv2-MIB snmp snmpSilentDrops 0
SNMPv2-MIB snmp snmpProxyDrops 0
SNMPv2-MIB snmpSet snmpSetSerialNo 2103378064

```

BLUECOAT-INFO-MIB

The INFO MIB is used to provide general information about the appliance—product information, version, serial number.

```

bash-4.1# snmpwalk -v2c -cp public localhost 1.3.6.1.4.1.3417.2.19
SNMPv2-SMI::enterprises.3417.2.19.1.1.0 = STRING: "Blue Coat
Management Center"
SNMPv2-SMI::enterprises.3417.2.19.1.2.0 = STRING: "2.4.1.1"
SNMPv2-SMI::enterprises.3417.2.19.1.3.0 = STRING: "0000000000"

```

You can display similar information from the CLI:

```

# show BLUECOAT-INFO-MIB
BLUECOAT-INFO-MIB blueCoatInfo blueCoatSoftware "Blue Coat
Management Center"
BLUECOAT-INFO-MIB blueCoatInfo blueCoatVersion 2.4.1.1
BLUECOAT-INFO-MIB blueCoatInfo blueCoatSerialNumber 0000000000

```

BCSI-MC-RESOURCES-MIB

The BCSI-MC-RESOURCES-MIB shows the current memory utilization.

```
bash-4.1# snmpwalk -v2c -cpublic localhost 1.3.6.1.4.1.14501.6.2
BCSI-MC-RESOURCES-MIB bccmResMonSystem
bccmResMonMemoryUsedPercentage 63
```

You can display similar information from the CLI:

```
# show BCSI-MC-RESOURCES-MIB
BCSI-MC-RESOURCES-MIB bccmResMonSystem
bccmResMonMemoryUsedPercentage 63
```

SNMP Traps

SNMP traps send notification to the SNMP management server when appropriate conditions or thresholds are met. You configure Management Center SNMP traps using the user interface settings on the **Administration > Alerts** page. The alerts conform to the format described in the BCSI-MANAGEMENT-CENTER-MIB.

Refer to [Receive Error Notifications](#) to get more information about the types of alert notifications that can be sent with traps.

Additional Information

Additional information and resources are listed under the support section of the Symantec website at:

https://support.symantec.com/en_US/product.management-center.html

Legal Notice

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Copyright © 201x-2020 Broadcom. All Rights Reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Add Packages to Management Center

Use the **Administration > Packages** page to load add-ons to Management Center. Currently, the page only supports downloads for the new Blue Coat ProxySG appliance Admin Console package. However, other downloads will be supported in future releases.

See "Install the ProxySG Admin Console" on page 82 for more information.

Note: You can limit the actions users are allowed to perform on this page by adding the **Settings - View** or **Settings - Update** permission to a new or existing role. See "Grant Permissions" on page 572 for more information.

Note: Management Center replaces special characters in file names.

Add a Package

1. Select **Administration > Packages**.
2. Add the file using one of the following methods:
 - By browsing:
 - a. Click **Add Package**.
 - 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 Package**.
 - b. Drag and drop the files into the **Upload From Browser** window.
 - c. Click **Upload**.
- By specifying a URL:

Note: To add packages from a URL, you must first enable HTTP. For information on enabling HTTP, see "security" on page 908. At this time, Management Center does not challenge you when downloading from a secure web site.

- a. Click **Add Package**.
- b. In the **URL** field, specify the location of the package.
- c. Click **Upload**.

Delete Uploaded Packages

To delete a file, select the file and click **Delete**.

Configure Consent Banner

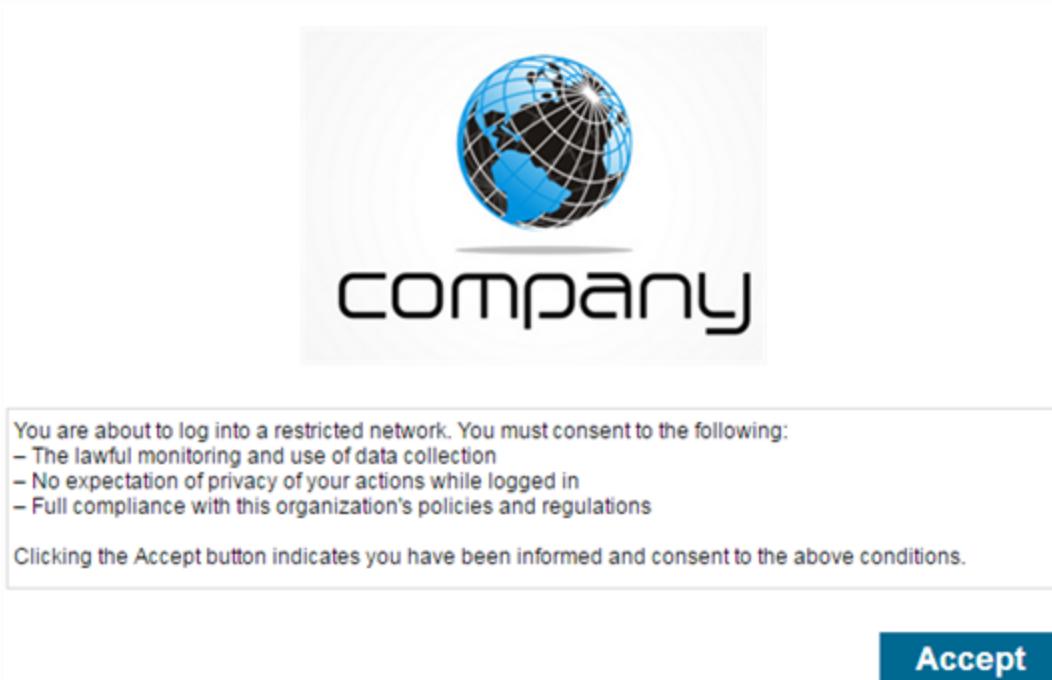
A Notice and Consent banner provides consent information to users of computer networks, computers, and other systems and resources. Users are required to accept the terms in the banner prior to authentication. The banner is presented to users before a login process, and it requires users to acknowledge 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 Center 1.10.1.1, 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.



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.

Note: 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 797 for more information.

Editor Example

Consent Banner

Show consent banner:

Consent text:

B I H H_v H_a | ≡ ≡ | “ ” %

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.

![]
(<https://.../fs/download/4593fb43835e406abbf3eaa374cae2b8>)

Click ****Accept**** to continue.

Consent image:

company-logo.png

[download](#)[remove](#)

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.

Setting	Description	Input Value/Format
Monitor Enabled	Enable or disable hardware monitor	true/false
Monitor Interval (min)	The threshold at which the hardware monitor polls the device (in minutes).	5 ▲
Disk Usage - Warning	The threshold at which the monitor polls the device for disk usage events.	85 ▲
Disk Usage - Critical	The threshold at which the monitor polls the device.	95 ▲
Disk Usage - Shutdown on critical?	Shuts down the web console when the threshold for Critical is reached.	true/false
Memory Usage - Warning	The threshold at which the monitor polls the device for memory usage events.	95 ▲
Memory Usage - Critical	The threshold at which the monitor polls the device for memory usage events.	99 ▲

4. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

Note: 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.

Set HTTPS Server Certificate Hostname for Secure Device Communication

This page refers to the hostname option on the [Administration > Settings > Device Communications](#) page.

When devices communicate with Management Center over secure channels, certificate information is exchanged. In order to qualify as legitimate, the hostname used by devices to communicate with Management Center should match the Common Name (CN) field of a PEM certificate, or one of the Subject Alternative Name fields. Define that hostname here.

If no value is provided for device communication, managed assets use the first IP address configured on the Management Center appliance.

Caution: If you are using PDM data collection, it is strongly recommended that you specify a hostname. If no hostname is specified, PDM data collection may fail.

Set a Hostname

1. Identify the hostname used in Management Center's HTTPS server certificate, and enter it in the field on the [Administration > Settings > Device Communications](#) page.
2. Click **Activate** to save your changes.

This value can also be applied from the command line interface. See device-communication in the Management Center Command Line Interface reference.

Management Center Mail Settings

Management Center has three different email settings.

Function	Option	Description
Device health notifications	SMTP alerting	These options configure the mail server for sending device health monitoring notifications from Management Center.

Function	Option	Description
Management Center health notifications	SMTP (CLI)	This CLI option configures Simple Mail Transfer Protocol (SMTP) settings for Management Center core health monitoring notifications.
Password reset notifications	Mail Settings	These options configure the server that Management Center uses to send alerts related to users of the system, for example, password resets.

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.

Note: 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**.

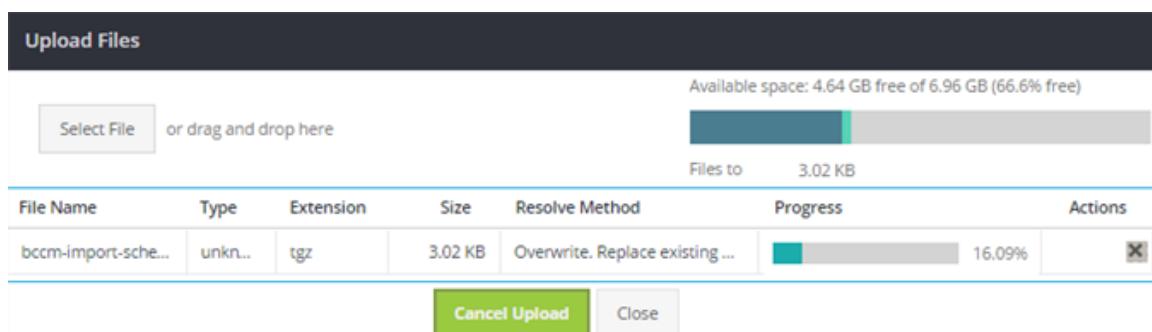
By dragging and dropping one or more files:

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.

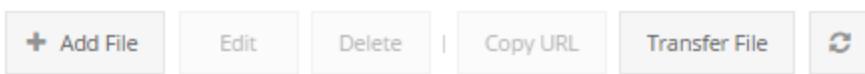


You can cancel the upload after it begins by clicking **Cancel Upload** or the icon.

Transfer Files

Click **Transfer File** to retrieve files from a URL.

Files



1. Click Transfer File. The system displays the File Transfer window.

The screenshot shows the 'File Transfer' window. At the top, there is a header bar with the title 'File Transfer' and a close button (X). Below the header, there are two input fields: 'Server URL:' with a yellow asterisk (*) and 'File Type:' also with a yellow asterisk (*). A note below the URL field states 'protocols supported: http/https'. Underneath these fields, there is a section titled 'If the file already exists:' with three radio button options:

- Overwrite. Replace existing file.
- Cancel. Do not transfer.
- Keep both. Rename transferred file to: "FileName(n)"

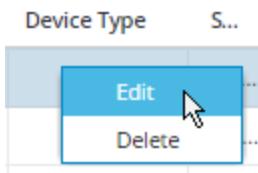
At the bottom of the window, there is a toolbar with three buttons: 'Cancel' (gray), 'Create Job...' (gray), and 'Run Now' (green).

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.

The screenshot shows the 'Edit File' dialog box. It contains fields for 'File Name' (bccm-import-schema.tgz) and 'File Type' (unknown). Below these, there is a 'Device Type:' field with a dropdown menu open, listing several device types: Advanced Secure Gateway, Content Analysis System, Malware Analysis, Management Center, PacketShaper, ProxySG, and Router.

Device Type:
Advanced Secure Gateway
Content Analysis System
Malware Analysis
Management Center
PacketShaper
ProxySG
Router

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**
- **Resource ID**
- **Description**

For the **Resource ID**, you must enter a string of alpha numeric characters (maximum of 36 characters) which can be used to reference the file:

- The Resource ID needs to be unique; you can't have the same resource ID for two separate files.
- The resource ID can't be an empty string.
- Special characters are not allowed.

The changes you make in this field are reflected in the file URL, as described in the following section.

Change the File URL

By default, the last part of the file URL is a random string of alphanumeric characters. For example:

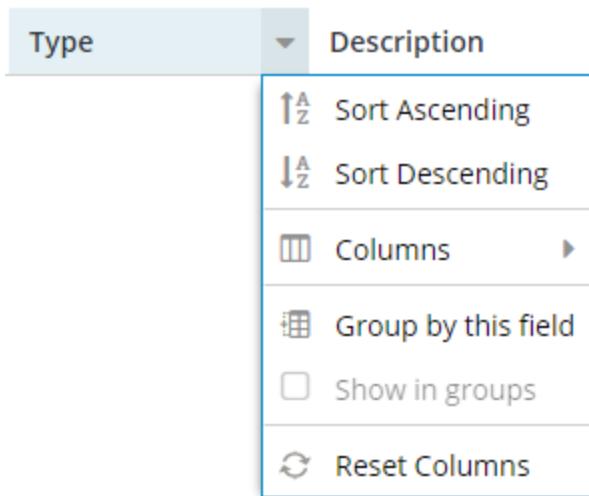
<https://198.51.100.24:8082/fs/download/a57a1aed5ac64c399a8d1877fc15bd8f>

To make the URL more user friendly or descriptive, enter descriptive text in the Resource ID field as described in "Edit Uploaded Files" on the previous page.

1. Select the uploaded file and click **Edit**.
2. Add or change the text to the **Resource ID** field.
3. Click **Copy URL**. The URL should now reflect the text you entered in step 2.

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.

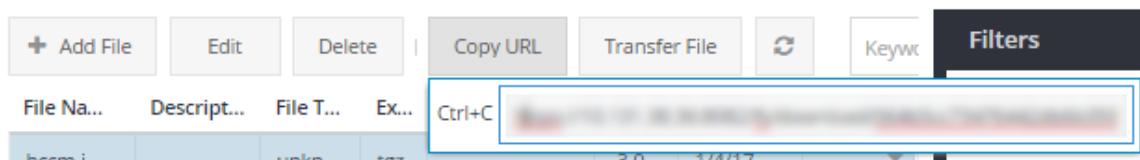
Delete Uploaded Files

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 past the URL into Management Center CLI commands (for example, installing a new image), and other options or operations that accept URLs.

Files



Note: You can also "Change the File URL" on page 801.

Migrate From Director to Management Center

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.

Migration recommendations and limitations:

- Before you begin, push all pending policy changes from Director to your devices to ensure that all devices have the latest configuration.
- Remove any devices from your Director configuration that are no longer in use.
- Remove any overlays that include policy, as Management Center cannot import them. Once migrated, Management Center can pull existing policy from these devices.
- Make note of jobs that you run on a regular basis, as Director jobs will not import to Management Center.
- Profiles are also not imported in the migration from Director to Management Center. Rather, this functionality can be recreated using scripts to create a proper image of your devices to use as a generic source for your configuration file updates.
- Device configurations can be imported into a Management Center script directly from each device post-migration.

Export Metadata from Director as an

Encrypted File

The metadata file produced in this procedure cannot be opened outside of Management Center and is the export procedure recommended by Symantec. If you would rather produce an unencrypted file to work with, see "Migrate From Director to Management Center" on the previous page

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

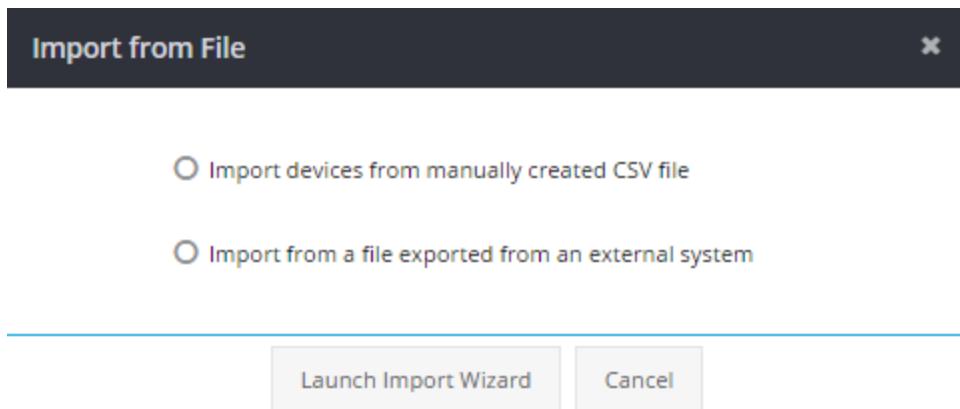
ftp://hostname_or_address/path_and_filename
scp://hostname_or_address//path_and_filename

Note: If necessary, copy or move the file to a location that Management Center can access.

Import Director Metadata as Scripts into Management Center

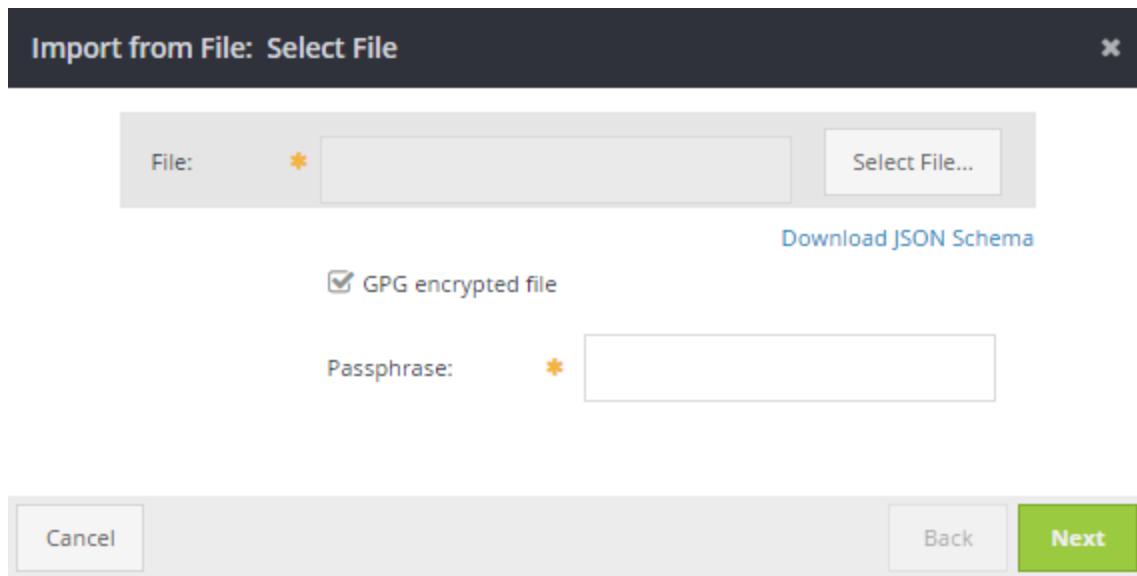
From the Management Center web console, import the device metadata file that is currently saved on an external server.

1. Log into the Management Center web console.
2. Click the **Network** tab.
3. **Select Operations > Import from File. The web console displays the Import from File dialog.**

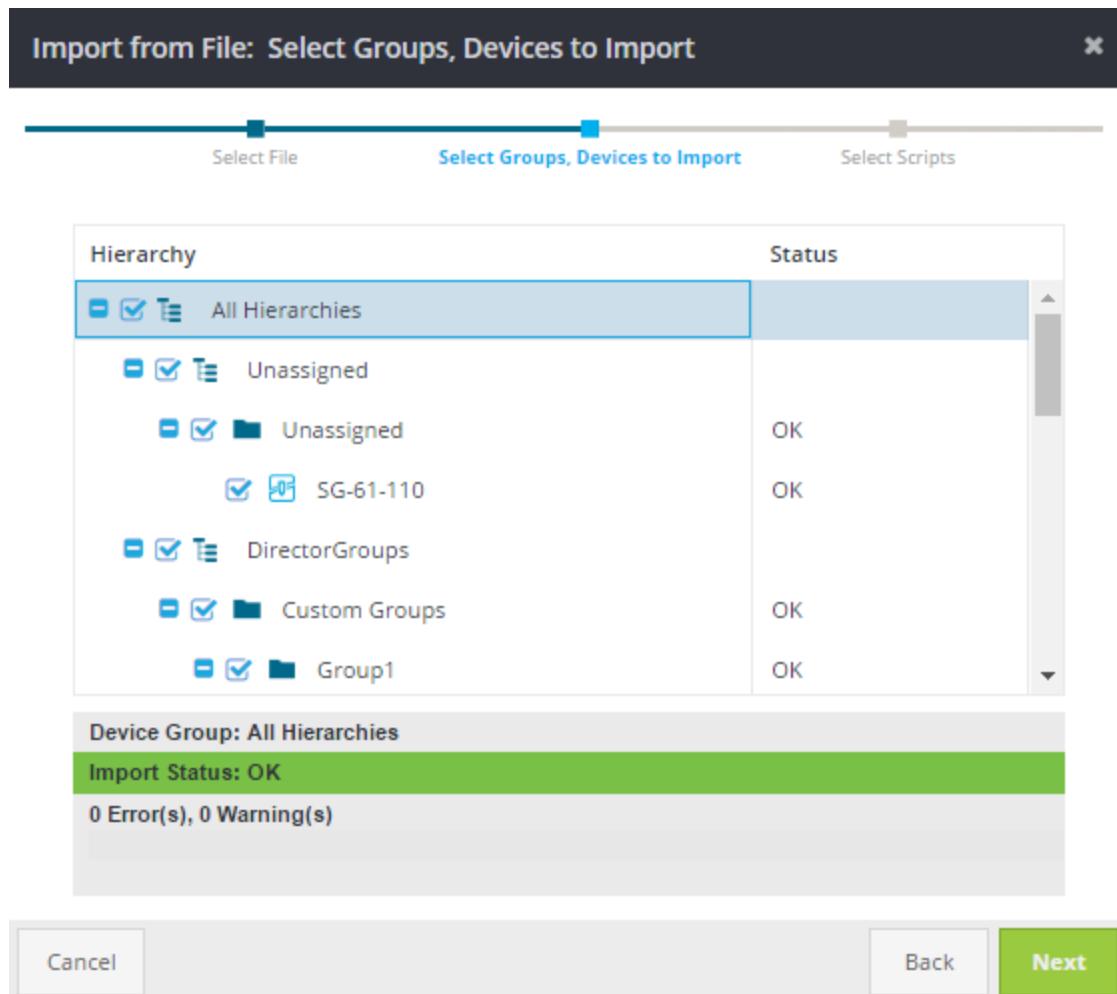


4. Select the **Import from file exported from an external system** check box, then click **Launch Import Wizard**.
5. On the Import from File: Select File dialog, select the file that you want to import. The **GPG encrypted file** check box is selected by default for (*.gpg) files. Clear the check box if your file is not encrypted (*.tar.gz or *.tgz format).

Note: 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.**



Note: 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.**

Import from File: Select Scripts

Select File Select Groups, Devices to Import **Select Scripts**

<input checked="" type="checkbox"/>	Name	Description	Replace Vars	Type	Author	Date	Script
<input checked="" type="checkbox"/>	Test Script 001	Test desc...	Yes	ProxySG	[REDACTED]	2/12/16	Sed ut perspiciatis un...
<input checked="" type="checkbox"/>	Test Script 002	Test desc...	Yes	Advance...	[REDACTED]	2/12/16	At vero eos et accusa...
<input checked="" type="checkbox"/>	Test Script 003	Test desc...	Yes	ProxySG	[REDACTED]	2/12/16	Sed ut perspiciatis un...

Info: Imported overlays will be stored as scripts under Configuration > Scripts

Cancel **Back** **Import**

Note: 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.

The screenshot shows the 'Device Import Status' dialog box. It contains three main sections: Groups Summary, Device Summary, and Overlays Summary. Under Groups Summary, there is a table with two rows: 'Successfully imported: 8 of 8' and 'Overridden: 0 of 8'. Under Device Summary, there are four rows: 'Successfully registered: 10 of 10', 'Registration failed: 0', 'Overridden: 0 of 10', and 'Deployment failed: 10' with a 'Retry all' button. Under Overlays Summary, there is a table with two rows: 'Successfully imported: 3 of 3' and 'Import failed: 0 of 3'. Below these sections is a grid of device cards for SG-61-101, SG-61-102, SG-61-103, and SG-61-104. Each card has an 'Edit' and 'Retry' button. At the bottom right of the dialog is a 'Close' button and a checked checkbox for 'Show successfull imports'.

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

What do you want to do next?	Refer to this topic
Ensure that all devices belong to a hierarchy and group	"Ensure Devices Belong to Device Groups" on page 169
Change device information	"View and Edit Device Information" on page 69

Upgrade Management Center

Caution: Always back up your Management Center configuration before upgrading or downgrading. Then, store the backup off-box. This ensures that you can restore your configuration if you experience problems with upgrading or downgrading.

Caution: Although Management Center 2.1.x and later use only TLS 1.2 by default, previous TLS settings may be retained if the upgrade path included Management Center 2.0.x. To delete the older TLS protocols, explicitly disable TLSv1 and TLSv1.1 after upgrading. See "Upgrade from 2.2.x or 2.3.x" on page 813 for more details.

Caution: Before upgrading to Management Center 2.2.2.x or 2.3.x releases, ensure that the device communications ssl-context option is not configured to any of internal "bluecoat-*" SSL contexts. If that option is set to a "bluecoat-*" SSL context, remove it by entering the following command:

```
# (config) no device-commuincation ssl-context
```

Upgrade Best Practice

When upgrading or downgrading the version of Management Center, try to stay within 2 versions of what is currently running. Refer to [this article](#) for more information.

Manage Management Center 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.

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 4 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](#) for a description of the commands for adding, deleting, locking, unlocking, and viewing images.

Special Notes Regarding Management Center 2.x Software Image Installation:

Due to some major changes to the underlying systems Management Center relies on, there are several important points to be aware of:

- Backups are not compatible or transferable between FIPS and Non-FIPS mode, for the following reasons:
 - Encryption differences between FIPS/Non-FIPS mode.
 - Non-FIPS backup cannot be restored to FIPS appliance without omitting certain backup portions.
- Starting with Management Center 2.1.1.1, the password used for the admin account is the same for both the CLI and user interface (UI). This means you cannot log into the UI as "admin user" unless you use the CLI admin account password.
- Although Management Center 2.1.x and later use only TLS 1.2 by default, previous TLS settings may be retained on upgrade if the upgrade path included Management Center 2.0.x. To delete the older TLS protocols, you will have to explicitly disable TLSv1 and TLSv1.1 after upgrading. See "Upgrade from 2.2.x or 2.3.x" on the next page for more details.
- The new system will generate a new, unique public SSH RSA key.
- The initial upgrade will take up to ten minutes to complete. Wait for the upgrade to complete—any interruption in the upgrade process may result in instability.

Upgrade Management Center Failover Pair

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).

To upgrade a Management Center failover pair, you must first backup the configuration, export it off box, and then disable the failover pair. For full details, refer to [Configure Management Center Failover](#).

Upgrade from 2.2.x or 2.3.x

Management Center supports upgrade from 2 previous versions of what is currently running. (In this case, 2.2.x and 2.3.x).

1. Before you begin, [backup your Management Center configuration](#) and export it off-box. This will be used if you need to recover from a failed upgrade.
2. Access the Broadcom Support portal.

Follow the instructions in the [Getting Started](#) guide to learn how to download your software and retrieve license keys.

Note: If you are upgrading Management Center on AWS, use only aws.bcsi images.

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.

Note: If you require HTTP service, enable it using the following command:

```
(config)# security http enable
```

For security reasons, you should immediately disable the HTTP service after retrieving the system image.

4. Add the system image using the `#installed-systems load <URL>` command.

Note: By default, the URL provided is in HTTPS. If your Management Center does not have a signed HTTPS certificate, installation of the image from the HTTPS URL provided will fail. If that is the case, follow step 4b to modify the provided URL To use HTTP and port 8080 instead.

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 to HTTP and 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://localhost:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e`

- c. Execute the `installed-systems load` command and wait for upgrade to complete.

5. Reboot the hardware appliance to run the new image:

```
# restart
```

When the appliance restarts, the network connection closes. If boot failure occurs upon an upgrade, Management Center downgrades to the previous version automatically.

6. Access the web-based management console at https://management_center_ip/8082
7. Access the CLI using an SSH client.
8. If your upgrade path included 2.0.x, verify your TLS settings to ensure that TLSv1 and TLSv1.1 are not being used.

Note: Although Management Center 2.1.x and later use only TLS 1.2 by default, previous TLS settings may be retained on upgrade if the upgrade path included Management Center 2.0.x.

```
# ssl view ssl-context default
Name: default
Keyring: default
CCL: browser-trusted
Protocols: tlsv1.2 tlsv1.1 tlsv1
Cipher suites: ecdhe-rsa-aes256-sha dhe-rsa-aes256-sha aes256-sha256 aes256-sha ecdhe-rsa-aes128-gcm-sha256 ecdhe-rsa-aes128-sha256 ecdhe-rsa-aes128-sha dhe-rsa-aes128-sha aes128-sha256 aes128-sha
```

9. If necessary, disable TLS versions prior to TLSv1.2:

```
(config)# ssl edit ssl-context default
(config ssl-context default)# protocols view
tlsv1.2 tlsv1.1 tlsv1
(config ssl-context default)# protocols remove tlsv1
ok
(config ssl-context default)# protocols remove tlsv1.1
ok
```

Downgrade Management Center

Downgrading has the following special guidelines you must follow:

- Downgrades can be performed down 2 dot releases within the same major release version (e.g., from 2.3 to 2.1).

- All maintenance/patch releases of a version are 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 supported in the older version) is lost.
- Upon downgrade, newer configuration settings (settings from the upgraded image that are not supported in the older version) are lost.
- If you are running 2.2.2.1 or later and downgrade to version 2.2.1.1 or earlier, all security questions must be reconfigured to re-enable the password reset feature.
- 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 Management Center.
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
```

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.

Caution: 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 Command Line Interface (CLI)" on page 873.
2. Enter enable mode, then configuration terminal mode.
3. At the command prompt, type the following command and press Enter:
`(config)# 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:

1. Version : 2.1.0.0 (196304-Debug), Creation Time : 2017-01-09 21:05:27 UTC
Statistic Monitoring Trend Data : false, Size : 4.6 MB
Description : none
2. Version : 2.0.0.0 (214174-Debug), Creation Time : 2018-02-23 19:03:00 UTC
Statistic Monitoring Trend Data : false, Size : 2.7 MB
Description : before upgrade to 2.0
3. Version : 2.0.0.0 (216160), Creation Time : 2018-03-27 13:26:56 UTC
Statistic Monitoring Trend Data : false, Size : 2.7 MB,
Description : none

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.

```
(config)# 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 determine the restore point you want to use:

```
(config)# backup restore view
```

- To restore a specific version:

```
(config)# 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 2018-Mar-29  
03:33:00 UTC? [yes, no]
```

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—its sole purpose is to replicate actions occurring on the primary node so that it can take over if something happens to primary node.

Because the secondary failover partner replicates the primary partner's data, it is ready to take over at any time. When the primary failover partner becomes unresponsive, you configure the secondary to take over and start servicing requests.

There are two options for providing failover support for your virtual appliance. The recommended solution is to use the vMotion feature of ESX. The alternative approach is to use the built-in support for failover provided by the appliance. If you have vMotion in your installation, Symantec recommends that you use it instead of the manual failover support described in this section. See [Verify VMware Requirements](#) for more information.

Important Failover Notes

- A one-time authorization token is required to set up failover in Management Center 2.x and later. The token is generated during the configuration of the primary partner and is good for 24 hours. See "Configure Failover" on page 822.
- For systems setup in failover, the data [encryption key](#) is kept in sync between the primary and secondary devices.
- Management Center supports multiple network interfaces. Symantec recommends that failover partners communicate over a separate channel.
- You can use IPv6 for failover communication in Management Center 2.x and later.
- If you intend to upgrade the failover pair, you must first disable failover. After upgrade, you can then reestablish failover.
- A Management Center assigned as the secondary partner can only be accessed by users logging in with the admin account. For example, to make the secondary partner the primary, you must be logged in with the admin account. See "Add Local Users" on page 524 for more information.

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 configuration settings in **Administration > Settings**:
 - **General**
 - **SMTP Alerts**
 - **SNMP Alerts**
 - **Housekeeping**
 - **Mail Settings**
 - **Consent Banner**
 - **Hardware Monitor Settings**
- Optional replication:

The user can also choose to replicate the following on the secondary failover partner:

- Authentication (Active Directory/LDAP/RADIUS) configuration
- Logging and alert configuration
- Access Control List (ACL) configuration

See "failover" on page 890 for more information.

The following data is not replicated on the failover partner:

- Management Center licensing and system settings
- Management Center backup images stored 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 and password of the "admin" account of this device.

- Ensure that port 2025 is open between the primary and secondary partners. Management Center failover employs an SSH connection.
- SSH connections will attempt RDNS; you must have a valid DNS setup for the pair when using failover.
- Ensure you have a method for recording the one-time authorization token generated while configuring the primary appliance. This token is required for configuring the secondary appliance.

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. Enter Configuration mode:

```
# configure
```

4. Confirm that failover has not already been configured on the appliance:

```
(config) #failover view
```

```
Failover:
```

```
Status: Disabled
```

5. Make this appliance the primary failover partner. This process generates a one-time authentication to be used for configuring the secondary partner.

```
(config) #failover make-primary
```

The command output is similar to the following:

```
One-time initial authentication token for secondary node: 58f1ddaa6f878f96
Failover:
```

Management Center Configuration & Management

```
Status: ERROR: Secondary not configured
Primary*: 198.51.100.20
Secondary: 0.0.0.0
Token Expires: Mar 28, 2018
Last status update 1 second(s) ago
(*) this Management Center
Please record authentication token for setup with primary and press Enter.
```

Because the secondary failover partner has not been configured, the failover icon displays with an exclamation mark:



Note: 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. Enter Configuration mode:
configure
4. Confirm that failover has not already been configured on the appliance:

```
(config) #failover view
```

```
Failover:
Status: Disabled
```

5. Make this appliance the secondary failover partner. To complete the operation, you must enter the token generated by the primary appliance during failover configuration. See "Step 1—Configure the Primary Appliance" on page 822.

Note: During this process, the services on both the primary and secondary appliances are unavailable.

```
(config) #failover make-secondary
```

```
Value for 'primary-ip' (<IP address>):198.51.100.20
```

```
Value for 'token' (<string, min: 12 chars, max: 36 chars>): *****
```

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 198.51.100.20 (primary) or 198.51.100.16 (secondary) during this operation. Services on 198.51.100.20 (primary) will not be available while initial failover setup is performed.

Are you sure you want to continue?y

```
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.

6. Verify that failover has been successfully configured:

```
(config) # failover view
```

```
Status: Healthy (1 second replication delay)
Primary: 192.0.2.56
Secondary*: 192.0.2.34
Replicating:
ACL Configuration: false
Authentication Configuration: false
Diagnostics Configuration: true
Last status update 11 second(s) ago
```

Management Center Configuration & Management

(*) this Management Center

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.



7. Optional—Use the CLI to configure other replication settings.

failover replicate ?

See "failover" on page 890 for more information.

Switch to Secondary When the Primary is Unresponsive

If the primary failover partner is unresponsive, you must:

On the Secondary Failover Partner:

1. Log into the secondary failover partner using the CLI admin account of the device. See "Add Local Users" on page 524 for more information.
2. Enter Configuration mode and make the secondary failover partner active. Do this by entering the command:
3. (config) #**failover make-primary**
4. Reactivate statistics monitoring.

At this point, the secondary is active and is now the primary failover partner. For details, see "Configure Management Center Failover" on page 818 and "Configure Management Center Failover" on page 818

On the Original Primary Device:

1. Fix the problem on the original primary failover partner.
2. On the original primary failover partner, enter Configuration mode and make it (the device that was unresponsive) the new secondary failover partner:

```
(config) #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.

```
(config) #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 reactivate 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**.

Upgrade the Failover Pair

Upgrading is a complex procedure. Please review the document "Upgrade Management Center" on page 811 before starting this procedure.

Step 1 - Back Up the Primary Partner

Before upgrading your failover pair, back up the Primary partner's configuration and export it off-box to a secure location. See "Back Up the Management Center Configuration" on page 627. You do not need to back up the Secondary partner.

Step 2 - Disable Failover on the Primary and Secondary Partners

Complete the following procedure on both the Primary and Secondary failover partners *before*

upgrading.

1. Log into the CLI and enter configuration mode.

2. Enter the following command:

```
(config)# failover
```

3. Enter the following command to disable the Primary partner:

```
(config-failover)# disable
```

The system terminates the CLI session when you run the **disable** command.

4. Log back into the CLI and go step 5.

5. Enter the following command to verify that failover has been disabled.

```
(config-failover)# view
```

Step 3 - Download the System Image on Both Primary and Secondary Partners

Download the desired image on both the Primary and Secondary partners:

- Transfer the image directly to Management Center. Select **Configuration > Files** and transfer the image using the [Transfer File](#) button.
- 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.

Note: If you require HTTP service, enable it using the following command:

```
(config)# security http enable
```

For security reasons, you should immediately disable the HTTP service after retrieving the system image.

Step 4 - Upgrade Both Primary and Secondary Partners

Follow the procedures in "Upgrade Management Center" on page 811 to upgrade the Primary and Secondary partners.

Step 5 - Re-enable Failover on Both Primary and Secondary Partners

Follow the procedures in "Configure Management Center Failover" on page 818 to re-enable failover on the Primary and Secondary partners.

Configure SNMP Alert or SMTP Trap for Failover Alerts

You can configure an SNMP alert and/or SMTP trap to notify you if there is an error in the failover state. When configured, the health check runs every 60 seconds to determine the health of the failover configuration. Possible error states include:

- Secondary not configured
- Host not configured as failover partner
- Partner IP address is not active

If the health check encounters a failover error, it checks two more times before it confirms the error. If the health check confirms the error, a trap is sent and the health check will resume. When it detects that the failover pair is healthy again, the health check sends another trap indicating that the problem has been resolved.

Note: The failover health check can be configured only from the Management Center CLI. You cannot configure this option using the user interface.

Configure Failover Health SNMP Trap

To receive an SNMP trap when the health check detects a failover error, you must configure the following from the Management Center CLI: SNMP community name, vacm view, vacm, group, vacm access, notify target name, and notify target IP address. Then, you must enable the SNMP agent.

Example SNMP Trap Configuration

```
(config)# snmp community public
(config-community-public)# exit
(config-snmp)# vacm view bc subtree 1.3 included
(config-snmp)# vacm group public member public sec-model v2c
(config-snmp)# vacm group public access v2c no-auth-no-priv notify-view bc read-
view bc write-view bc
(config-snmp)# notify target1 type trap tag target1
(config-snmp)# target target1 ip 192.0.2.14 tag target1 udp-port 162 v2c sec-
name public
(config-snmp)# agent enable
```

Note: The SNMP failover health trap uses the BLUECOAT-SG-HEALTHMONITOR-MIB, which is included in the BLUECOAT-MIB. You can download these MIBs on the [Download](#) site.

Configure Failover Health SMTP Trap

To receive an SMTP trap when the health check detects a failover error, you must configure the

Management Center Configuration & Management

following from the Management Center CLI:

```
(config)# smtp  
(config-smtp)# destination-address add address  
(config-smtp)# from-address address  
(config-smtp)# gateway gateway
```

View Failover Health Check Logs

View failover health check logs in the following location:

/var/log/user_syslog

Disable Failover

Use the `failover disable` command to disable failover.

```
(config)#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

Note: 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.

Note: The Network Protection Licensing Portal (NPLP) has been replaced by [MySymantec](#).

You can update your existing license from [MySymantec](#), download the license from a web server or workstation, or install it manually.

License Update Procedure

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.

Note: Use the passphrase field when you are installing a license you generated with a passphrase; the passphrase is required for VA Offline licensing.

3. Install the license using one of the methods shown in the **Install New License** tab.

See "Install the license from MySymantec using the Management Center web console" on the next page, "Install the license from URL" on page 834, or "Paste license text from a text editor" on page 834 for instructions.

4. (Optional) To troubleshoot the license installation, do the following:
 - To check the status of a license, run the CLI command **#licensing view**.
 - To verify network settings, run the following CLI commands:
 - **# show running-config interface**
 - **# show running-config ip**
 - **# show running-config dns**
 - 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 **(config)# licensing load**.
 - Try to update the license again, after running the CLI command **#restart**.
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 **# licensing view** to determine if the license was installed and is valid.

Install the license from MySymantec using the Management Center web console

1. Select **Administration > License**.
2. Click the **Install New License** tab.
3. Select **Install from NPLP**.
4. Enter your [MySymantec](#) (formerly known as NPLP) user ID and password.
5. Click **Install License**.
6. Click **Refresh** to display the updated license information in the License Components table.

Manually download the license key from

MySymantec

If your Management Center appliance does not have Internet access, follow the procedure below to manually download the license key from [MySymantec](#). For more information on downloading a license, refer to the [Getting Started](#) web page.

Locate the appliance serial number in your shipping alert email.

1. Log in to your MySymantec account.
2. In the **My Products** list, locate the serial number of the appliance you want to license.
3. Generate a new key; this downloads the license file.

You can then "Install the license from URL" below or "Paste license text from a text editor" below.

Install the license from URL

Before you can install your license you must first get the license file (*.bcl or *.bin) from MySymantec (as described [above](#)) and save it to a location on a web server or workstation that the VA can access.

1. Select **Administration > License**.
2. Click the **Install New License** tab.
3. Select **Install from URL**. The web console displays a text field.
4. Enter the location (a valid URL) of the license file into the field.
5. Click **Install License**.
6. 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) from MySymantec (as described [above](#)) 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 **Administration > License**.
2. Click the **Install New License** tab.
3. Select **Paste license text**. The web console displays a text box.
4. Copy and paste the license from the text editor to the box.
5. Click **Install License**.
6. 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: A Division of Broadcom)
 - Number of Maximum Devices allowed
 - Serial Number
 - Appliance Model
 - Appliance Identifier (Enterprise licensed appliances only)
 - Status
 - Component Name
 - Activation date

- Expiration date
- License Type

Next steps

If you are deploying AWS, go to Step 5: Disassociate User Data from the Instance.

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.

The password reset process requires that you configure three different settings:

- You must enable the password reset feature (**Administration > Settings > General**).
- You must configure the email server (**Administration > Settings > Mail Settings**).
- Each user must set up a security question in their user profile (**Banner > **).

These actions are described in the following section.

Enable Password Reset

1. Select **Administration > Settings > General**.
2. Check the box in the **Is Reset Password enabled?** field.
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*.

Note: The message contains two substitution variables: `{fullname}` and `{link}`. Management Center automatically replaces `{fullname}` with the user's first and last name and replaces `{link}` with a password reset URL.

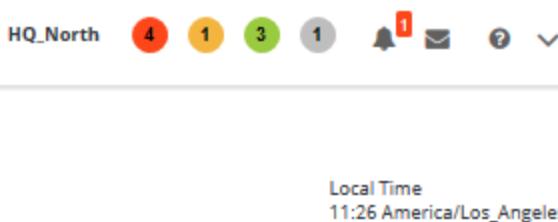
5. Click **Save** and then **Activate**.
6. Make sure an email server is configured. See "Configure Mail Settings" on page 776.
7. Ensure that all users have added a security question to their [user profile](#). Users are challenged to answer their security question during the password reset process.

8. Optional—To capture log data, configure the **Security Logging Level** to **INFO** or a higher severity (**Administration > Settings > Diagnostics**). See "Configure Diagnostics Logging" on page 773.

Display Local Time on Management Center

Use the options on this page to display the local timezone on the Management Center user interface Dashboard.

Note: This setting applies only to displaying the local time on the Management Center dashboard. It does not affect any other time zone settings on Management Center.



Display Local Time on Management Center User Interface

1. Go to **Administration > Settings > Time Zone**.
2. Select **Display local time on Dashboard**.
3. Set the desired time zone in the **Local time zone** option.
4. Click **Save**.
5. Navigate back to the Management Center Dashboard to view the changes.



Federal Information Processing Standards (FIPS) Mode

The Federal Information Processing Standards (FIPS) mode puts Management Center into a mode that is compliant with the publicly announced standards developed by the United States federal government. You can put Management Center into FIPS mode if you are running 2.1.x or later.

You use the [fips-mode](#) CLI command to enable or disable FIPS mode.

Note: In Management Center 2.2.x and later, when the appliance is in FIPS mode, you must specify a setup password to secure the initial configuration wizard. The system prompts you for the password during initial configuration. While in FIPS mode, command line access via the serial console is protected with the admin user password. If you subsequently downgrade to a release earlier than 2.2.x, that protection is lost.

Note: TLS 1.0 is not supported in FIPS mode in Management Center 2.2.x and later.

Caution: Entering or exiting FIPS mode is a destructive operation where all user defined configuration and data is destroyed. When you enter FIPS mode, the appliance is restored to factory defaults and all previous data and configurations are destroyed. When you exit FIPS mode, the appliance goes through same zeroization process, destroying all data and configuration

Caution: Backups are not compatible or transferable between FIPS and Non-FIPS mode. See "Back Up the Management Center Configuration" on page 627 for more information.

What Happens When FIPS Mode is Enabled in Management Center

2.1.1.2

FIPS mode on Management Center 2.1 enforces the requirements of Federal Information Processing Standard 140-2 on the Management Center appliance and ensures the use of FIPS 140-2 approved algorithms and behavior. The term FIPS mode refers to secure configuration that meets FIPS requirements.

Note: Management Center 2.1.1.2 is the only FIPS certified release. If you enable FIPS mode on Management Center images released later than 2.1.1.2, system operation is compliant with the FIPS requirements specified at the time that 2.1 was validated; however, those releases are not certified. This is because later releases may contain new features, such as new ciphers, that will make system operation non-compliant with the FIPS requirements.

When FIPS mode is enabled, it enforces the following changes on the appliance:

- The web management console is secured with a TLS v1.2 connection. TLS v1.1 is available but not recommended.
- The remote-access command line interface is secured with SSHv2.
- The SNMPv3 agent is available for configuration. SNMPv1 and SNMPv2 are disabled.
- Only secure NTP is available.
- FIPS-relevant services must use a set of approved cryptographic algorithms. For more information about approved algorithms, see "FIPS Cryptographic Algorithms for Management Center 2.1.1.2" on the next page .

Additionally, management communication channels for Symantec products are restricted to the cryptographic parameters stated in "FIPS Cryptographic Algorithms for Management Center 2.1.1.2" on the next page.

- Only HTTPS, SCP, and Secure FTP are allowed for transferring device backups from managed devices to Management Center.

Management Center Configuration & Management

- RADIUS is not permitted as an authentication protocol.
- Managed device backups are not compatible or transferable between FIPS and non-FIPS mode for the following reasons:
 - Encryption differences between FIPS/non-FIPS mode
 - Non-FIPS backup cannot be restored to FIPS appliances without omitting certain backup portions

Note: See "Back Up the Management Center Configuration" in the *Symantec Management Center Configuration & Management Guide* for more information.

- SSL-context features are affected in the following ways:
 - HTTP connections to devices are not allowed.
 - The CA certificate list, keyring, and CCL associated with the SSL context need to be FIPS compliant.
 - Only FIPS-compliant objects—CA certificate lists, keyrings, and CCLs—are available as configuration choices. All non-FIPS-compliant objects are unavailable.
 - If an SSL context is not specified in FIPS mode, Management Center uses the default SSL context.
- Additional testing is performed when the appliance is powered on or reset. See "Section 2.8: Self-Tests" on page 31 of the *FIPS 140-2 Non-Proprietary Security Policy for Management Center S400 Appliances* (*Management Center Security Policy Guide*) for more information.

FIPS Cryptographic Algorithms for Management Center 2.1.1.2

FIPS-relevant services include local and remote administration of Management Center:

- Web console (HTTPS over TLS).
- Remote login utility (SSHv2).

- SNMP (v3 only).
- Connections to managed Symantec products and connections to Symantec for services, such as licensing entitlements.
- FIPS-relevant services also include creation, storage, management, and deletion of Critical Security Parameters (CSPs) as defined in the Security Policy.

These services must abide by the algorithms specified in the following tables on pages 21–30 of the [*Management Center Security Policy Guide*](#).

In FIPS mode, FIPS-relevant services must use only the cryptographic algorithms and functions listed in the tables below, available in the [*Management Center Security Policy Guide*](#).

- **Table 10: FIPS-Approved Algorithm Implementations for the MC Java Cryptographic Library v1.0**
- **Table 11: FIPS-Approved Algorithm Implementations for the MC OS Cryptographic Library v1.0**
- **Table 12: FIPS-Approved Algorithm Implementations for the MC SSH Library v1.0 Table 13 FIPS-Approved Algorithm Implementations for UEFI OS Loader Library v4.14**
- **Table 14: FIPS-Allowed Algorithms**
- **Table 15: List of Cryptographic Keys, Cryptographic Key Components, and CSPs**

Approved algorithms can change over time. The tables listed above include the algorithms that were approved for the latest Management Center FIPS 140-2 validation for Management Center 2.1.1.2.

Cryptographic Restrictions for Products Managed by Management Center

Symantec products that are managed by Management Center have specific cryptographic protocol restrictions enforced by enabling FIPS mode. Additionally, enabling FIPS mode on the following devices imposes restrictions on the individual products (see the FIPS guides for each product for more information):

- Symantec ProxySG/Advanced Secure Gateway (ASG) (management communications occur over SSH):
 - Key Exchanges: DHGexSHA256, DHGexSHA1, DHG14, DHG1
 - Ciphers: AES256CTR, AES192CTR, AES128CTR

- Symantec devices on which management communications occur over HTTPS:
 - Cipher suites: AES256-SHA256, AES256-SHA, ECDHE-RSA-AES128-SHA256, AES128-SHA256, AES128-SHA

Enable FIPS Mode on Management Center

To determine how to enable FIPS mode on Management Center, refer to the [Management Center Security Policy Guide](#) for the model and operating system you are using.

Note: Currently, only 2.1.1.2 is FIPS certified.

To determine if a model or version is FIPS 140-2 validated, refer to the Cryptographic Module Validation Program (CMVP) validated module listing:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

To determine if a model or version is Common Criteria certified, refer to the Common Criteria Certified Products listing: <https://www.commoncriteriaportal.org/products/>

FIPS 140-2 Non-Proprietary Security Policy Documents

The following documents describe how Management Center meets the security requirements of FIPS 140-2, and how to run the appliance in FIPS mode:

[FIPS 140-2 Non-Proprietary Security Policy for Management Center S400 Appliances](#)

[FIPS 140-2 Non-Proprietary Security Policy for Management Center 2.1 Virtual Appliances](#)

Enable FIPS Mode

The CLI command `fips-mode` enables or disables FIPS mode.

When you enter FIPS mode, the appliance is restored to factory defaults and all previous configurations are destroyed. When you exit FIPS mode, all FIPS configurations are destroyed.

See "fips-mode" on page 893 for the CLI command syntax.

What Happens When FIPS Mode is Disabled in Management Center 2.1.1.2

Caution: Entering or exiting FIPS mode destroys all user-defined configurations and data. When you enter FIPS mode, the appliance is restored to factory defaults, which destroys all previous data and configurations. When you exit FIPS mode, the appliance goes through same zeroization process, and destroys all data and configurations.

Caution: Backups are not compatible or transferable between FIPS and Non-FIPS mode for the following reasons:

- Encryption differences between FIPS/Non-FIPS mode
- Non-FIPS backup cannot be restored to FIPS appliances without omitting certain backup portions

See [Back Up the Management Center Configuration](#) for more information.

Troubleshoot and Resolve Issues

This section discusses troubleshooting steps and advanced procedures for Management Center.

The following topics provide information for resolving common issues:

Audit Transactions	846
Determine Which Management Center Version You are Using	851
Configure Management Center to Trust Its Image Store	852
Install Management Center Certificates on Content Analysis to Establish SSL Trust ..	854
Can't Connect to Device After Upgrading to 2.x	856
A Device is Unassigned to a Device Group	857
User has "does not support" error when adding target device to edited policy	857
Prevent Licensing Issues on Management Center Virtual Appliances	858
Stop or Restart Services	859
Test Network Connectivity	860
Upload System Diagnostics	861
View Hardware Diagnostics and Memory Resources	862
Problems and Errors	863
Review Open Source Attributions	867

Audit Transactions

To access the Audit Log Viewer, click **Administration > Auditing**.

Operation Time	Operating User	Object Type	Operation Type	Info 1	Info 2
2017-01-13 06:57:32	SYSTEM	User	Update	Admin...	
2017-01-13 06:57:32	SYSTEM	Authentication	Authenticated	Admin...	10.155...
2017-01-13 06:41:06	SYSTEM	License	Validated		OK
2017-01-13 05:41:06	SYSTEM	License	Validated		OK
2017-01-13 04:41:15	SYSTEM	Device	Monitoring Enabled		
2017-01-13 04:41:15	SYSTEM	Device	Monitoring Enabled		
2017-01-13 04:41:15	SYSTEM	Device	Monitoring Enabled		
2017-01-13 04:41:06	SYSTEM	License	Validated		OK
2017-01-13 04:41:04	SYSTEM	Housekeeping Serv...	Housekeeping Co...	4	
2017-01-13 04:41:04	SYSTEM	Housekeeping Serv...	Housekeeping Task...	FileSer...	OK
2017-01-13 04:41:04	SYSTEM	Housekeeping Serv...	Housekeeping Task...	AlertP...	OK
2017-01-13 04:41:04	SYSTEM	Housekeeping Serv...	Housekeeping Task...	JobExe...	OK
2017-01-13 04:41:04	SYSTEM	Housekeeping Serv...	Housekeeping Task...	AuditP...	OK
2017-01-13 04:41:04	SYSTEM	Housekeeping Serv...	Housekeeping Star...		
2017-01-13 04:21:38	SYSTEM	License	Validated		OK

Displaying 1 - 50 of 93210

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 849.

Note: 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.

Column	Description
Operation Time	The date (in YYYY-MM-DD format) and time (in 24-hour notation) the transaction was completed.
Operating User	The user who performed the operation. If no user is associated with the operation, SYSTEM is displayed.
Record Type	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 "Understand Transaction Types" on the next page. This column is hidden by default.
Object Type	The type of object on which the operating user performed the action.
Operation Type	The operation that was completed.
Info 1 - Info 5	Additional reference fields for the record. Not all transaction types have additional information. Columns Info 3 through Info 5 are hidden by default.

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.

The screenshot shows the 'Audit Log Viewer' interface. On the left is a table with columns: Operation Ti..., Operating User, Object Type, Operation Ty..., Info 1, and Info 2. The table contains ten rows of audit log data. On the right is a sidebar titled 'Filters' with sections for Object, Operation, User, and Record Type. The 'Record Type' section has a dropdown set to 'EVENT'.

Operation Ti...	Operating User	Object Type	Operation Ty...	Info 1	Info 2
2017-01-13 0...	SYSTEM	User	Update	Ad...	
2017-01-13 0...	SYSTEM	Authentication	Authenticated	Ad...	10....
2017-01-13 0...	SYSTEM	License	Validated		OK
2017-01-13 0...	SYSTEM	License	Validated		OK
2017-01-13 0...	SYSTEM	Device	Monitoring E...		
2017-01-13 0...	SYSTEM	Device	Monitoring E...		
2017-01-13 0...	SYSTEM	Device	Monitoring E...		
2017-01-13 0...	SYSTEM	License	Validated		OK
2017-01-13 0...	SYSTEM	Housekeepin...	Housekeepin...	4	
2017-01-13 0...	SYSTEM	Housekeepin...	Housekeepin...	File...	OK
2017-01-13 0...	SYSTEM	Housekeepin...	Housekeepin...	Ale...	OK

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 manage many devices 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.

Note: 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

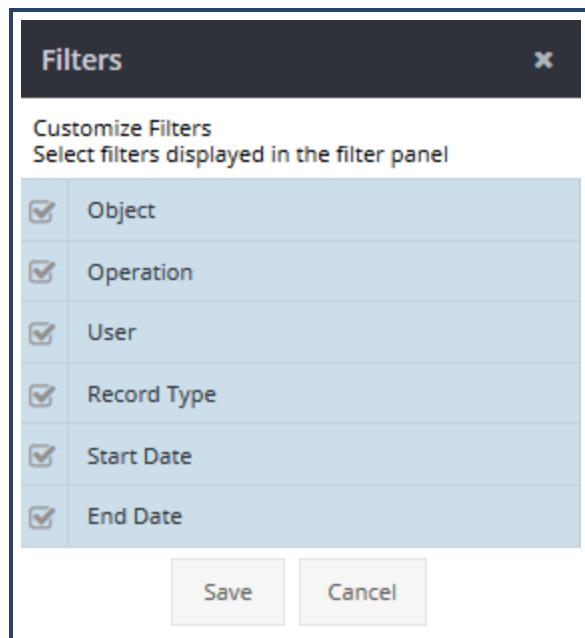
Because the Audit Log displays records in descending chronological order by default, you can re-arrange them to analyze the data more effectively. By default, the records are sorted in descending order of Operation Time (latest to earliest).

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.



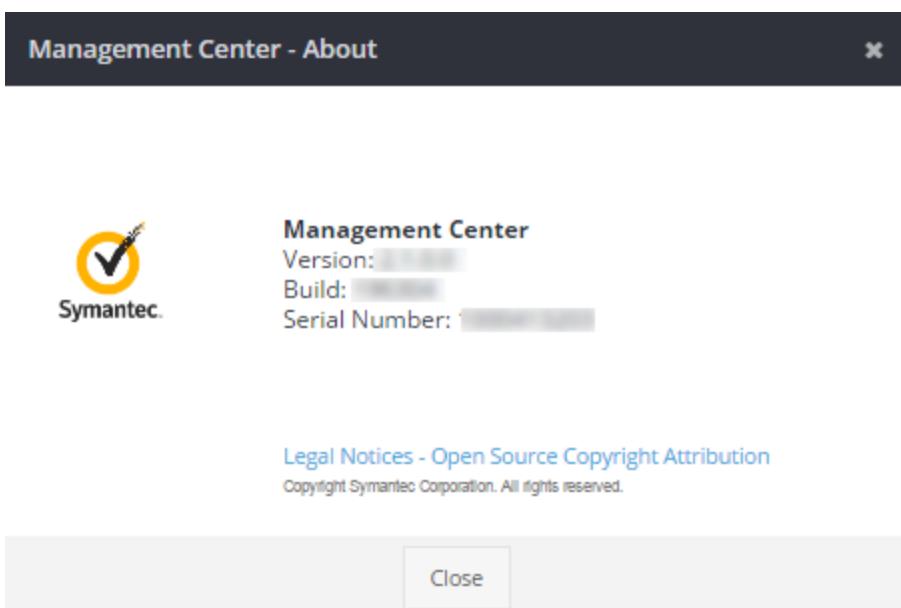
If applying a filter results in too few records or not the right records, remove or change some filters. To reset the filters to default, click **Clear**.

Determine Which Management Center Version You are Using

To aid in troubleshooting, you might need to determine the version and build of Management Center that is currently running.

Note: 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.
2. Click **Close** to close the dialog.



Build Information Fields

Field	Description
Version	The Management Center version.
Build	The number of the installed build.
Serial Number	The serial number of the appliance.

Configure Management Center to Trust Its Image Store

This topic describes how to configure Management Center to establish SSL trust when installing images from its own file store. Consider the following system image installation error:

```
# installed-systems load https://198.51.100.8:8082/fs/download/bccm_main-235430.bcsi
failed
% ErrorCode : -14500
% ErrorMessage : Connection error
% Reason : Invalid server certificate
```

This error means that the default SSL certificate is not trusted by Management Center (it has not been added to the browser-trusted certificate list). If you receive this error, complete the following procedure.

1. Access the Management Center CLI.
2. Log into enable mode.
3. View the Management Center default certificate:

```
# ssl view certificate default
-----BEGIN CERTIFICATE-----
MIIECjCCAvKgAwIBAgIJA0HKNes6SjX6MA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcxJDAi
BgNVBAoTG0JsdWUgQ29hdCBNYW5hZ2VtZW50IE1bnRlcjETMBEGA1UECxMKMTAw
MTQxODE0OTEVMBMGA1UEAxMMMTAuMTY5LjIxLjgzMB4XDTE5MDQxMTE0MzU1N1oX
DTIxMDQxMTE0MzU1N1owgYQxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEwMBQG
A1UEBxMNTW91bnRhaW4gVm1ldzEkMCIGA1UEChMbQmx1ZSBdb2F0IE1hbmfNzW11
bnQgQ2VuGVyMRMwEQYDVQQLEwoxMDAxNDE4MTQ5MRUwEwYDVQQDEwwxMC4xNjku
MjEuODMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQcmygUkX0g3Nc2q
LE+2lja6I1bZHWPjXavroDhd2+8uA1dvAeKZhb7OqfkxCmVF+wt30dNET5EIM7E
oJGITTpegzD86BVoa79CrqxOSd/AD40YUOMVDE6GAmmpZ1MquZ+3Pj54DJz3wUeY
rG3+18AVqgN5DVzCgnkKrW1Pc66xpIFvOHPyXSh+ada841jI+VCCAKI148nuDzfh
oKFNar8Ukj3k/SXgoGBRcdkJnRQRhvj8a2gSHJ38p/1D4uHusYcTm28RC/9UnqX8
rafu7td12iXmqwNSvbLYHp0fisWVKGH7ay/OreDYaeftIG+/s7jCzf5XHqf4eCr8
bWt2RdujAgMBAAGjFTB7MA8GA1UdEQQIMAaHBAqxFVMwCQYDVROTBAlwADAdBgNV
HSUEfjAUBggrBgfFBQcDAgYIKwYBBQUAwEwHQYDVROOBByEFOPy+TLUIyyAQ0+M
```

```
/n66Y7n3vST+MB8GA1UdIwQYMBaAFOPy+TLUIyyAQ0+M/n66Y7n3vST+MA0GCSqG
SIB3DQEBCwUA4IBAQBSp8TV7kmn2hX8aVQlutN6vw1z6psJ6DSUW5utDLwV5/1n
HVGagdDOSTnz3OUxJOWVSzAUIABG5JGuFA7IwXUowdsBxz++VHPZ26AbNs9xZ65D
/gfcBCebocmdLw15pbEvb0I1mPogGAGPma5D7y0BeJTLTYQVCmhV0YffhfdL7gqi
P/P8aEMn5oucrp4ZeRFAwYGd3uEzbmjwZxjF1ry1nsp29nSxAEZseN8sdSe0aiz
DUF8oBBT/7GN9v9Dsg714CckjCULId0uSgZMzTDtyq1exzF7ayK2Ka+Vat0Q6Xe1
3PVHcEdxrBnmq795U0a9eLXJfQfvh4cfIO8oSUw3
-----END CERTIFICATE-----
```

4. Copy the certificate.
5. Enter the following command to view the certificate names in the Management Center CA chain (if any are installed):

```
# ssl view ccl management-center
```

For example:

```
# ssl view ccl management-center
Certificates:
customer-ca-1
customer-ca-2
```

6. View and copy each certificate.

```
# ssl view certificate cert_name
```

For example:

```
# ssl view certificate customer-ca-1
```

7. Enter SSL configuration mode and use the inline command to paste the certificates. For example:

```
# configure terminal
(config)# ssl
(config-ssl)# inline ca-certificate mc_server_cert
Enter the certificate below and end it with a Ctrl-D
-----BEGIN CERTIFICATE-----
MIIECjCCAvKgAwIBAgIJJA0HKNes6SjX6MA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcxJDAi
BgNVBAoTG0JsdWUgQ29hdCBNYW5hZ2VtZW50IENlbnRlcjETMBEGA1UECxMKMTAw
MTQxODE0OTEVMBMGAAUEAxMMTAuMTY5LjIxLjgzMB4XDTE5MDQxMTE0MzU1N1oX
DTIxMDQxMTE0MzU1N1owgYQxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEWMBQG
A1UEBxMNTW91bnRhaW4gVm1ldzEkMCIGA1UEChMbQmx1ZSBdb2F0IE1hbhFnZW11
bnQgQ2VudGVyMRMwEQYDVQQLEwoxMDAxNDE4MTQ5MRUwEwYDVQQDEwwxMC4xNjku
MjEuODMwggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQcmygUkX0g3Nc2q
LE+21jau6I1bZHWPjXavroDhd2+8uA1dvAeKZhB7OqfkxCmVF+wt30dNET5EIM7E
oJGITTpegzD86BVoa79CrqxOSd/AD40YUOMVDE6GAmmpZlMquZ+3Pj54DJz3wUeY
rG3+18AVqgN5DVzCgnkKrW1Pc66xpIFv0HpyXSh+ada841jI+VCCAKI148nuDzf
oKFNaR8Ukj3k/SXgoGBRcdkJnRQRhvj8a2gSHJ38p/1D4uHusYcTm28RC/9UnqX8
rafu7td12iXmqwNSvbLYHpOfisWVKGH7ay/OreDYaeftIG+/s7jCZf5XHqf4eCr8
bWt2RdujAgMBAAGjftB7MA8GA1UdEQQIMAAHBaqpFVMwCQYDVROTBAlwADAdBgNV
```

Management Center Configuration & Management

```
HSUEFjAUBggrBgEFBQcDAgYIKwYBBQUH AwEwHQYDVR0OBBYEFOPy+TLUIyyAQ0+M  
/n66Y7n3vST+MB8GA1UdIwQYMBaAFOPy+TLUIyyAQ0+M/n66Y7n3vST+MA0GCSqG  
SIb3DQEBCwUAA4IBAQBSp8TV7kmn2hX8aVQ1utN6vw1z6psJ6DSUW5utDLwV5/1n  
HVGagdDOSTnz30UxJ0WVsZAUlABG5JGuF7IwXUowdsBxz++VHPZ26AbNs9xZ65D  
/gfCBeboCMDLw15pbEvb0I1mPogGAGPma5D7y0BeJTLTYQVCmhV0YffhfdL7gqi  
P/P8aEMn5oucrp4ZeRFAwYGD3uEzbmjjuWZxjFlry1nsP29nSxAEZseN8sdSe0aiz  
DUF8oBBT/7GN9v9Dsg714CckjCULId0uSgZMzTDtyq1exzF7ayK2Ka+Vat0Q6Xe1  
3PVHcEdxrBnmq795U0a9eLXJfQfvh4cfIO8oSUw3  
-----END CERTIFICATE-----  
ok
```

Repeat for each certificate you recorded in the previous steps.

8. Add each certificate to the Certificate Authority Certificate List (CCL). For example:

```
(config-ssl)# edit ccl browser-trusted  
(config-ccl-browser-trusted)# add mc_server_cert  
ok
```

You should now be able to install the Management Center image.

Install Management Center Certificates on Content Analysis to Establish SSL Trust

If you attempt to retrieve a system image from Management Center using the Content Analysis (CA) CLI, image installation will fail unless the Management Center certificates have been added to the CA browser-trusted CCL. This topic describes how to collect the Management Center certificate chain and install it onto the CA appliance so it will trust the HTTPS URL when loading a software image from Management Center.

Step 1: Collect Management Center Certificates

1. View the Management Center default certificate:

```
# ssl view certificate default  
-----BEGIN CERTIFICATE-----  
MIIECjCCAvKgAwIBAgIJA0HKNes6SjX6MA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD  
VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcxJDAi  
BgNVBAoTG0JsdWUgQ29hdCBNYW5hZ2VtZW50IEhnbR1cjETMBEGA1UECxMKMTAw  
MTQxODE0OTEVMBMGa1UEAxMMMTAuMTY5LjIxLjgzMB4XDTE5MDQxMTE0MzU1N1oX  
DTIxMDQxMTE0MzU1N1owgYQxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEWMBQG  
A1UEBxMNTW91bnRhaW4gVm1ldzEkMCIGA1UEChMbQmx1ZSBDb2F0IE1hbmfNzW11  
bnQgQ2VudGVyMRMwEQYDVQQLEwoxMDAxNDE4MTQ5MRUwEwYDVQQDEwwxMC4xNjku  
MjEuODMwggiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCmygUkX0g3Nc2q  
LE+21jau6I1bZHWPJXavroDhd2+8uA1dvAeKZh70qfkxcmVF+wt30dNET5EIM7E
```

```

oJGITTpegzD86BVoa79CrqxOSd/AD40YUOMVDE6GAmmqZ1MqUZ+3Pj54DJz3wUeY
rG3+18AVqgN5DVzCgnkKrW1Pc66xpIFv0HpyXSh+ada841jI+VCCAKI148nuDzf
oKFNar8Ukj3k/SXgoGBRcdkJnRQRhvj8a2gSHJ38p/1D4uHusYcTm28RC/9UnqX8
rafu7td12iXmqwNSvbLYHpOfisWVKGH7ay/0reDyaeftIG+/s7jCZF5XHqf4eCr8
bWt2RdujAgMBAAGjftB7MA8GA1UdEQQIMAAhBAqppFVMwCQYDVR0TBAIwADAdBgNV
HSUEFjAUBgggrBqEFBQcDAgYIKwYBBQUAwEwHQYDVR0OBBYEFOPy+TLUIyyAQ0+M
/n66Y7n3vST+MB8GA1UdIwQYMBaaFOPy+TLUIyyAQ0+M/n66Y7n3vST+MA0GCSqG
SIB3DQEBCwUAA4IBAQBSp8TV7kmn2hX8aVQlutN6vwlz6psJ6DSUW5utDLwV5/1n
HVGagdDOSTnz30UxJOWVSzAUIABG5JGuFA7IwXUowdsBxz++VHPZ26AbNs9xZ65D
/gfcBCebocmdLw15pbEvb0I1mPogGAGPma5D7y0BeJTLTYQVCmhV0YffhfdL7gqi
P/P8aEMn5oucrp4ZeRFawYGD3uEzbmjwZxjFlry1nsp29nSxAEzseN8sdSe0aiz
DUF8oBBT/7GN9v9Dsg714CckjCULIdOuSgZMzTDtyq1exzF7ayK2Ka+Vat0Q6Xe1
3PVHcEdxrBnmq795U0a9eLXJfQfvh4cfIO8oSUw
-----END CERTIFICATE-----

```

2. Copy the default certificate.
3. Enter the following command to view the certificate names in the Management Center CA chain (if any are installed):

```
# ssl view ccl management-center
```

For example:

```

# ssl view ccl management-center
Certificates:
customer-ca-1
customer-ca-2

```

4. View and copy each certificate.

```
# ssl view certificate cert_name
```

For example:

```
# ssl view certificate customer-ca-1
```

Step 2: Install Management Center Certificate(s) on the Content Analysis Appliance:

1. Access the Content Analysis CLI and enter configuration mode.
2. Install the Management Center certificates you recorded in [Step 1](#).

```
(config)# ssl inline ca-certificate ca-name
```

For example:

```

(config)# ssl inline ca-certificate mc-default
Enter the certificate below and end it with a Ctrl-D
-----BEGIN CERTIFICATE-----

```

Management Center Configuration & Management

```
MIIECjCCAvKgAwIBAgIJAMrnxW4MVDN/MA0GCSqGSIB3DQEBCwUAMIGEMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcxJDAi
BgNVBAoTG0JsdWUgQ29hdCBNYW5hZ2VtZW50IE1bnR1cjETMBEGA1UECxMKMTAw
MTQxNzgxMDEVMBMGAA1UEAxMMMTAuMTY5LjIxLjY3MB4XDTE5MDIwNTE5MTQ0MFoX
DTIxMDIwNTE5MTQ0MFowgYQxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEWMBQG
A1UEBxMNTW91bnRhaW4gVm1ldzEkMCIGA1UEChMbQmx1ZSBDb2F0IE1hbmfNzW11
bnQgQ2VudGVyMRMwEQYDVQQLEwoxNDE3ODEwMRUwEwYDVQQDEwxwMC4xNjku
MjEuNjcwggEiMA0GCSqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQc5FvTJcJPe/v7b
1hYv9wIf81G12/9zu0+1y1Gsz7+Sif+hzUmcT1v4rtOfGbklYw/FZOAPQxp9YYER
E28Sn4HnbVDcErDC5cvL1L7A6hp0xpgba0OGFpw2eH20c8gf4iWmIVf+1BPyL81
xxFBDOwRuyXpQqs0aSMzbA9vb6V91WTmSWUPvmIgRoFPcV7IEw9j87Max83UD/S
ui8lWQb0+1twaas1sy5FuvfId2ZUsrrC4RRHkRcsSJvVACxFZONfty1ZE7k42oWC2
FDTuc04IhwioM57xEsK2io8bRHVLuj3+5xUh70xCE01rcn63ptRBasqbD2FmNBQ
SgxcWocVAgMBAAGjftB7MA8GA1UdEQQIMAaHBAQpFUMwCQYDVROTBAlWADAdBgNV
HSUEFjAUBggrBgeFBQcDAgYIKhYBBQHUAWewHQYDVROOBByEFH2gIv7VsVd3EIpr
qCHbQmwf3/ATMB8GA1UdIwQYMBaAFH2gIv7VsVd3EIprqCHbQmwf3/ATMA0GCSqG
SIb3DQEBCwUAA4IBAQCPMWtqpfFLCb7jcCdzwJ0hoNhniJaH1yCSs1k5IU4zz8zp
7cQZv7L5CvgUZN9GRnaG5Juef7CnfCakrjxvFsjw2RpT638giH0aCTpQXY9Ib0x
M3x9N62nDMo+jSuEnjNayVIL03qWvB4YH7WLpsz2Z+VY16Vxe1QMMqs7KiZhms7a
PLpqRQikLcOY7EHaYcBZW/21Mfme2+wZyLSsSNKrC0pYAbYhnyjZQZt50VsI6vS
7inN2xPy56AwbPZTkHeiQIPYtIRLYjTVLeQRpb+sNdF7s+T4NsWpitS4ygRwYbih
hWiRo/SA18WBjdomAA7y2/3nJyc10Iea+XVi01E
-----END CERTIFICATE-----
CA certificate mc-default is added successfully.
```

3. Repeat step 2 for each Management Center certificate you have recorded.
4. Add each certificate authority to the browser-trusted CCL:

```
(config)# ssl ccl browser-trusted
(config-ccl-browser-trusted)# ca-certificate cert_name
```

5. Verify that the certificate(s) have been added to the browser_trusted CCL:

```
# show running-config ssl ccl browser-trusted
```

Can't Connect to Device After Upgrading to 2.x

Problem: You were able to connect to and manage a device prior to upgrading to 2.x. After upgrading to 2.x, you can no longer connect to the device.

Resolution: Check that the "#" symbol does not appear in any of the following:

- The proxy name
- The SSH banner page

- The password

The # symbol is not supported for these in Management Center 2.x.

A Device is Unassigned to a Device Group

Problem: At times a device is not a member of a device group. This can happen when no groups were selected when the device was added to Management Center, or if the groups to which the device was assigned were deleted.

Resolution: "Ensure Devices Belong to Device Groups" on page 169

User has "does not support" error when adding target device to edited policy

Problem: Before pushing policy to targets ProxySG Appliances, a user adds a target device. While the targeted device is selected, select **Compare Policy**. The expected result is comparison table of the version of policy stored on Management Center and the version already installed on the device. An error is displayed instead: "x.x.sgos6x.policy.command.x.x." does not support version 5.5.11.7.

Resolution: The ProxySG appliance SGOS version was downgraded after it was added to Management Center. Upgrade the SGOS version to 6.3.x or later before continuing.

Prevent Licensing Issues on Management Center Virtual Appliances

To prevent licensing issues, ensure that the Virtual Appliance (VA) is permitted to access to the license validation server at <https://validation.es.bluecoat.com> through your infrastructure. See "Verify Web Console Access" on page 39

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 any of your virtual appliances are deployed with the same serial number, Symantec will record a violation, and that license may be invalidated. Verify your license in [MySymantec](#) 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.



The web console banner displays an alert for each licensed component.

Once a 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). Once the license is renewed, the warning is marked as complete and removed from the Alerts page. See "Manage Alerts" on page 134 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 `(config)# licensing load` or see `#licensing` in the Configuration Management Guide for more information.

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. Go to the Management Center CLI, as described in "Access the Management Center Command Line Interface (CLI)" on page 873.
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**:

```
#system-services stop [ management-center | report-generator | statistics-monitoring ]
```

The CLI displays the command prompt.

Restart Services

1. Go to the Management Center CLI, as described in "Access the Management Center Command Line Interface (CLI)" on page 873.
2. Enter privileged mode by typing **enable** at the command prompt.
3. Enter your enable password and press **Enter**.
4. At the # prompt, type **system-services restart ?** and enable each service.

```
# system-services restart management-center  
# system-services restart report-generator  
# system-services restart statistics-monitoring
```

Warning: 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 Command Line Interface (CLI)" on page 873.

2. Enter Privileged mode. Privileged Mode Commands.

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 Command Line Interface (CLI)" on page 873.
2. Enter the privileged mode password and press Enter.
3. Enter the appropriate command to upload the diagnostics:

Using Your SR Case Number

```
# diganostics service-info send<case_number>
```

Upload the diagnostics to Symantec Support with your existing case number.

FTP

```
# diagnostics service-info send url ftp://host:port/path username <username>
password <password>
```

where *username* and *password* are the username and password to authenticate to the server. If the FTP server does not require authentication, these values are not required.

Note: If your password contains an exclamation mark, the Management Center CLI interprets it as a comment character, unless it is quoted. For more information, see Command Line Overview.

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).

- **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

Note: 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

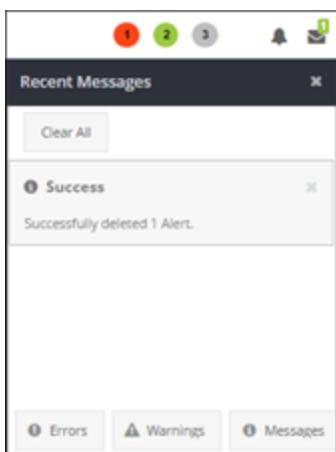
The following are error messages that you might encounter in Management Center.

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 32.

Tip: To manage alerts, click on the Alerts icon  to get to the Alerts page. See [Manage Alerts](#) for more information.

Tip: When you navigate to another screen, Message-level alerts are removed from the Messages dialog, but Errors and Warnings remain on the dialog until you read them.

"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

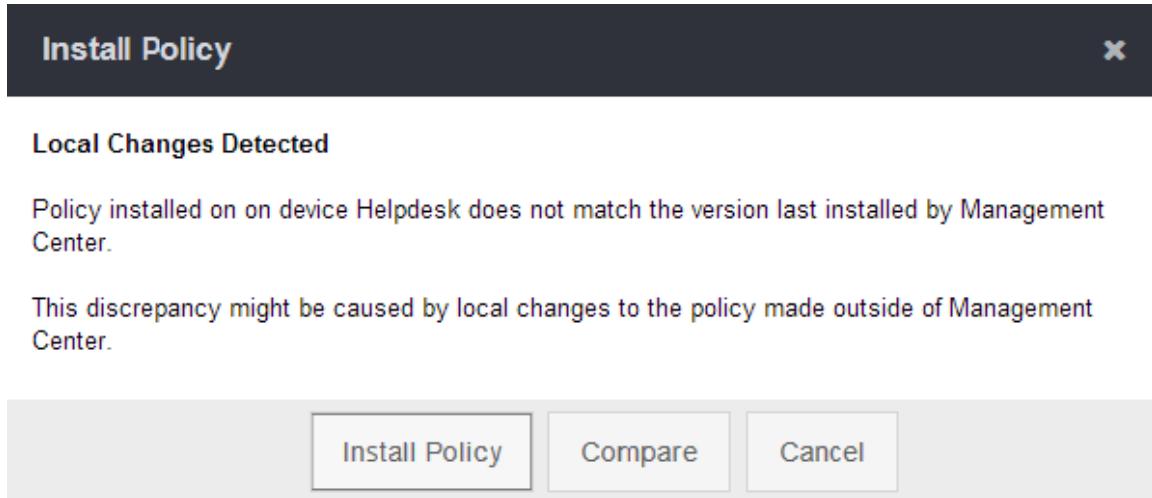
Problem: When you import devices, you receive the error "Import batch contains duplicate device name violation."

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:



This message means that the policy on a device has changed outside of Management Center. It could have been changed on the ProxySG appliance itself, or through an overlay installation if you also use Symantec Director to manage devices.

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 491 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 517.

"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 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.

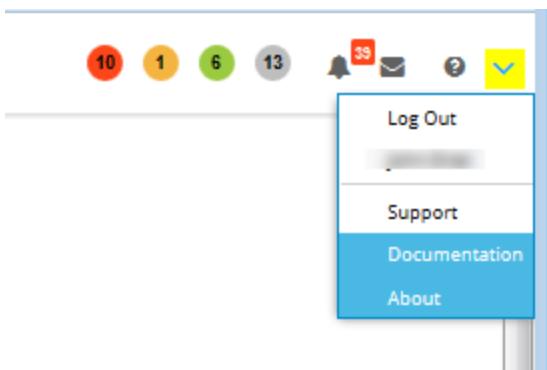
Resolution 3: Multi-tenant policy is not enabled on the device. To enable it, enter the following commands:

```
#(config) general  
#(config general) multi-tenant enable  
ok
```

Review Open Source Attributions

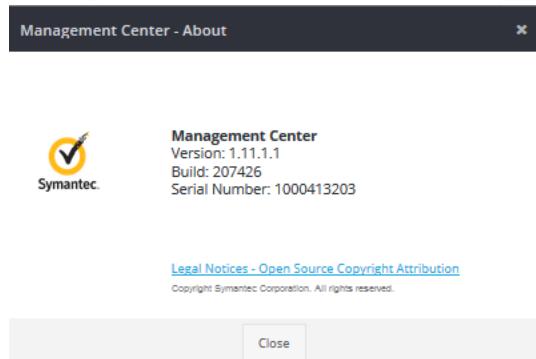
This topic describes how to download the open source attributions used in Management Center.

1. Log into Management Center.
2. In the right-side of the banner, click the down arrow (highlighted below) > **About**.



Management Center Configuration & Management

3. Click **Legal Notices - Open Source Copyright Attributions.**



4. Click the link for the zip file and save it to local disk.

Tips and Use Cases

- "Organize Scripts by Attribute " on page 278
- "Restrict Access Only to a Specific Object Included in a VPM Layer" on page 327
- [{if} \\${else} Logic in Scripts and Policy](#)

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.

CLI Command Reference

Management Center includes a command-line interface (CLI) that allows you to perform 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 Command Line Interface (CLI)" on the next page—Describes how to access the CLI via an SSH connection.
- "Command Line Overview" on page 1—Describes the standards and conventions in the Management Center CLI.
- "CLI URL Syntax" on page 875—Describes the valid syntax for commands that require a URL path.
- "CLI Output Processing" on page 876—Describes how to modify CLI output.
- "CLI Command Reference: List" on page 1—Navigate links to view command descriptions and syntax.

Access the Management Center Command Line Interface (CLI)

Log on to the CLI through an SSH connection or through the VMware or KVM console.

Tip: For hardware appliances, access the CLI through the serial console.

ESX: 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 Management Center
 - **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

Note: 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.

KVM: 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:
 - **KVM Host IP address**)—The IP address of the KVM host.
 - **Port**—The custom SSH port you set in Configure Access to the Management Center KVM Instance
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 KVM (virsh) console

1. Login to the CentOS server.
2. Enter the following command to open the console on the Management Center KVM instance:
`# virsh console mc_vm_name`
3. Press **Enter** three times. The console displays the CLI banner.
4. To exit a virsh console session, type **CTRL+]**.

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

http://yourserver.com/d/backup%202.tgz.gpg.

CLI Output Processing

You can process command output using an output redirect. The pipe command | character is used for this purpose. The commands can be chained to achieve more complex processing.

Syntax

```
(config)# cli_command | processing_options
```

Example

```
# show health-monitoring | ?
```

Possible completions:

begin	Begin with the line that matches
count	Count the number of lines in the output
display	Display options
exclude	Exclude lines that match
include	Include lines that match
linnum	Enumerate lines in the output
more	Paginate output
nomore	Suppress pagination
notab	Suppress table output
repeat	Repeat show command with a given
interval	
tab	Enforce table output
until	End with the line that matches

The following table describes these redirect targets.

begin Begin with the line that you have specified. For example:

```
# show history | begin 08-22
08-22 21:53:32 -- show configuration | count
08-22 21:54:00 -- show configuration | count
08-22 21:54:52 -- show configuration commit | count
08-22 21:55:07 -- show configuration
08-22 21:55:36 -- show configuration commit list | count
08-22 22:05:14 -- show configuration commit list
08-22 22:06:09 -- show
08-22 22:06:15 -- show history
```

count This redirect target counts the number of lines in the output. For example:

```
(config)# show configuration commit list | count
Count: 39 lines
```

displ Set display options. For example:

```
ay
# show timezone current | display json
{
    "result": "Local time: 2019-08-22 22:22:24+00:00 UTC \nTimezone:
UTC"
}
```

exclu Exclude the specified lines. For example:

```
de
# show clock local
local-time:          2019-08-22T22:25:27+0000
year:                2019
month:               08
day:                 22
hour:                22
minute:              25
second:              27
ntp ntp:             false
ntp-synchronized ntp-synchronized:      false
# show clock local | exclude ntp
local-time:          2019-08-22T22:25:53+0000
year:                2019
month:               08
day:                 22
hour:                22
minute:              25
second:              53
```

inclus Show only lines that include the specified lines. For example:

```
de
# health-monitoring view current | include Memory
2019-09-09 18:42:34 | Memory Utilization
```

linnu Enumerate lines in the output. For example:

```
m
# diagnostics heartbeat view | linnum
1: {
2:   "machine_status" : {
3:     "partitions" : [ {
4:       "name" : "/dev/mapper/live-rw",
5:       "used" : "1452520",
6:       "free" : "42486540"
7:     }, {
8:       "name" : "/dev/mapper/vg_persist-cache--data",
9:       "used" : "10232",
10:      "free" : "44740744"
11:    }, {
```

more Paginate the output. For example:

```
# diagnostics heartbeat view | more
{
  "machine_status" : {
    "partitions" : [ {
      "name" : "/dev/mapper/live-rw",
      "used" : "1452520",
      "free" : "42486540"
    }, {
      "name" : "/dev/mapper/vg_persist-cache--data",
      "used" : "10232",
      "free" : "44740744"
    }, {
      "name" : "/dev/mapper/vg_persist-core",
      "used" : "23044",
      "free" : "49626420"
    }, {
      "name" : "/dev/mapper/vg_persist-data",
      "used" : "5027900",
      "free" : "454578448"
    }, {
      "name" : "/dev/mapper/vg_persist-data",
      "used" : "5027900",
      "free" : "454578448"
    }, {
```

nomor Suppress pagination. For example:

```
e
# show running-config | nomore
```

repea Repeat show command with a given interval
t

```
# show subscriptions | repeat ?
Possible completions:
<interval in seconds> | <cr>

#show subscriptions | repeat 240
--- repeat refresh ---
subscriptions
application-protection
license-type Subscription
licensed-until 2020-11-27
subscription-validity Valid
data-validity Valid
data-version 20190808
last-download-info
time 2019-09-09T19:20:03.394+0000
url https://subscription.es.bluecoat.com/application-
protection/database
status "Not modified"
```

tab Enforce table output. For example:

```
show running-config interface | tab
DEVICE MTU
NAME DESCRIPTION ENABLED SPEED DUPLEX SIZE IP ADDRESS
-----
0:0 enable enable auto auto 1500 10.9.47.12
255.255.252.0
```

until End with the line that matches.

```
# show history | until 19:03
08-27 20:44:31 -- en
08-27 20:44:34 -- con
09-09 18:40:50 -- en
09-09 18:41:17 -- health-monitoring view
09-09 18:41:26 -- health-monitoring view current
09-09 18:43:18 -- health-monitoring view current | include Memory
09-09 18:47:46 -- ssh view
09-09 18:47:54 -- ssh view | linnum
09-09 18:48:12 -- event-log view
09-09 18:48:18 -- event-log
09-09 18:48:36 -- event-log view log
09-09 18:48:44 -- event-log view log | linnum
09-09 18:49:29 -- show licenses | linnum
09-09 18:52:14 -- smtp view
09-09 18:52:37 -- diagnostics view
09-09 18:52:59 -- diagnostics heartbeat view
09-09 18:53:09 -- diagnostics heartbeat view | linnum
09-09 18:57:11 -- diagnostics heartbeat view | more
09-09 19:00:56 -- diagnostics heartbeat view | nomore
09-09 19:01:55 -- failover view
09-09 19:02:10 -- system-services status
09-09 19:03:46 -- view
```

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
show        Show system information
```

ping

Generate pings to test connectivity with another device on the network. If the device answers the pings from Management Center, a message displays such as *5 packets transmitted, 5 received, 0% packet loss, time 3007ms*. If Management Center is unable to connect with the device, the system displays a message such as "*5 packets transmitted, 0 received, 100% packet loss, time 13999ms.*"

Note: Previous releases of Management Center supported disabling how the appliance responds to ping from other sources on your network. This functionality is not supported in Management Center 2.0.x; the appliance will always respond to ICMP requests received on configured and connected interfaces.

Syntax

```
# ping ipv4|ipv6source <source ip address>dont-fragment repeat <ping count>size <packet size><ip address>|<hostname> ?
```

ipv4|ipv6

Explicitly force an IPv4 or IPv6 ping.

When an IP version isn't specified, the program will try to resolve the name given, and choose the appropriate protocol automatically. If resolving a host name returns both IPv4 and IPv6 addresses, ping will use IPv4.

source <source ip address>

The source IP address to put in the ping packet

repeat <ping count>

The number of ping packets to send. The default is 5.

size <packet size>

The size of the ping packets (in bytes). The default is 100 bytes.

dont-fragment

Set the dont-fragment flag on the ping packets.

<ip address>|<hostname>

The destination to ping. This is the only required ping parameter.

Examples

```
# ping repeat 3 size 50 cnn.com
PING cnn.com (157.166.226.25) 50(78) bytes of data.
58 bytes from www.cnn.com (157.166.226.25): icmp_seq=1 ttl=115 time=63.2 ms
```

```
58 bytes from www.cnn.com (157.166.226.25): icmp_seq=2 ttl=115 time=62.8 ms
58 bytes from www.cnn.com (157.166.226.25): icmp_seq=3 ttl=115 time=62.9 ms
--- cnn.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 62.880/63.022/63.268/0.338 ms
# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 100(128) bytes of data.
--- 10.10.10.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 13999ms
```

fips-mode

Enables or disables Federal Information Processing Standards (FIPS) mode. When you enter FIPS mode, the appliance is restored to factory defaults and all previous configurations are destroyed. When you exit FIPS mode, all FIPS configurations are destroyed.

Note: Refer to the Management Center [documentation](#) for more information about running Management Center in FIPS mode.

Syntax

```
# fips-mode {subcommands}
```

Subcommands

```
# fips-mode enable
```

Enables FIPS mode.

```
# fips-mode disable
```

Disables FIPS mode

Configure Mode Commands

The following commands are available in configure mode. This mode offers commands that change the configuration of the appliance.

To enter configure mode, type **configure** at the enable prompt (#). The prompt will change to (config)#. To see a list of commands available in configure mode, type **help** or **?** at the (config) # prompt.

acl

Create firewall rules—access control lists—for accessing services on the appliance.

Syntax

(config)# acl ?	
disable	Disable the user-defined access control list. This command is useful when locked out of the interface with a misconfigured access list.
enable	Enable the user-defined access control list.
rule <source IP> <service>	Define the IP addresses (individual, range, or subnet) that are allowed to access an appliance service (such as Management or SNMP).

Notes

- The sub-commands listed above can either be entered in acl configuration mode (at the config-acl prompt or in configuration mode (at the config prompt)).
- To see the access control list, use the **show full-configuration acl** command.
- To remove a rule, enter **no rule** followed by the rule definition.
- Up to 1000 ACL rules can be entered in the access control list.
- The access control list only apply to incoming connections. Connections originating from the appliance are not subject to the access control list.
- Changes take effect immediately after a new rule is added or removed. It's not necessary to reboot.
- Existing connections that are allowed under a access control list are not affected when the rule is removed.

Examples

```
(config)# acl
(config-acl)# rule 10.167.9.0/24 Management
(config-acl)# rule 10.167.9.129 255.255.255.0 SNMP
(config-acl)# no rule 10.167.9.0/24 Management
```

appliance-name

Assign a unique name to the appliance. The appliance name is used when alerts are sent out to recipients, plus in other elements such as the command-line prompt and SNMP logs. Consider using a geographic or other location-based name to ensure each appliance in your network can be identified easily.

The name defined here also appears in the top bar in the Management Center Web UI

Syntax

```
(config)# appliance-name <name>
```

Notes

- While in the CLI, the name change occurs right away, so a restart of the appliance is required for the name change to appear in the web Management Console.
- 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.

Examples

```
ManagementCenter(config)# appliance-name management_center_main
management_center_main(config)#
```

authentication

Define authentication settings for administrative logins to Management Center.

Syntax

(config)# authentication ?	
enable-password	Change the password for entering enable (privileged) mode.
<hr/>	
management max-concurrent-logins <value>	Set the maximum number of concurrent logins per user. By default, the number of concurrent administrative logins is unlimited.

management inactivity-timeout <seconds>	Specify the number of seconds a session can be inactive before it is terminated. By default, this is 1800 seconds.
password	Specify a new password for the default admin account.

Notes

- The sub-commands listed above can either be entered in authentication configuration mode (at the **config-authentication** prompt or in configuration mode (at the **config** prompt).
- Use the **show full-configuration** command in authentication configuration mode to display the authentication settings.

Examples

```
(config)# authentication password
Enter current password: *****
Enter new password: *****
Confirm new password: *****
ok
```

backup

Back up the Management Center configuration, and view, export, and restore existing backups.

Syntax

```
(config)# backup [subcommands]
```

Note: While you may also run this command from the enable prompt, Symantec recommends running this command at the (config) prompt.

Subcommands

```
(config)# backup create [description] [statistics-monitoring-trend-data]
(config)# backup create <cr>
```

Create a full system backup.

```
(config)# backup create description
```

Create a Management Center backup and provide a description of that backup.

```
(config)# backup create statistics-monitoring-trend-data[include|exclude]
```

Define whether to include Statistics data when creating backups. By default, this data is excluded.

```
(config)# backup delete <index_number>
```

Delete the specified configuration backup.

Use the **backup view** command to determine the index number to use.

```
(config)# backup export <index_number> <URL> [passphrase <value>] [password <value>] [username <value>]
```

Note: If your password contains an exclamation mark, the Management Center CLI interprets it as a comment character, unless it is quoted. For more information, see Command Line Overview.

Export the specified backup to a destination FTP/FTPS, HTTP/HTTPS, or SCP/SFTP server. When exporting configuration backups, the CLI requires that you enter a passphrase to encrypt the backup file before sending it to the specified server. Password and Username entries are optional, and dependant on the destination server's requirements.

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. Verify the filename on the server, and include that in the path as in the following example: `ftp://192.0.200.68/bcmc_backup_20180402_191517.tgz.gpg`.

```
(config)# backup import <URL> [passphrase <value>] [password <value>] [username <value>]
```

Import a backup from a specified server. To import the backup, you must enter the passphrase that was used to encrypt the backup during the initial backup export.

<URL> is the URL of the external server and path. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP.

```
(config)# backup restore <index_number>
```

Restore a Management Center backup, specified by the index number. This command is only available when the backup command is entered from a (config) prompt.

Use the **backup view** command to determine the index number to use.

```
(config)# 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, SCP, or SFTP 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** command.

Warning: Configuration backups are not human-readable, and can only be restored to Management Center appliances running the same version as the original appliance was running at the time the backup was recorded.

Example

```
(config)#backup create description "before upgrade to 2.0" statistics-monitoring-trend-data exclude
ok
(config)#backup view
1. Version : 2.1.0.0 (196304-Debug), Creation Time : 2017-01-09 21:05:27 UTC,
Statistic Monitoring Trend Data : false, Size : 4.6 MB,
Description : none
2. Version : 2.0.0.0 (214174-Debug), Creation Time : 2018-02-23 19:03:00 UTC,
Statistic Monitoring Trend Data : false, Size : 2.7 MB,
Description : before upgrade to 2.0
(config)#backup export 2 ftp://192.0.200.55/appliance_backups/ passphrase "this is a test passphrase"

Securing backup archive ...
Exporting backup archive ...
ok

(config)# backup import ftp://192.0.200.55/appliance_backups/bcmc_backup_20180402_200649.tgz.gpg
Value for 'passphrase' (<string>): ****
Importing backup archive bcmc_backup_20180402_200649.tgz.gpg ...
Downloading backup archive ...
Verifying backup archive ...
Securing backup archive ...
```

```
Backup archive successfully imported.  
ok
```

clock

Manually set the time and date of the appliance in Coordinate Universal Time (UTC).

Syntax

```
# clock day <value>|hour <value>|minute <value>|month <value>|second  
<value>|year <value>
```

Each value must be entered as a separate command.

Examples

To set the date to September 2, 2016:

```
# clock day 2  
  
# clock month 9  
  
# clock year 2016
```

Note: If you are using an NTP server, you do not need to manually set the clock.

device-communication

Sets the hostname/IP that managed devices will use to contact Management Center. This is necessary when multiple IP addresses are configured on the appliance. The hostname provided needs to match the common name (CN) field in the certificate, or x509 extension for hostname on Management Center's server certificate for devices to be able to validate SSL connection.

If no value is provided for device-communications, Management Center uses the CN value from the default server certificate used to secure HTTPS connections.

Caution: If you are using PDM data collection, it is strongly recommended that you specify a hostname. If no hostname is specified, PDM data collection may fail.

Syntax

```
(config)# device-communication hostname <value>
```

<value> Represents either the IP address of the interface on which management connections are expected, the common name (CN) or the hostname from an x.509 certificate extension.

Example

```
MC_Draper(config)# device-communication hostname managementcenter1
```

dns

Configure servers and domains for the domain name system (DNS).

Syntax

```
(config) # dns ?
```

name-server <IP address>	IP address of a DNS server. Enter one or more IP addresses, each separated by a space.
domain-list <domain> <domain> ...	A list of DNS domain names of which this appliance will consider itself to be a member. DNS queries which use a short name will append these domains, in turn, until a match is found.

Notes

- To clear these settings, use the **no** command. For example, **no dns name-server**.
- To view the current settings, type **show full-configuration dns**.

Examples

```
(config) # dns name-server 10.2.2.10 10.2.2.11
```

failover

Configures Management Center failover. Management Center supports failover using two appliances. One appliance is delegated as the *primary* partner and the other as the *secondary* partner. During continuous replication, users can perform all normal operations on the primary appliance. Users cannot access the secondary appliance—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 for more information.

Tip: Management Center 2.0.x supports multiple network interfaces. Symantec recommends that failover partners are configured to communicate over a separate channel. This communication takes place on TCP port 2025. Ensure that this port is open between the two appliances in your security infrastructure.

Syntax

This command is available from an enable mode prompt (#) or the (config)# mode prompt. Running failover in enable mode provides only the view option, while (config)# mode provides all of the options detailed below.

```
# failover [subcommands]
```

Subcommands

```
# failover view
```

Display current failover settings.

```
# failover make-primary
```

Configures the appliance to be the primary partner in the failover group and creates an authentication token for the secondary node that is valid for twenty-four hours.

Warning: Make note of this token, as it is required for failover make-secondary.

```
# failover make-secondary [interface|primary-ip|token]
```

Configures the appliance to be the standby partner in the failover group. Use the optional interface parameter to configure an IP address used by the primary failover host to connect to the secondary node. To force the outgoing communications for failover, define routes in the routing table to force the device-name. See "ip" on page 899 for syntax and additional details.

Note: To avoid conflicts with the primary appliance, the secondary appliance cannot run the following CLI commands: `installed-systems`, `diagnostic-systems`, `licensing`, `db-maintenance`, `service purge-vpm-cache`, `snmp`, and `statistics-monitoring`.

```
# failover replicate [authentication-configuration|acl-configuration|diagnostics-configuration] [false|true]
```

This command is only available on the secondary failover partner. The command allows you to optionally replicate the authentication, logging and alert, and access control list (ACL) configuration of the primary failover partner.

```
# 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
```

The failover view command output is different on the secondary failover partner:

```
# failover view
Status: Healthy (1 second replication delay)
Primary: 198.51.100.20
Secondary*: 198.51.100.24
Replicating:
ACL Configuration: false
Authentication Configuration: false
Diagnostics Configuration: true
Last status update 11 second(s) ago
(*) this Management Center

#failover make-primary
One-time initial authentication token for secondary node: 58f1ddaa6f878f96
Failover:
Status: Healthy (0 second replication delay)
Primary*: 192.0.100.20
Secondary: 192.0.100.21
Token Expires: Mar 28, 2018
Last status update 1 second(s) ago
(*) this Management Center
Please record authentication token for setup with primary and press Enter.

# failover make-secondary
Value for 'primary-ip' (<IP address>): 192.0.100.20
Value for 'token' (<string, min: 12 chars, max: 36 chars>): *****
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 192.0.100.20 (primary) or 192.0.100.21 (secondary) during this operation. Services on 192.0.100.20 (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@192.0.100.20's password:
Shelving operational data on secondary...done.
Stopping services on secondary...done.
Stopping services on primary...done.
Retrieving snapshot of primary's data...

# failover replicate diagnostics-configuration true
```

This command, available only on the secondary failover partner, replicates the logging and alert configuration of the primary failover partner.

fips-mode

Enables or disables Federal Information Processing Standards (FIPS) mode.

When you enter FIPS mode, the appliance is restored to factory defaults and all previous configurations are destroyed. When you exit FIPS mode, all FIPS configurations are destroyed.

Note: Refer to the Management Center [documentation](#) for more information about running Management Center in FIPS mode.

Syntax

```
# fips-mode {subcommands}
```

Subcommands

```
# fips-mode enable
```

Enables FIPS mode.

```
# fips-mode disable
```

Disables FIPS mode

health-monitoring

View Health Monitoring (HM) events and status, and view and change HM settings.

Syntax

```
(config-health-monitoring)# ?
```

```
clear-history
```

Clear the entire event history

```
product1234-10414124(config-health-monitoring)#  
clear-history  
Event history has been cleared for all metrics.
```

history-duration	Sets the number of days that the HM framework is to store its history of events. <ul style="list-style-type: none">■ It takes one argument, an integer representing the number of days.■ Default value is 30.■ Once per day, the HM framework clears the event history of all events older than the specified number of days.
view	Show health status and metric settings. Get detailed information.

health-monitoring view

The **view** command in the health monitoring system is used for showing the event history and metric settings. While **health-monitor** can be accessed from the enable or configure terminal prompts, the **view** subcommand is only available when in **(config-health-monitoring) #**.

Syntax

```
(config-health-monitoring) # view ?
```

current	View the current state of all metrics. The output lists each metric, when the health monitoring system last checked it, the current state (OK, Warning, Critical) and the current value (for example, 28%).
----------------	---

```
events [ all]
[duration <value>
d|h|m]
```

Shows the event history for all metrics or for one metric, for the specified duration. An *event* is an occasion where the metric exceeded a configured threshold and changed state (for example, from OK to Warning, Warning to Critical).

- The **metric** and **duration** parameters are optional.
 - If the **metric** parameter is omitted, 'all' is assumed.
 - If the **duration** parameter is omitted, "24h" is assumed.
 - The **d**, **h**, or **m** suffix is used to indicate days, hours, or minutes, respectively.
-

Examples

View the current state (OK, Warning, Critical) and value of all metrics.

```
ManagementCenter# health-monitoring view current
```

Last Check	Metric Name
	State
2018-04-03 15:26:49	CPU Utilization OK - 11.00%
2018-04-03 15:27:00	License Server Communication Status OK
2018-04-03 15:27:20	License Validation Status OK
2018-04-03 15:27:20	Memory Utilization OK - 1762/7858MB 22%

installed-systems

Manage images installed on the system. Up to six images can be installed on the system. If your system already has six images installed and you add another image, the oldest unlocked image will be replaced with the new image, unless you have designated a particular image to be replaced.

Syntax

```
# installed-systems ?
```

cancel	Cancel the download process of an image that is currently downloading
default <image#>	Specify the image that will be run the next time the system is restarted. Tip: Use the installed-systems view command to identify the image number.
delete <image#>	Delete an image from the system. Use the installed-systems view command to identify the image number to delete. Note: You cannot remove a locked image or the current running image.
load <URL>	Download and install an image on the system. <URL> is the path to an image on a web server that the appliance has access to. Example: http://webserver.mycompany.com/images/542386.bcs
<p>Note: Management Center always uses the HTTP proxy if it is enabled. Therefore, if you are attempting to load an image from localhost, disable the HTTP proxy first.</p>	
<p>Note: To enforce failover replication, the installed-systems CLI command is disabled on both failover partners (to deny installing and changing system images). To upgrade, you must first disable failover. For more information, refer to the failover documentation in the <i>Configuration and Management Guide</i>.</p>	
lock <image#>	Lock an image to protect it from accidental deletion.
replace <image#>	Designate which image will be replaced next (if the system already has six installed images and you load another image). If you do not specify an image to be replaced, the oldest unlocked image on the system will be replaced.
unlock <image#>	Unlock an image that you no longer want to protect from deletion. You have to unlock a locked image before you can remove it.

unset-replace	Unset image to be replaced next. When a replacement image is not designated, the oldest image will be replaced when you load a seventh image.
view	Show a list of installed images along with their image numbers, software versions, release IDs, whether the image is locked or unlocked, whether it has ever been booted, creation date/time, and boot date/time. The summary at the bottom of the list indicates which image number is the current running system, the default system to run the next time the appliance is restarted, and the image number that will be replaced next.

Examples

```
# installed-systems view
# installed-systems load http://webserver.mycompany.com/images/542386.bcs
```

interface

Configure the interface settings (such as IP address) on the appliance.

Syntax

```
(config)# interface <interface number> ?
```

where *<interface number>* is the interface (0:0, 1:0, 1:1, and so forth) that you want to configure.

description <i><text></i>	Description of the interface; enclose in quotes if the description contains spaces.
disable	Disable the interface.
enable	Enable the interface.
ip-address <i><ip address></i>	Set the static IP address of the interface.
mtu-size <i><size></i>	Specify Maximum Transmission Unit (MTU) size (default=1500 bytes).
speed <i><speed></i>	Set the speed of the interface (for example, 1gb,10gb,100mb). The default setting is auto .

Notes

- The sub-commands listed above can either be entered in interface configuration mode (for example, at the config-interface-1:0 prompt or in configuration mode (at the config prompt).
- Use the **show full-configuration** command in interface configuration mode to display the interface settings. (See example below.)
- An interface can have both an IPv4 and IPv6 address (dual-stack).

Examples

```
(config)# interface 0:0
(config-interface-0:0)# ip-address 203.0.113.17 255.255.248.0
(config-interface-0:0)# ip-address FE80::0202:B3FF:FE1E:8329/64
```

ok

```
(config-interface-0:0)# show full-configuration
interface 0:0
  description "management interface"
  enable
  speed auto
  duplex auto
  mtu-size 1500
  ip-address 203.0.113.17 255.255.248.0
  ip-address fe80::202:b3ff:fe1e:8329/64
```

ip

Configure the gateway, IPv6 neighbors, ARP table entries, and static routes.

Syntax

```
(config)# ip ?
```

arp <IP address> <MAC address>	Add a static IPv4 or IPv6 address to the Address Resolution Protocol (ARP) table, correlating the specified MAC address to the IP address.
default-gateway <IP address>	Change the IP address of the default gateway used by Management Center.
route <prefix IP>(/<mask bits> <subnet mask>) <next hop IP> [device-name <interface>] [metric <value>]	<p>Specify the static route.</p> <p>For deployments where the default gateway does not route traffic to all segments of the network, you can define additional routes. Typical uses for the route table include routing to an SMTP or DNS server located on an internal network, or to force failover node communications to use a second network interface.</p> <p>The route metric is used by routing protocols to determine whether one route should be chosen over another. With all else being equal, lower metrics are given preference when choosing routes. The specific metric values you assign are arbitrary, but they should have values relative to routing priority. For example, a route you want to assign high priority could have a metric value of 5 and a lower priority route could have a metric value of 10 or 20.</p>

Examples

```
(config)# ip arp 1.1.1.1 01:23:45:67:89:ab
```

```
(config)# ip route 10.64.0.0/16 10.63.158.213 device-name 0:0 metric 10
(config)# ip route 2001:db8::/32 2001:0db8:0000:0000:0000:ff00:0042:8329
metric 20
(config)# ip route 10.63.0.0 255.255.0.0 10.63.158.213 metric 30
(config)# ip neighbor 2001:db8::ff00:42:8329 01:23:45:67:89:ac
```

Example: Force Failover Node Communication Through a Second Network Interface

```
(config)# ip route 10.169.21.63 255.255.255.255 10.169.21.1 device-name 1:0
```

Equivalent with Mask Bits

```
(config)# ip route 10.169.21.63/32 10.169.21.1 device-name 1:0
```

ipv6

Enable or disable support for IPv6 networking. Once enabled, IPv6 support is available in configuration sections for Packet Captures, Backups, Failover, Ping, Traceroute, SNMPWALK, Syslog, and in networking and interface configuration.

To enable IPv6, add an IPv6 address to the interface.

Syntax

```
(config) # ipv6[enable|disable]
```

Examples

```
(config)# ipv6 enable
(config)# show full-configuration ipv6
ipv6 enable
#show running-config ipv6
ipv6 enable

(config)# interface 0:0
(config-interface-0:0)# ip-address 203.0.113.17 255.255.248.0
(config-interface-0:0)# ip-address FE80::0202:B3FF:FE1E:8329/64
```

The previous commands add an IPv4 and an IPv6 address to interface 0:0.

login-banner

Configure a banner message to appear before users log in to the appliance. The message will appear before users log in to the CLI (via serial console and SSH) and the web user interface. This feature meets the security technical implementation guideline STIG V-3013. Messages can contain up to 2,047 characters and can be defined using multi-byte UTF-8 characters.

Syntax

```
# login-banner ?
```

disable	Disable the login banner message.
enable	Enable the login banner message. (You cannot enable the feature until you define the message.)
inline message	Define the login banner message. You will be prompted to enter the message text and press Ctrl-D when finished.
view message status	Show the currently defined message and feature status (enabled vs. disabled).

Examples

```
# login-banner inline message
Enter the login banner message below and end it with a Ctrl+D
This is a banner message.
ok
# login-banner enable
# login-banner view message
This is a banner message.
# login-banner view status
Login banner is enabled.
```

licensing

Configure licensing, including the loading of licenses on to the appliance.

Syntax

```
(config)# licensing
(config-licensing)#+
```

inline license-key [passphrase <value>]	Import a license from terminal input (typically by pasting the license content with a right-click). Include the passphrase to decrypt the private key if the license has birt h-cert and birth-key in it.
	Press Ctrl-D after pasting the certificate content.

load [username <value>] [password <value>] Enter your MySymantec credentials to download the appliance license from the Network Protection Licensing Portal (NPLP).

Note: MySymantec Credentials are only required for Management Center Virtual Appliances.

load url <url> passphrase <value> Download a license from the specified URL.

view [status|configuration] Display the license install status or licensing configuration details.

Note: The sub-commands listed above can either be entered in licensing configuration mode (at the config-licensing prompt) or in configuration mode (at the config prompt).

Note: If your password contains an exclamation mark, the Management Center CLI interprets it as a comment character, unless it is quoted. For more information, see Command Line Overview.

Examples

To load a license from the Symantec: A Division of Broadcom licensing server from a Virtual Appliance installation of Management Center:

```
(config)# licensing load username john.smith@test.com password helloworld
```

To load a license from the Symantec: A Division of Broadcom licensing server from a hardware appliance:

```
(config)# licensing load
```

To load a license from a URL other than NPLP:

```
(config)# licensing load http://test.server.com/license.txt
```

To view the currently installed license:

```
(config-licensing)# view
Appliance Serial Number : 100041XXXX
Licensable component information:
Serial Number : 100041XXXX
Part Number : 076-02019
```

```
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management
subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Policy Management
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management
subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Device Configuration
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management
subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Management Center
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management
subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Device Inventory
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management
subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Performance Monitoring
```

ntp

Configure Network Time Protocol (NTP) settings. Use NTP to synchronize the time on the appliance with another server or reference time source. You can configure up to 10 NTP servers.

Syntax

```
(config) # ntp ?
```

disable	Stops the NTP service on the appliance. The NTP service is configured to not start when the appliance is rebooted.
	(config)# ntp disable
enable	Starts the NTP service on the appliance. The NTP service is configured to start automatically when the appliance is rebooted. At least one NTP server must be defined in order to enable the NTP service.
	(config)# ntp enable
server <hostname or IP address>	Domain name or IP address of the NTP server. The default NTP servers are ntp.bluecoat.com and ntp2.bluecoat.com.
symmetric-key key-id <value 1-65534> algorithm <sha1> [encrypted-secret <value> secret <string>]	If your NTP server supports symmetric-key authentication, enter the key with this series of commands. Only SHA1 is supported in this release. Defer to your NTP provider's instructions on whether to use an encrypted secret or unencrypted.
update-now	Forces the NTP service to update the appliance's clock. # ntp update-now System date and time successfully updated.

Notes

- Type **ntp** to enter NTP configuration mode. The prompt will display as (config-ntp)#.
- Use the **no server** command in the NTP configuration mode to remove a configured server. (See example below.)
- Use the **show full-configuration** command in the NTP configuration mode to display the NTP settings. (See example below.)

Examples

```
(config-ntp)# show full-configuration
ntp
  enabled
  server ntp.bluecoat.com
  server ntp2.bluecoat.com
```

```
(config-ntp)# no server ntp2.bluecoat.com
```

To view the current configuration:

```
# show running-config ntp
ntp
enable
symmetric-key 1 algorithm sha1
symmetric-key 1 encrypted-secret $AES256-
CBC$4dQX+D0tMmVWdhtM4PG/+g==gFDz7v2vfOM0A1D+qjzLPB5jqfqsEZhdoYx8Es1IvkY=$k
KZd4y09r3hNn1hzilwArw==$eR4tJbJSB7309qcDCQ+jmLnCXUhfv7gQAcwvHdwFyEKfZUx5Qqy
KptrQiGGjjRwveM5UXcmem43v65eZan/WGzBow8YjdwlZN0coN87xhdN456EWJ8wsKsmld/60dhz
VoMu5k3PQS1nQbCtmAn1BreBsrh2L/9zaJF18C1HrdV5AYZpNokiakrMjxvw01ZAwxsaCflqqr
2udV0KSQSH0FISPJbRJr/1rAjFIP/2LBL3EVahfRr+iwXROzUKMoW04PJj05SF3idHMz2NwecIo
Xby3nA2e/WY0u/8UhqJauZ/+d1vr5H/809VC1ASR4PL0Nrx2Vi0wjG25WYwuZNe+hQ==
server ntp.bluecoat.com
server ntp2.bluecoat.com
server symmetric-key
!
```

password-policy

Configure password rules for administrative users. For example, you can require that the password contain at least one uppercase letter, one number, and one special character. By default, the password length and prohibit-common-words rules are defined. The default minimum password length is six characters.

Tip: After the initial upgrade to Management Center 2.0.x, any admin passwords that were defined in MC 1.x that do not adhere to the default password policy are respected. When they are changed, however, or when new administrator passwords are defined, these rules apply.

Syntax

```
(config)# password-policy ?
min-digits <value>
```

Set the minimum number of digits required in a password. Range: 0-255. By setting this rule to 0 (the default), numbers are not required in a password.

min-groups <value>	Set the minimum number of password rules (min-digits, min-lowercase, min-special, min-uppercase) that must be met. Range: 0-4. By setting this rule to 0 (the default), the password does not have to meet a minimum number of rules. For example, if you set min-digits and min-special rules, you would set min-groups to 2. Note: min-length is not counted as a rule for the purposes of the min-groups command.
min-length <value>	Set the minimum number of characters required in a password. Range: 0-255. The default password length is 6, but the password can have any length.
min-lowercase <value>	Set the minimum number of lowercase letters required in a password. Range: 0-255. By setting this rule to 0 (the default), lowercase letters are not required in a password.
min-special <value>	Set the minimum number of special characters (symbols) required in a password. Range: 0-255. By setting this rule to 0 (the default), special characters are not required in a password. Here are some supported examples of special characters: !\"#\$%&' ()*+, -./:;<=>?@[\\`^_{}]. This release does not support the tilde (~) as a special character.
min-uppercase <value>	Set the minimum number of uppercase letters contained in a password. Range: 0-255. By setting this rule to 0 (the default), uppercase letters are not required in a password.
prohibit-common-words builtin	Don't allow common dictionary words to be specified in passwords.
prohibit-whitespace true false	Enable/disable rejection of white space in passwords. Default=false.

Notes

- The sub-commands listed above can either be entered in password-policy configuration mode (at the config-password-policy prompt) or in configuration mode (at the config prompt).
- Use the **show password-policy-configuration** command to display the password policy settings.
- To remove a rule, type **no** before the rule command. For example: **no min-lowercase**
- If you configure multiple password policy rules but don't configure the **min-groups** command, the rules will not take effect; only the **min-length** rule will be enforced.
- If your password contains an exclamation mark, the Management Center CLI interprets it as a comment character, unless it is quoted. For more information, see Command Line Overview.

Examples

To require a password to have at least 8 characters, and have at least one number, one symbol, and one uppercase letter, set the following rules:

```
(config)# password-policy
(config-password-policy)# min-length 8
(config-password-policy)# min-digits 1
(config-password-policy)# min-special 1
(config-password-policy)# min-uppercase 1
(config-password-policy)# min-groups 3
(config)# show password-policy-configuration
min-uppercase: 1
min-groups: 3
prohibit-whitespace: false
min-special: 1
min-digits: 1
min-length: 8
min-lowercase: 0
prohibit-common-words: No dictionary defined
```

After these rules are configured and a user tries to specify "test" for the user password, the following message will appear:

```
(config local-user-list john_jones)# password test
Please enter a valid password.
Password must contain at least 1 uppercase characters.
Password must contain at least 1 special characters.
Password must contain at least 1 digit characters.
Password matches 0 of 3 character rules, but 3 are required.
Password must be at least 8 characters in length.
```

proxy-settings

Configure an HTTP proxy server in situations where your network requires all

servers to connect through a proxy to access Internet resources.

Syntax

(config)# proxy-settings enable disable host <hostname or IP address> password <string> port <value> username <string>	
(config)# proxy-settings view	
disable	Turn the proxy settings off.
enable	Turn the proxy settings on.
host <hostname or IP address>	Configure the HTTP proxy host name or IPv4/IPv6 address.
password <string>	Enter the password for the HTTP proxy server.
port <value>	Define the port number of the HTTP proxy server (0-65535).
username <string>	Enter the user name for the HTTP proxy server.
view	View the HTTP proxy config settings

You can enter all the subcommands in one line, or enter each command on a separate line.

Note: If your password contains an exclamation mark, the Management Center CLI interprets it as a comment character, unless it is quoted. For more information, see [Command Line Overview](#).

Examples

```
(config)# proxy-settings enable host 10.10.12.11
(config)# proxy-settings enable
(config)# proxy-settings host 10.10.12.11
(config)# proxy-settings port 8008
(config)# proxy-settings view
enabled:true
host :10.10.12.11
port no:8008
username:becky
```

security

Specify security options for Management Center, including where administrators can access the appliance from, what client certificates they require (if enabled) and whether they can access the appliance by HTTP or not.

Caution: The options and subcommands listed here are applicable when the security command is run from a (config)# prompt. You may also run this command from an enable prompt, but the primary focus of that is to view your existing security configuration.

Syntax

(config)# security [subcommands]	
allowed-hosts [add delete view]	Add, remove, or view the IP addresses that are allowed to access Management Center.
client-authentication [disable password-requirement <enable/disable> set-mandatory <cr> set-optional <cr> set-regex <value>]	Set restrictions for how Management Center challenges administrative users to use X.509 client certificates to login.
hsts [disable enable view]	Enable, disable, or view support for HTTPS Strict Transport Security (HSTS) protocol.
http	Enable, disable, or view the current setting for HTTP management console access on ports 8080 and 9009.

Example

```
(config)# security allowed-hosts
```

Tip: Changes to this security command will take effect the next time Management Center is restarted.

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:

```
(config)# 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.

Note: The `security allowed-hosts` command has no effect on Management Center failover pairs.

```
(config)# security client-authentication disable
```

Disable X.509 client authentication.

```
(config)# security client-authentication password-requirement
```

Subcommands:

```
(config)# security client-authentication password-requirement enable  
(config)# security 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 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 the following topics in the Configure Users, Roles, and Attributes section of this guide for more information:

- Use LDAP Subject Alternative Name Data for Certificate Validation
- Authenticate Users with SSL Mutual Authentication

#security 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 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 client-authentication set-regex

Sets the regex command used to extract the certificate's name or data set in the certificates Subject Alternative Name (subjAltName); the default is `CN=(.*?), .`

Subcommand:

default

Resets the principal regex to the default.

Subject alternative name example:

```
(config)#security client-authentication set-regex  
"1\\.3\\.6\\.1\\.4\\.1\\.311\\.20\\.2\\.3,\\s\\[0\\](.*?)@\"
```

Refer to Use LDAP Subject Alternative Name Data for Certificate Validation for more information.

```
# security client-authentication view
```

View current X.509 client authentication settings.

```
(config)# security hsts [enable | disable | view]
```

Enable, disable, or view the HTTPS Strict Transport Security (HSTS) protocol and adds Strict-Transport-Security header to responses. Support for HSTS depends on your client software and its support of this feature.

Warning: Before enabling this option, ensure that your Management Center appliance has a DNS record, that all administrators access it using the hostname associated with that DNS record, and that an SSL certificate that has been signed by a trusted certificate authority (CA) is installed. See [Statistics Monitoring over HTTPS](#) for steps to install a CA-signed certificate.

```
(config)# security http
```

Subcommands:

```
# 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.

Note: If you enable HTTP after using HTTPS, you must delete the HTTPS cookie from your browser to be able to use the HTTP connection for the UI.

Tip: Changes to this security command will take effect the next time Management Center is restarted.

service-action

The service-action command allows you to view disk usage and troubleshoot the following:

- Disk space or possible file corruption issues
- Cache repository index issues
- Possible VPM cache corruption issues

Perform Disk Maintenance

Clean your disk by using the **#service-action 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-action db-maintenance
```

Note: 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.

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 **#service-action purge-vpm cache** command.

Syntax

```
#service-actionpurge-vpm cache
```

Rebuild Cache Repository Index

Management Center maintains an index of device backups, policy, scripts, and other configuration elements. If issues arise with this index, Management Center may behave in an unexpected manner. As directed by Symantec support staff, run this command to rebuild the cache repository index.

Syntax

```
#service-actionrebuild-repository-index
```

Remove Orphan Device Count in Statistics Monitoring Dashboard

One or more "orphan" devices can be shown in the Statistics Monitoring Dashboard if the following is true:

- A user replaced a monitored device on the network with a different device that used the same IP address, without completing the **RMA Device** operation.

This caused Management Center to retain information about removed device in Statistics Monitoring Database. You can now remove these orphan devices using the following CLI command.

Syntax

```
# service-action purge-statistics-monitoring-orphans
```

After you execute the command, Management Center deletes the orphans and writes the results to syslog.

snmp

Configure Secure Network Management Protocol (SNMP).

Syntax

```
(config) # snmp ?
```

agent	Configure the SNMP agent. When an SNMP manager polls a device for information, the SNMP agent on the device responds to the queries. See "snmp agent" on the next page.
community	Define the community strings for SNMP v1/v2c. See "snmp community" on the next page.
system	System configuration (contact, location, name). See "snmp system" on page 916.
usm local	Define an SNMP local user entry. See "snmp usm local" on page 917.

usm remote	Define a user or a management system that receives notification of SNMPv3 traps and informs. See "snmp usm remote" on page 918.
vacm	Configure view-based access control model. See "snmp vacm group access" on page 918 and "snmp vacm group member" on page 919.

snmp agent

When an SNMP manager polls a device for information, the SNMP agent on the device responds to the queries.

Syntax

(config) snmp agent ?	
disabled	Disable the agent
enabled	Enable the agent.
max-message-size <value>	The maximum length of SNMP message the agent can send or receive. Range: 484-214748364. Default=50000.
version v1 v2c v3	SNMP protocol version used by the agent.

Examples

```
(config)# snmp agent enabled
(config)# snmp agent version v3
```

snmp community

Define community strings for SNMP v1/v2. The community string acts as a password for accessing statistics on the device. Equipment usually ships with a read-only community string set to *public* but network managers typically change the community string to a customized value. Each system that polls your appliance could potentially have a different community string.

Note: SNMP community strings are used only by devices that support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

Syntax

```
(config)# snmp community <string>
```

After defining the community string, the command prompt changes, indicating the community string. For example, for a community string `public`, the prompt looks as follows:

```
(config-community-public)#
```

The following sub-commands are available in community string configuration mode.

<code>name <string></code>	Necessary only when the community string is not the same as the index.
<code>sec-name string <value></code>	Initially set to the value of 'index.'
<code>target-tag <target_name></code>	Limit access for this community to the specified target(s). See <code>snmp target</code> for more information.

Examples

```
(config)# snmp community public
(config-community-public)# target-tag v1target
```

snmp system

Configure SNMP system settings to identify the contact name, location, and fully-qualified domain name of the appliance.

Syntax

```
(config) snmp system ?
```

<code>contact <name></code>	The name of the person managing the appliance; <code><name></code> can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.
<code>location <place></code>	The physical location of the appliance (room, floor, building), where <code><place></code> can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.
<code>name <fqdn></code>	The appliance's fully-qualified domain name for SNMPv1, where <code><fqdn></code> can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.

Examples

```
(config)# snmp system contact "Gail Jellison"
(config)# snmp system location "building B, 1st floor"
```

snmp usm local

Define an SNMPv3 local user entry.

Syntax

```
(config)# snmp usm local user <user_name>
```

After defining the local user name, the command prompt changes, indicating you are in configuration mode for the local user. You can then define authentication and/or privacy keys that a management system can use to access the appliance.

```
auth [md5 | sha {key <key> | password <password>}]
```

Specify either the MD5 or SHA hash algorithm and enter an authentication key or password for the user (8-32 characters).

```
priv [aes | des {key <key> | password <password>}]
```

Specify either the AES or DES encryption algorithm and enter the privacy key or password (8-32 characters).

Examples

```
(config)# snmp usm local user altman
(config-user-altman)# auth md5 password Gquw4321
(config-user-altman)# priv aes password Gquw4321
```

Note: If your password contains an exclamation mark, the Management Center CLI interprets it as a comment character, unless it is quoted. For more information, see Command Line Overview.

snmp usm remote

Define the remote engine ID that receives notification of SNMPv3 traps and informs.

Syntax

```
(config)# snmp usm remote
```

snmp vacm group access

Define access for an SNMP group. Each group is defined by a name, a security model (and level), and a set of views that specifies which types of MIB data that access group can read or write.

Syntax

```
(config)# snmp vacm group <group_name> access {usm | v1 | v2c} {auth-no-priv | auth-priv | no-auth-no-priv}
```

auth-no-priv	A connection that is secured with a passphrase and authentication but no encryption.
---------------------	--

auth-priv	A connection that is secured with both authentication and encryption.
------------------	---

no-auth-no-priv	A connection that uses a simple passphrase (known as a shared secret) to secure the communication.
------------------------	--

After defining the access rights for the group, the command prompt changes, indicating the security level. For example:

```
(config-access-v1/auth-no-priv) #
```

You then need to specify the name of the MIB view for each type of access.

notify-view <MIB_view>	Specify the name of the MIB view of the SNMP context authorizing notify access. For example, in Content Analysis the view is named cas-view (and is not user-definable).
-------------------------------------	--

read-view <MIB_view>	Specify the name of the MIB view of the SNMP context authorizing read access. Note that SNMPv1 is not permitted in read-view.
-----------------------------------	---

write-view <MIB_view>	Specify the name of the MIB view of the SNMP context authorizing write access. Note that write-view is not implemented in all products.
------------------------------------	---

Examples

```
(config)# snmp vacm group cas-group-v2c access v2c auth-no-priv
(config-access-v1/auth-no-priv) # read-view cas-view
```

snmp vacm group member

Define an SNMP access group member for a defined set of access rights.

Syntax

```
(config)# snmp vacm group <group_name> member <member_name> {sec-model usm  
| v1 | v2c}
```

Examples

```
(config)# snmp vacm group cas-group-2vc member member1 sec-model v2c  
(config)# snmp vacm group cas-group-2vc member member2 sec-model v2c
```

After defining members, you can define the access rights for the group. See "snmp vacm group access" on the previous page.

splunkforwarder

Manages the Splunk forwarder service. Forwarders collect data (primarily log events) from employee endpoints and servers, and deliver the data to Splunk Enterprise or Splunk Cloud for indexing and analysis.

For Management Center (MC), the Splunk forwarder forwards MC system-specific logs. Essentially, this is the MC syslog.

Syntax

```
(config) # splunkforwarder ?
```

host <host name or ip address>	Configure the host name or IP address of the Splunk forwarder.
port <number>	Define the Splunk forwarder's listening port number.
reload	Reload configuration and restart Splunk forwarder service.
status	Display the status of the Splunk forwarder service (running or stopped).
stop	Stop the Splunk forwarder service.

Examples

```
(config)# splunkforwarder host 10.10.10.10  
(config)# splunkforwarder port 9997  
(config)# splunkforwarder status  
running
```

ssh generate

Generate a 2048-bit RSA host key pair. If you believe the key's security was compromised, you can generate a new SSH key pair.

Syntax

```
(config) # ssh generate host-keypair | view
```

Example

```
(config) # ssh generate host-keypair
Are you sure you want to regenerate the keypair? [yes,no] y
SSH host key successfully regenerated
```

ssh ciphers

Enable or disable Cipher Block Chaining (CBC) ciphers. By default, CBC ciphers are disabled.

Syntax

```
(config) # ssh ciphers
```

disable-cbc	Disables CBC ciphers.
enable-cbc	Enables CBC ciphers.
view	View the available ciphers.

Example

```
(config-ssh) # ciphers view
Ciphers: aes128-ctr,aes192-ctr,aes256-ctr
(config-ssh) # ciphers enable-cbc
(config-ssh) # ciphers view
Ciphers: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes256-cbc
```

ssl

Configure Secure Socket Layer (SSL) settings.

Syntax

```
(config) # ssl ?
```

create [keyring ccl self-signed-certificate signing-request ssl-context]	Create SSL objects. See "ssl create" on page 923.
---	---

<code>delete [ca-certificate certificate keyring signing-request ssl-context]</code>	Delete SSL objects. See "ssl delete" on page 924.
<code>edit [ca-certificate certificate keyring signing-request ssl-context]</code>	Edit the appliance's current SSL settings. See SSL Edit .
<code>inline [ca-certificate ccl certificate keyring signing-request]</code>	Import SSL keyrings, CA certificate lists, signing requests, and certificates. See "ssl inline" on page 926.
<code>regenerate certificate <keyring-id> subject <subject> [alternative-names] [force]</code>	Regenerate an existing CA certificate and provide new subject and alternative name data. Force is optional, and will overwrite an existing certificate without confirmation.
<code>trust-package [auto-update download-now update-interval url]</code>	Manage the list of trusted CA certificates provided by Symantec, how frequently to update it, and from where.
<code>view [ca-certificate ccl certificate keypair keyring signing-request ssl-context]</code>	View available SSL objects.

Notes

- The sub-commands listed above can either be entered in SSL configuration mode (at the config-ssl prompt or in configuration mode (at the config prompt).
- Use the **show full-configuration ssl** command in configure mode to display basic SSL settings, and **(config-ssl-view)# ?** to view specific keyrings, CA Certificate Lists, Certificates, and Certificate Signing Requests.

Examples

Add a certificate from a Certificate Authority; the certificate name in this example is *ca1*.

```
(config)# ssl
(config-ssl) inline ca-certificate ca1 content
Enter the certificate below and end it with a Ctrl-D
-----BEGIN CERTIFICATE-----
MIIEDTCCAvWgAwIBAgIJAIIk7y/gggzO8MA0GCSqGSIb3DQEBBQUAMIGcMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsawZvcm5pYTEsMBAGA1UEBwwJU3Vubn12YWx1
MRIwEAYDVQQDALCbHV1IENvYXQxFDASBgNVBAsMC0RldmVs3BtZW50MRQwEgYD
VQQDDAtjYS5ibhV1Y29hdDEkMCIGCsqGSiB3DQEJARYVZXJpYy5jaG1AYmx1ZWNv
YXQuY29tMB4XDTE1MDExMzAxMzI0MFoXDTI1MDExMDAxMzI0MFowgZwxCzAJBgNV
BAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDA1Tdw5ueXZhbgUx
EjAQBgNVBAoMCUJsdWUgQ29hdDEUMBIGA1UECwwLRGV2ZWxvcG1lbnQxFDASBgNV
BAMMC2NhLmJsdWVjb2F0MSQwIgYJKoZIhvCNQkBFhVlcmljLmNoaUBibHV1Y29h
dC5jb20wggEiMA0GCSqGSiB3DQEBAQUAA4IBDwAwggEKAoIBAQCyxBQYApdEvNc
Nv6e7ELUTYRvnixueKceQM1y28Lj171MPng6Dghs3ZKF/VPXw+1Esc+LG11a75d9
WziSsv7u4nKjt2Y2nPC4jE8jzgI7Fej26B6//bePh91v/+bJRWNSYR9z6wNa0cQt
prxe6SvUbq7MkuE6vC9paqBqz4TQL0vyVHalZXxodRLJaKGsZmq1yn1ogxjBT9+
Mj3HdmzVVRPQ5jNNjV6oKppGOrqpFkz0wcjpkWuf0gk850kjB2mOBE4QDHbJhtg
UtLMSGLaj2hmb58v6JdDR0n4T3piEDzAP1/4N9a0fb1f2nrdrNi2n5d8Q2JaXH
hXPGBGrVAgMBAAGjUDBOMB0GA1UdDgQWBTCph9yrG16afTN6vaZJDTT2iv6xDaf
BgNVHSMEGDAwBTCph9yrG16afTN6vaZJDTT2iv6xDAMBgNVHRMEBTADAQH/MA0G
CSqGSiB3DQEBBQUAA4IBAQCMi+pLumWXIAiznvq+zU/3/PTHwzcVcwJdK+ngWbHa
-----END CERTIFICATE-----
```

<Ctrl-D>

CA certificate *ca1* is added successfully.

To view the certificate details for the *ca1* certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
Fingerprint: DB:AF:B1:82:EF:0C:9F:AD:84:F7:D8:35:0A:AA:0B:5D:93:DA:77:A5
```

ssl create

Create SSL keyrings, CA Certificate Lists (CCLs), signing requests, self-signed certificates, and ssl-contexts.

Syntax

```
(config)# ssl create ?
```

```
ccl
```

Create a
CA Certificate
List (CCL).

```
keyring <keyring id> algorithm rsa length <key_Length>  
showable [yes | no | management]
```

Create a keyring.
Keyrings are
containers for
SSL certificates
and their
associated
public and
private keys on
the appliance,
and can be used
to manage self-
signed or CA-
signed
certificates.

For RSA keys,
key length
values are 2048,
3072, 4096.
Default = 2048.

```
certificate <keyring id>
```

Create a self-
signed
certificate
associated with
the specified
keyring. You will
be prompted to
define values for
each of the
certificate fields
(country, state,
and so forth).

signing-request <keyring id>	Create a request for a signed certificate associated with the specified keyring. You must specify all parameters when prompted for 'Value' for 'subject'
---	--

Examples

```
(config)# ssl create keyring sslkey algorithm rsa length 3072 showable no
(config)# ssl create signing-request sslkey
Value for 'subject' (<Certificate subject>): C=US,ST=CA,O=Symantec,CN=mc
alternative-names 198.51.100.20, csr.symantec.com
ok
```

ssl delete

Delete SSL certificates, keyrings, and signing requests.

Syntax

(config)# ssl delete ?	
ca-certificate <certificate name>	Delete CA certificate.
certificate <keyring id>	Delete the certificate that's in the specified keyring.
keyring <keyring id>	Delete the specified keyring.
signing-request <keyring id>	Delete the certificate request for the specified keyring.
ssl context <context_id>	Delete the specified SSL context.

Example

```
(config-ssl)# delete signing-request sslkey
```

ssl edit

Edit CA certificate lists (CCLs) or SSL contexts.

Syntax

(config)# ssl edit ccl <ccl_name> [action] ?	
add	Add a certificate by name to the selected CA certificate list.
remove	Remove a certificate from the selected CA certificate list.
reset	Empty the CA certificate list for this CA certificate list.
set	Set CA certificate list for this CA certificate list.
view	View the certificates in the selected CA certificate list.
(config)# ssl edit ssl-context <context_id> [action] ?	
ccl	Set the CCL for the SSL context.
cipher-suites	SSL context cipher suite configuration.
keyring	Set the keyring for the SSL context.
protocols	Set SSL context protocols.
view	View the SSL context configuration.

Examples

```
(config)# ssl
(config-ssl)# edit ccl browser-trusted

(config-ccl-browser-trusted)# add esignit.org
ok

(config-ccl-browser-trusted)# view

Name: browser-trusted
FIPS compliant: no
Certificates:
  1st_Data_Digital
  A-Trust-Qual-02
  A-Trust-Root-05
  A-Trust-nQual-03
  AC1_Raiz_Mtin
  ACA_ROOT
  ACCV_ACCVRAIZ1
  ACEDICOM_Root
  ..
  ..
```

ssl inline

Import SSL keyrings, signing requests, and certificates.

Syntax

(config)# ssl inline ?	
ca-certificate <certificate name> content	Import a Certificate Authority (CA) certificate from terminal input (typically by pasting the certificate content with a right-click).
certificate <keyring id>	Press Ctrl-D after pasting the certificate content.
	Import a certificate into the specified keyring.

keyring <keyring id>	Install a keyring. Keyrings are containers for SSL certificates on the appliance, and can be used to manage self-signed or CA-signed certificates.
	You will be prompted to paste the keyring content and press Ctrl-D when finished.
signing-request <keyring id>	Install a request for a signed certificate associated with the specified keyring.
	You will be prompted to paste the signing request content and press Ctrl-D when finished.

Examples

Add a certificate from a Certificate Authority; the certificate name in this example is *ca1*.

```
(config)# ssl
(config-ssl) inline ca-certificate ca1 content
Enter the certificate below and end it with a Ctrl-D
-----BEGIN CERTIFICATE-----
MIIEOTCCA...bGvWgAwIBAgIJAk7y/gggz08MA0GCSqGSIb3DQE...CQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvc...pYTESMBAGA1UEBwwJU3Vubn12YWx1
MRIwEAYDVQQKDA1CbHV1IENvYXQxFDASBgNVBA...MC0R1dmVs...3BtZW50MRQwEgYD
VQQDAtjYS5ibHV1Y29hdDEkMCIGCSqGSIb3DQEJARYVZXJpYy5jaG1AYmx1ZWNv
YXQuY29tMB4XDTE1MDExMzAxMzI0M...oFwZwx...CzAJBgNV
BAYTA1VTMRMwEQYDVQQIDA...pDYWxpZm9ybmlhMRIwEAYDVQQHDA1Tdw5ueXzbGUx
EjAQBgNVBAoMCUJsdWUgQ29hdDEUMBIGA1UEC...wLRGV2Z...vcG11bnQxFDASBgNV
BAMMC2NhLmJsdWVjb2F0MSQwIgYJKoZIhv...cNAQkB...hV1cm...l...jLmNoaUBibHV1Y29h
dC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ...CysxBQYApdEvNc
Nv6e7ELUtYRvnixueKceQM1y28Lj17lMPng6Dghs3ZKF/VPXw+1Esc+LG11a75d9
WziSsv7u4nKjt2Y2nPC4jE8jzgI7Fej26B6//bePh91v/+bJ...RwNSYR9z6wNa0cQt
prx8e6SvUbq7MkuE6vC9paqBqz4TQL0vyVHaWZX...odRLJaKGsZmq1yn1ogxjBT9+
Mj3HdmzVVRPQ5jNNjV6oKppGOrqpFkz0wcjpKwuf0gk850kj...sB2mOBE4QDHbJhtg
UtLMSGLaj2hb...58v6JdDRon4T3piZDzAP1/4N9a0fb1iF2nrdRNi2n5d8Q2JaXH
```

```

hXPGBGrVAgMBAAGjUDBOMB0GA1UdDgQWBTCph9yrG16afTN6vaZJDTT2iv6xDAf
BgNVHSMEGDAwGBCph9yrG16afTN6vaZJDTT2iv6xDAMBgNVHRMEBTADAQH/MA0G
CSqGSIB3DQEBBQUAA4IBAQCMi+pLumWXIAiznvq+zu/3/PTHwzcVcwJdK+ngWbHa
GGVAhC+aMe+k3K+tT00+3zxkSA7zF5X0NSZSRUAovZMrbXRxj+Ruk1CMETEVAFzI
70uJv1EQoSt/Fg+Ax0h8M0Jn4lvUGsYPIAbcLjlxCtMNyfcOUG1Ss0yo/A/GXg13
eWINmdtdZHT/+ge01EEssswLxbyw3Py14CRMprjxlzg15Rx/PWV+zB+P2yo1IrV4
pb5fsCuNrK41Ysdco5XE6P2m0c3P8QL/pB4SiZgWCr1sd0IKIoEphTk0kI++PTYx
d8cuVqPUXEi+UmibOBtfDz2ZffNkmBTdyvLfesINz0ce
-----END CERTIFICATE-----

```

<Ctrl-D>

CA certificate ca1 is added successfully.

To view the certificate details for the ca1 certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
Fingerprint: DB:AF:B1:82:EF:0C:9F:AD:84:F7:D8:35:0A:AA:0B:5D:93:DA:77:A5
```

ssl view

View certificate and keyring details and signing request confirmations.

Syntax

(config)# ssl view ?	
ca-certificate <certificate name> [verbose]	Show CA certificate and content.
ccl <ca certificate List name>	View the details for a specific CA Certificate List.
certificate <keyring id>	Show the certificate that's in the specified keyring.
keypair <keyring id>	Show the RSA private key for the specified keyring.
	If the keyring was created with the "showable no" option, the key will not be displayed.
keyring <keyring id>	Show details about the specified keyring, including its certificate and any signing requests.

signing-request <keyring id>	View certificate request for the specified keyring.
ssl-context <context id>	View SSL context configuration.

Examples

To view the certificate details for the ca1 certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
Fingerprint: DB:AF:B1:82:EF:0C:9F:AD:84:F7:D8:35:0A:AA:0B:5D:93:DA:77:A5
```

To show information about a keyring, in this case called **sslkey**:

```
(config-ssl)# view keyring sslkey
Keyring ID: sslkey
Private key showability: no-show
Signing request: absent
Certificate: present
Certificate subject:
/C=us/ST=ca/L=pa/O=symantec/OU=marketing/CN=symantec.com/emailAddress=test@test.com
Certificate issuer:
/C=us/ST=ca/L=pa/O=symantec/OU=marketing/CN=symantec.com/emailAddress=test@test.com
Certificate valid from: Jul 21 05:17:51 2017 GMT
Certificate valid to: Jul 21 05:17:51 2017 GMT
Certificate thumbprint:
D7:3A:40:69:1A:D1:C2:77:95:B0:0F:DB:97:55:DE:02:BB:A9:54:00
```

To view the CA certificates contained in the CA certificate list, bluecoat-licensing:

```
(config-ssl)# view ccl bluecoat-licensing
Name: bluecoat-licensing
FIPS compliant: no
Certificates:
BC_Engineering_CA
```

To view the default SSL context:

```
(config-ssl)# view ssl-context default
Name: default
Keyring: default
CCL: browser-trusted
Protocols: tlsv1.2 tlsv1.1 tlsv1
```

```
Cipher suites: ecdhe-rsa-aes256-sha dhe-rsa-aes256-
sha aes256-sha256 aes256-sha ecdhe-rsa-aes128-gcm-
sha256 ecdhe-rsa-aes128-sha256 ecdhe-rsa-aes128-sha
dhe-rsa-aes128-sha aes128-sha256 aes128-sha
```

statistics-monitoring

The **statistics-monitoring** command can be used view the parameters for the storage of device statistics for managed devices and to set thresholds for how long Management Center will retain that data. The thresholds set here control the data used for reports in Management Center's management console, under **Reports > Statistics Monitoring**. These reports contain data from devices that have been configured to report statistics, and their associated hardware statistics such as CPU and memory utilization, and traffic flow.

This command is available in both enable # mode and (config)# modes, however only the **view** subcommand is available in enable mode.

Syntax

# statistics-monitoring [subcommands]	
maintenance[enable disable]	Enable or disable database maintenance for gathered statistics. Database maintenance initiates constant analysis of the stored data with the goal of optimizing query performance for reports that use this data. The default value is enable.
set-per-hour-lifetime [<n> default]	Set a lifetime for how long the appliance will retain per-hour trend data. Must be entered in number of days between 1 and 732. The default value is 366 days.
set-per-minute-lifetime [<n> default]	Set a lifetime for how long the appliance will retain per-minute trend data. Must be entered in number of days between 1 and 30. The default value is 7 days.
view	View current statistics monitoring lifetime settings, record statistics, and disk usage data.

Example

```
# statistics-monitoring view
Total devices: 2
Reporting devices: 1
Maintenance: enabled
```

Data Characteristics:

	Lifetime Records	Disk Usage
minute	7 days 140439	91 MB
hour	366 days 142380	52 MB

timezone

Set the time zone where the appliance is located or choose the Coordinated Universal Time (UTC) time standard.

Syntax

```
(config)# timezone [<area>/<Location> | UTC | GMT]
```

Supporting Commands

show timezone current	Display the currently configured timezone
show timezone	Display the available timezone areas.
show timezone <area>	Display the full list of timezones in a specific area.
show timezone <value>	Display the current time to see the local time in a specific timezone.

Examples

To select UTC as the time standard (instead of setting a time zone):

```
(config)# timezone UTC
```

To set an Antarctica time zone:

```
(config)# show timezone
Africa
America
Antarctica
Arctic
Asia
Atlantic
Australia
Europe
Indian
Pacific
UTC
GMT
all
current
```

```
(config)# show timezone Antarctica
Antarctica/Mcmurdo
Antarctica/Rothera
Antarctica/Palmer
Antarctica/Mawson
Antarctica/Davis
Antarctica/Casey
Antarctica/Vostok
Antarctica/DumontD'Urville
Antarctica/Syowa
Antarctica/Troll
Antarctica/Macquarie
(config)# timezone set Antarctica/Davis
```

upload

Upload the third-party attributions zip file to an FTP site.

Syntax

```
# upload ATTRIBUTIONS <full-url/filename><username> <password>
```

Note: ATTRIBUTIONS must be in uppercase.

Note: If your password contains an exclamation mark, the Management Center CLI interprets it as a comment character, unless it is quoted. For more information, see Command Line Overview.

Example

```
upload ATTRIBUTIONS ftp://exampleftp.com/attribution.zip mary *****
```