Management Center 3.3.1.1 Release Notes

Revision: June 14, 2023

Table of Contents

Documentation Legal Notice 3
Management Center Release Notes 4
Licensing 5
Releases Directory 6
Upgrade Management Center 7
Downgrade Management Center 10
Back Up the Management Center Configuration 11
Management Center 3.3.1.1 12
New Features in Management Center 3.3.1.1 16
Management Center 3.2.1.1 21
New Features in Management Center 3.2.1.1 24
Management Center 3.1.3.1 (ABRCA Root CA Update Patch) 35
Management Center 3.1.1.1 37
New Features in Management Center 3.1.1.1 41
Management Center 3.0.1.1 48
New Features in Management Center 3.0.1.1 51
Management Center Known Issues and Fixes 58
Limitations 65
Reference Information 66
- Cross Product Support 66
- Third-Party Compatibility 66
- Reference: Management Center MIB Files 69
- Symantec Technical Support Resource 70
- Symantec Management Center Documentation Resources 71

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2005–2023 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Management Center Release Notes

Symantec® Management Center unifies management and reporting across Symantec products under a single operating environment and single pane of glass. Powerful central policy tools allow you to deploy effective web access security and governance across your entire organization. Management Center simplifies your tasks by providing inventory and health monitoring for the spectrum of our products: ProxySG, SSL Visibility, Content Analysis, Malware Analysis, Reporter, Integrated Secure Gateway, Advanced Secure Gateway, Web Security Service, and PacketShaper

This document provides information about the Symantec Management Center 3.3.1.1 release, including new features, known issues, and limitations. This document also provides reference information.

To determine the End-of-Life for this release, refer to the Broadcom support site.

Licensing

To enable features specific to your version of Management Center, you must install the correct license.

Your Management Center license contains components that expose all features available in this release, including the type of license that you have purchased. If features documented here are not available when you configure Management Center, contact your Sales Engineer immediately. Conversely, if you think that features are not fully documented, contact your Sales Engineer to give feedback.

By default, the automatic license check is enabled. That is, the **Auto-Update** option is selected on the **Administration** > **License** > **License Components** tab. A month before the currently installed license expires, the Management Center appliance automatically checks for license updates upon reboot (or once daily). To verify the current appliance license, navigate to the **Administration** > **License** tab and review the **Licensed Components**.

Releases Directory

This document presents information for each release in the Management Center 3.x software line. Each section for a specific release provides feature descriptions, and changes. Sections about known issues and limitations for each 3.x release are listed separately.

Release Index

- Management Center 3.3.1.1
- Management Center 3.2.1.1
- Management Center 3.1.3.1 (ABRCA Update)
- Management Center 3.1.1.1
- Management Center 3.0.1.1

Information About All Releases

- Management Center Known Issues and Fixes
- Limitations
- Reference Information

Upgrade Management Center

Best practices, important notes, and instructions for upgrading your Management Center appliance.

CAUTION
Always back up your Management Center configuration before upgrading or downgrading Then, store the backup off-box. If you experience problems with upgrading or downgrading, backing up the configuration ensures that you can restore it.

WARNING
When you first upgrade to 3.3.x from a non-3.3.x release, the system performs an upgrade and conversion of the statistics monitoring database to improve performance. The database upgrade often takes a long time. The system can appear to be ready—the user interface and CLI will be available—but the database conversion can still be in process.

Do not restart the statistics monitoring process before verifying that the database upgrade is complete. If you manually restart the statistics-monitoring service, the system interrupts the database upgrade, which puts the system in an unrecoverable state.

Before you perform any operations, verify that the statistics monitoring upgrade has completed by checking the **journal.txt** log:

1. Go to **Administration** > **Logs**.
2. Select the checkbox next to the **journal.txt** log.
3. Click **Download**.
4. Open the downloaded log file.
5. Search for the string `Successfully attached day_legacy table.`

If you find the string, the statistics monitoring upgrade has completed and you are free to resume operations.

Example

```
2023-04-07 03:20:59.857 [ type=LOG level=Major comp= guid=0 pid=19478 tid=7fa794ec39c0 tn=none
 sfile=cfg_db_ changelog.cpp sline=1005 sfunc=MigrateHourLegacyData ] Successfully attached
 day_legacy table as partition.
```

Failure Scenario

1. The admin initiates an upgrade from a non 3.3.x release (For example, 3.1).
2. The admin sees that the system user interface and CLI are available and assumes that the system is ready.
3. The admin attempts to perform an operation that requires the statistics monitoring database (for example, failover). but the operation fails (because the statistics monitoring upgrade is still in process).
4. To address the error, the admin restarts the statistics monitoring process.
5. The system interrupts the database upgrade, which puts the system in an unrecoverable state.

Upgrade Best Practice

When upgrading or downgrading Management Center, you must stay within two versions of what is running. Refer to this article for more information.

Potential 3.3 Upgrade Issues

After upgrading to Management Center 3.2 and later, you might lose communication with Management Center. This communication issue can occur in the following situation:

- You have assigned an IP address to Management Center in the range of `172.17.0.0/16` on your internal network.
- Management Center also has an internal Docker container that uses an IP address in the range of `172.17.0.0/16`.

Workaround: Add a static route for the problematic network to use the default gateway IP address. For more information, refer to this article.

Manage Management Center System Images

When new features and improvements are made to Management Center, you can download a system image from Symantec and can upgrade the appliance. If you 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.

When six images are stored on your system and you download another image, Management Center deletes the oldest unlocked image. Deleting the oldest image makes 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 3.x Software Image Installation:

Due to some major changes to the underlying systems that Management Center relies on, there are several important points to be aware of:

- Downgrades to 2.x or 1.x from any 3.x release are not supported. See Downgrade for more information.
- Upgrades from 1.x to 3.x are not supported. For the supported upgrade paths, consult the release note for your Management Center release.
- 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.
- The initial upgrade may take a long time to complete. Wait for the upgrade to complete. Any interruption in the upgrade process may result in instability. See this Warning.

Upgrade Management Center Failover Pair

During replication, configuration for both the primary and secondary failover partners is limited. Replication requires both the primary and secondary partners to run the same version of Management Center. To ensure that the partners are on the same MC version, 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 back up the configuration, export it off box, and then disable the failover pair. For full details, refer to About Management Center Failover.

Upgrade from 3.1.x or 3.2.x

> **NOTE**
> Management Center supports upgrading from two previous versions of what is running.

1. Before you begin, backup your Management Center configuration and export it off-box. If you must recover from a failed upgrade, you use this backup.
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.

   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`

   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 fails. If the installation fails, follow step 4b to modify the provided URL To use HTTP and port 8080 instead.

   If the image was uploaded to Management Center, complete the following steps:
   a. Copy the file URL. In the **Configuration > Files** page, select the image and click **Copy URL**. The file has a format similar to the following example:
      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, change the URL to the following format:
      http://localhost:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e
   c. Execute the `installed-systems load` command and wait for the upgrade to complete.

5. Reboot the hardware appliance to run the new image:

   ```
   # restart
   ```

   When the appliance restarts, the network connection closes. If a boot failure occurs upon an upgrade, Management Center downgrades to the previous version automatically.

6. Wait for the upgrade to complete. Do not attempt to restart the statistics monitoring service before verifying that it is ready. For more information, see this Warning.
7. Access the web-based management console at https://*management_center_ip*/8082
8. Access the CLI using an SSH client.
9. If necessary, disable TLS versions that were released before 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

When downgrading, adhere to the guidelines in this topic.

- You cannot downgrade from Management Center 3.3.1.1. The database structure in Management Center 3.3.1.1 has changed. Because of the database change, downgrading to an earlier release will not work because the database cannot be reconstructed.
- Downgrades cannot be performed from Management Center 3.x to 2.x or 1.x.
- 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.
- 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 required 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 noted previously 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 noted previously 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
   ```

Back Up the Management Center Configuration

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.

Important Management Center 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.

Management Center Backup Requirements

Backing up the Management Center configuration requires specific permissions. Sensitive data is encrypted with an encryption key. See the topic Understanding Job Permissions in the Management Center Configuration and Management Guide.

Management Center Backup Methods

You can back up Management Center in the following ways:

- Back Up Management Center Immediately
- Use a Job to Back Up Management Center
- Use the CLI to Back Up Management Center

Management Center 3.3.1.1

Release Information

- Release Date: February 16, 2022
- Build Number: 271087
- Document Revision: 2.0

Compatible With

See Third-Party Compatibility and Cross Product Support for information.

Deploying Management Center on Virtual Appliances

You can deploy Management Center virtual appliances on the following platforms:

- VMware® ESX Server 5.5, 6.5, and 6.7
- KVM 1.5.3 on CentOS 7.3
- Xen Hypervisor in Amazon Web Services (AWS)

  NOTE
  Use only `aws.bcsi` images to install or upgrade Management Center on AWS.
- Microsoft® Hyper-V Hypervisor
- Symantec Integrated Secure Gateway

  NOTE
  You must have a Management Center Enterprise License to deploy Management Center on ISG.

Refer to the following documents for deployment information:

- *Management Center VA Initial Configuration Guide*

Supported Upgrade Paths

Management Center 3.3.1.1 supports the following upgrade paths:

- 3.2.x to 3.3.1.1
- 3.1.x to 3.3.1.1

Downgrade Support

Downgrade from 3.3.1.1 is Not Supported

You cannot downgrade from Management Center 3.3.1.1. The database structure in Management Center 3.3.1.1 has changed. Because of the database change, downgrading to an earlier release will not work because the database cannot be reconstructed.

Important Changes in 3.3.1.1

Management Center Threat Lab Statistics Widget Removal Notice

As of June 29, 2023, Management Center will no longer support the Threat Lab Statistics widget. Refer to this knowledge article for more details.

Manage Exception Pages from a Central Location

Administrators can create, edit, manage, and activate exception pages for one or many devices from a central location within Management Center. Version control and simplified and efficient deployment ensure the continuity of an exception page standard across multiple devices.

For more information about these new features, see New Features in Management Center 3.3.1.1.

Management Center Supported As An ISG VIrtual Instance

You can now deploy Managment Center as a virtual instance on an ISG appliance. Refer to the Virtual Machine Sizing Guidelines and the ISG documentation for more information.

Important Notes

Potential 3.3 Upgrade Issues

- **Potential Database Corruption**: When you first upgrade to 3.3.x from a non-3.3.x release, the system performs an upgrade and conversion of the statistics monitoring database to improve performance. The database upgrade often takes a long time. The system can appear to be ready—the user interface and CLI will be available—but the database conversion can still be in process.

  Do not restart the statistics monitoring process before verifying that the database upgrade is complete. If you manually restart the statistics-monitoring service, the system interrupts the database upgrade, which puts the system in an unrecoverable state. For more information, see this important Warnng.
- **Communication Issues**: After upgrading to Management Center 3.2 and later, you might not be able to communicate with Management Center. This communication issue can occur in the following situation:
  - You have assigned an IP address to Management Center in the range of `172.17.0.0/16` on your internal network.
  - Management Center also has an internal Docker container that uses an IP address in the range of `172.17.0.0/16`.

  Workaround: Add a static route for the problematic network to use the default gateway IP address. For more information, refer to this article.
- **Java VPM Editor Does Not Launch**: Management Center 3.3.1.1 includes a known issue that is preventing the legacy Java VPM editor from launching.
- **Support for Installing Management Center Certificates on Content Analysis to Establish SSL Trust**: Due to a configuration change in Content Analysis, the procedure for installing MC certificates on Content Analysis devices to establish SSL trust is valid only for CA appliances running 3.0.x or earlier. You cannot use the procedure for CA appliances running 3.1.x or later.
- **Potential IP Mismatch on Default Certificate**: Due to bug MC-2899, when the IP address of your Management Center (MC) appliance changes (either manually or during initial configuration), the system does not update the default certificate with the new IP address. Because the default certificate is not properly updated, any features that rely on that certificate for communication attempt to communicate to MC using an incorrect IP address.

  The issue *always* occurs during initial configuration because DHCP assigns a default address when the user invokes the initial configuration wizard.

  The issue *always* occurs during initial configuration because DHCP assigns a default address when the user invokes the initial configuration wizard.

  Most MC functions and operations are not impacted by this issue. In fact, you might not notice the issue until you send PDM (statistics) data from a monitored device to MC. **WORKAROUND**:

  1. Enter the following command and record the certificate subject distinguished name:

     ```
     # ssl view keyring default
     ```
  2. Regenerate the certificate, inserting the subject data you collected in step 1:

     ```
     # ssl regenerate certificate default subject "insert subject" force
     ```
  3. Restart MC after regenerating the default certificate. The restart is required to clear the cached copy of the old certificate:

```
# restart
```

SSL regenerate certificate example:

```
# ssl regenerate certificate default subject "C=US,ST=CA,L=Los
 Angeles,O=Example,OU=0000000000,CN=203.0.113.5" force
```

NOTE
For more information on the ssl command, refer to ssl.

- **PDM Data Collection**: If you are using PDM data collection, specify a hostname in the Device Communications option (**Administration > Settings > Device Communications**). If no hostname is specified, PDM data collection may fail.

Web VPM Usage with SGOS Devices

Advanced Secure Gateway (ASG) version 6.7.4.2, ProxySG version 6.7.4.2, and Reverse Proxy (RP) version 6.7.4.2 have been removed from general availability on the customer download site but is available upon request in Limited Availability (LA). SGOS Release 6.7.4.2 contained an issue in the Web Visual Policy Manager (web VPM) that could result in changes to the installed policy with no warning displayed.

The new web VPM should NOT be used in ASG/SG/RP 6.7.4.2. If it has already been used, Symantec recommends that proxy administrators verify their existing policy and then download ASG/SG/RP version 6.7.4.3 which contains a fix for this issue.

For more details, refer to: https://support.symantec.com/en_US/article.TECH253006.html

Refer to Federal Information Processing Standards (FIPS) Mode for more information.

New Features and Feature Enhancements

- This release of Management Center introduces numerous new features and enhancements to existing features. See New Features in Management Center 3.3.1.1.

Limitations

- See Limitations.

Known Issues and Fixes

- See Management Center Known Issues and Fixes for a list of known issues and fixes that Symantec is aware of for Management Center.
- In rare instances, the web User Interface (UI) does not load immediately following an upgrade to this release. The upgrade process takes longer to upgrade the system database than the core system, and that can lead to the system not being ready following the OS upgrade. Symantec recommends that if you experience this issue, to wait an additional 5 minutes following the system upgrade before attempting to access the web user interface. If the service does not come up after 5 minutes, restart the management center service from the CLI. From the CLI privileged mode, type `system-services stop management-center` and then `system-services start management-center`.

Security Announcements

This release fixes the following vulnerability issues:

- SYMSA17650 Tomcat Vulnerabilities
- SYMSA17570 OpenSSL Vulnerabilities (CVE-2021-23840 and CVE-2021-23841)
- SYMSA17570 OpenSSL Vulnerabilities (CVE-2020-1968 and CVE-2020-1971)

Privacy Statement

This Product collects certain information, including personal data, in system logs regarding administrators who log in to configure the appliance. For support purposes, this information is uploaded to Symantec using a secure connection through a periodic “heartbeat." Customers can optionally upload additional data to Symantec using the “sosreport” feature to help Customer Support debug issues they are having. The personal data contained in “heartbeat” or “sosreport” includes user name and IP address of client machines.

New Features in Management Center 3.3.1.1

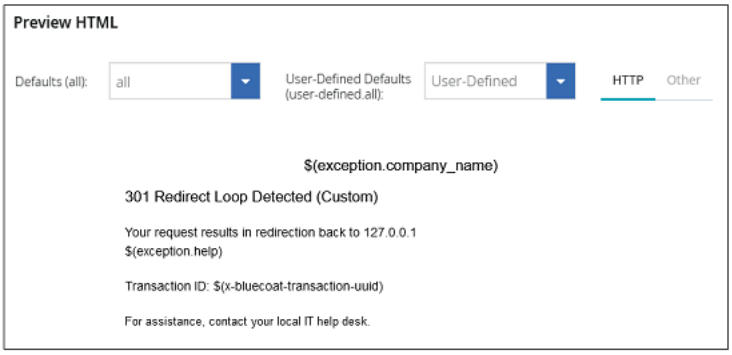
Management Center 3.3.1.1 Includes the following new features:

- Manage Exception Pages from a Centralized Location
- Management Center Supported As An ISG VIrtual Instance
- Integrated Secure Gateway (ISG) Enhancements
- Enterprise License SKU Support
- Ability to Filter ProxySG/ASG Policy Trace
- Ability to Select Content Analysis (CA) Backup Areas
- Concurrent Execution of Scripts
- Device Filtering for Summary Report
- Log Naming Enhancements
- Appstat Collector Improvements
- Optimizations to the Storage of PDM (Performance Data Management) Statistics

Manage Exception Pages from a Centralized Location

Administrators can create, edit, manage, and activate exception pages for one or many devices from a central location within Management Center. Version control and simplified and efficient deployment ensure the continuity of an exception page standard across multiple devices.

Exception pages can be created in Management Center, or imported from devices or files, and are stored as Policy Shared Objects. You can then edit the page to customize fields such as HTTP code, contact, and company name, or leave them blank and use a set of defaults. The editor supports any variables in the format of "$(variable.name)". The feature also includes a set of free-form fields where you can enter the custom HTML for the exception page. Then, you can preview the page as the user will see it.



You can also import exception page lists and deploy a collection of exception pages to a device or Cloud Secure Web Gateway (Cloud SWG), rather than deploying them individually.

Refer to Create and Manage Exception Pages for more information.

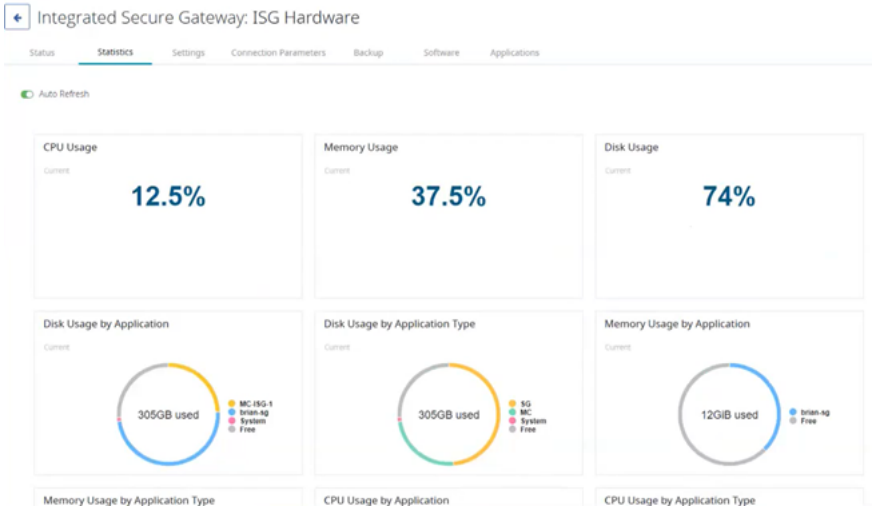
Management Center Supported As An ISG VIrtual Instance

You can now deploy Managment Center as a virtual instance on an ISG appliance. Refer to the Virtual Machine Sizing Guidelines and the ISG documentation for more information.

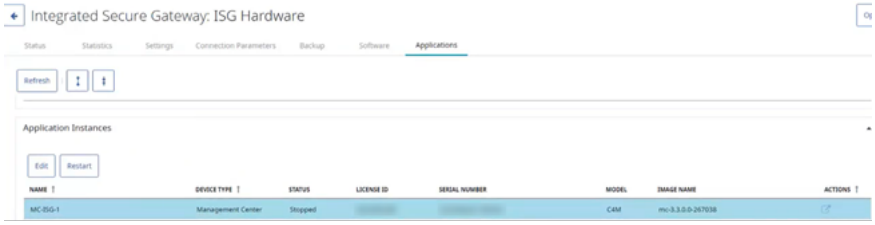
Integrated Secure Gateway (ISG) Enhancements

Management Center 3.3 includes the following ISG enhancements:

- **ISG Dashboard**: Management Center now displays a dashboard for ISG devices. The dashboard information includes CPU, memory, and disk usage. To view the dashboard, go to **Network** > ***Device*** > **Statistics**.



- **Management Center Applications**: Management Center now properly labels Management Center applications that have been installed on ISG devices. Previously, they were displayed as unknown applications. To view ISG applications, go to the **Applications** tab of the device details page (**Network** > ***Device*** > **Applications** > **Application Instances**).



- **Restart**. You can now restart ISG applications.
- **Edit**. When editing an ISG application, you can change the following properties:
  - The system image. Select a different system image from the list of applicable system images stored on that ISG.
  - The base model. Select a different model (and therefore, configuration) from the list of applicable model defined on that ISG. When you select a model, the system displays the details for each model, for example, CPUs, RAM, and so on. Refer to the ISG documentation for more information about ISG model numbers.

  When you change the system image or model number and click **Save**, the application restarts and reboots with the updated configuration.

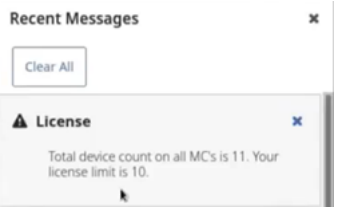
  To restart or edit an ISG application, go to **Network** > ***Device*** > **Applications** > **Application Instances**. Choose the instance and click **Restart** or **Edit**.
- **System Installation**: Installing a system image on a ProxySG that is installed as an ISG application is now supported, with the following caveats:
  - The ISG device hosting that ProxySG instance must also be managed by Management Center.
  - The system cannot mark the ProxySG image as default and will not reboot the ProxySG application on that ISG. To make the image the default image, you must install the system image and then use the Set Boot Image job to set the boot image. Alternatively, edit the ISG application to change the boot image. To edit an ISG application, go to

Network > *Device* > **Applications** > **Application Instances**. Choose the instance and click **Edit**. When you change the system image and click **Save**, the application restarts and reboots with the updated configuration.

- **Set Boot Image**: You can now set the boot image for ProxySG appliances running 7.3.6.1 or later installed as an Integrated Secure Gateway (ISG) application. However, the ISG device hosting the ProxySG instance must also be managed by Management Center. Management Center pulls the list of available images from that ISG.

Enterprise License SKU Support

Enterprise Licenses allow you to have several devices associated with a single license. The number of devices is dependent on your license. If you exceed the number of devices that are specified by your Enterprise license, Management Center (MC) displays a warning.



For example, consider that you have an Enterprise license with a 100-device limit. You have two MC appliances, one monitoring 40 devices and another monitoring 60 devices. If you add another device to either MC, the system displays a warning on both appliances indicating that you have exceeded your Enterprise license limit. If you clear the warning, you will not see it again unless you later add more devices. If you delete the offending devices, the system removes the message.

Ability to Filter ProxySG/ASG Policy Trace

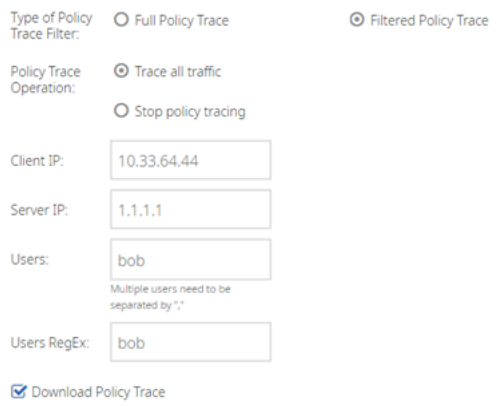
Management Center 3.3 includes a new feature that allows you to filter a ProxySG/ASG policy trace for specific data. When creating a policy trace using the device operations or by creating a Policy Trace Device job, you can apply one or more filters to the policy trace action. When you select **Filtered Policy Trace**, Management Center generates a snippet of policy and installs it at the end of the device's forward policy to enable filtering.

CAUTION
If you select **Filtered Policy Trace**, you must set at least one filter. A filtering rule with no trigger can cause the ProxySG appliance performance to substantially degrade.

The allowed filtering fields are as follows:

- **Client IP**: Enter a client IP address. Multiple client IP addresses are not supported.
- **Server IP**: Enter a server IP address. Multiple server IP addresses are not supported.
- **Users**: Enter one or more usernames, separated by commas.
- **Users Regex**: Enter a regex value to match one or more clients.

For example, consider that the admin entered the following filter data.



Using the data entered in the preceding example, Management Center generates the following snippet of policy and installs it at the end of the device's forward policy.

```
; START OF MC POLICY TRACE, DO NOT MODIFY <proxy>client.address=10.33.64.44 trace.request(yes)
 trace.destination("mc_trace") <proxy>user=bob trace.request(yes) trace.destination("mc_trace")
 <proxy>user.regex="bob" trace.request(yes) trace.destination("mc_trace") <proxy>server_url.address=1.1.1.1
 trace.request(yes) trace.destination("mc_trace"); END OF MC POLICY TRACE
```

NOTE
Management Center saves the filtered policy trace file as `mc_trace` . If you have created custom trace files on a device, you can also download those custom files. See Run ProxySG Policy Trace for more information. To view a policy trace file, go to **Jobs > Archived Files** and download the policy trace. See View ProxySG/ASG Policy Trace Report.

Ability to Select Content Analysis (CA) Backup Areas

Management Center 3.3 includes a method to select the specific CA configuration area to back up. This option only applies to CA appliances running 2.3.x and later. When you back up a device or schedule a backup job, you can now select the following CA backup areas:

- **Include Machine**: Includes machine-specific CA settings, such as the device name, IP address, and so on.
- **Include Network**: Settings that apply to machines on this network, such as proxy, DNS, NTP, and so on.
- **Include ca-policy**: Includes information about how a CA system operates when processing a file or object received for scanning, or how scanning operates.
- **Include ma-policy**: Settings that dictate how the malware analysis configuration handles a file or object.

NOTE
The system always displays the CA backup sections when a CA device is in the job. However, if the device is running a release earlier than CA 3.2.x, ignore the CA backup sections. The system does not process those sections unless the device is running CA 3.2.x or later.

Concurrent Execution of Scripts

When creating or editing a script (**Configuration** > **Scripts** > **Add** > **Add Script**), you can now specify whether to allow the concurrent execution of that script on a device. For example, if the script takes a long time to execute and is still running on *`Device A`*, clicking **Allow Concurrent Execution** allows the script to run again on *`Device A`*, even though the prior execution is still running.

Refer to Create and Distribute Configurations Using Scripts for more information.

Device Filtering for Summary Report

Management Center 3.3 includes a new device filter in Summary Reports. The **Filter Devices** option is only applicable for report sections that do not require a Reporter database. Create Summary Reports in the following ways:

- Select **Reports** > **Reporter** > **New Report** > **Summary Report**.
- Select **Jobs > Add > New Job**. On the **Add New Job** page, select **Summary Report**.

Refer to Run a Summary Report for more information.

Log Naming Enhancements

To make it easier to identify logs, Management Center 3.3 includes improved log naming:

- Active logs now include the appliance serial number: *`logname_appliance_name_date`*.log
  For example: `audit_1000000000_2022-01-28.log`
- Rotated logs are now formatted as follows: *`logname_appliance_name_date_log_rotated`*.zip
  For example: `audit_1000000000_2022-01-28_1.zip`

These changes apply to the following logs: audit, network, device, debug, log, security, and the ProxySG, Integrated Secure Gateway, and Content Analysis device logs.

Refer to Preview, Download, and Delete Logs for more information.

Appstat Collector Improvements

Management Center 3.3 introduces the following appstat collector improvements that improve system performance:

- Upgraded to newer version of `Postgresql` . Partitioning of tables is now supported.
- Partitioned hour/day tables to improve purging and querying. The system partitions the hour tables every day, and partitions the day tables every week.
- Changes to the API endpoint—created a service to immediately process the data.
- Changes to support the migration of 3.x databases to the new version.
- Changes to the statistics-monitoring command to show the archived count of unprocessed data.

Optimizations to the Storage of PDM (Performance Data Management) Statistics

To prevent the potential loss of data during a failover and restart, PDM data is now stored on disk instead of in memory. To avoid slowing down the failover process, the PDM data (such as customer ID, source IP, time) is queued on disk until the failover completes the initial sync. Further storage optimizations have been made through database table partitioning in order to reduce the impact of statistics collection on overall performance.

Management Center 3.2.1.1

Release Information

- Release Date: August 09, 2021
- Build Number: 265101
- Document Revision: 2.0

Compatible With

See Third-Party Compatibility and Cross Product Support for information.

Deploying Management Center on Virtual Appliances

You can deploy Management Center virtual appliances on the following platforms:

- VMware® ESX Server 5.5, 6.5, and 6.7
- KVM 1.5.3 on CentOS 7.3
- Xen Hypervisor in Amazon Web Services (AWS)

  NOTE
  Use only `aws.bcsi` images to install or upgrade Management Center on AWS.
- Microsoft® Hyper-V Hypervisor

Refer to the following documents for deployment information:

- *Management Center VA Initial Configuration Guide*

Supported Upgrade Paths

Management Center 3.2.1.1 supports the following upgrade paths:

- 3.1.x to 3.2.1.1
- 3.0.x to 3.2.1.1

Important Changes in 3.2.1.1

Content Analysis Admin Console Support

This release includes support for the Content Analysis Admin Console.

Zero Touch Provisioning Support

This release enables you to create Zero Touch Provisioning policy objects

For more information about these new features, see New Features in Management Center 3.2.1.1.

Important Notes

Potential IP Mismatch on Default Certificate

Due to bug MC-2899, when the IP address of your Management Center (MC) appliance changes (either manually or during initial configuration), the system does not update the default certificate with the new IP address. Because the default certificate is not properly updated, any features that rely on that certificate for communication attempt to communicate to MC using an incorrect IP address.

The issue *always* occurs during initial configuration because DHCP assigns a default address when the user invokes the initial configuration wizard.

Most MC functions and operations are not impacted by this issue. In fact, you might not notice the issue until you send PDM (statistics) data from a monitored device to MC.

WORKAROUND:

1. Enter the following command and record the certificate subject distinguished name:
   ```
   # ssl view keyring default
   ```
2. Regenerate the certificate, inserting the subject data you collected in step 1:
   ```
   #  ssl regenerate certificate default subject "insert subject" force
   ```
3. Restart MC after regenerating the default certificate. The restart is required to clear the cached copy of the old certificate:
   ```
   # restart
   ```

SSL regenerate certificate example:

```
# ssl regenerate certificate default subject "C=US,ST=CA,L=Los Angeles,O=Example,OU=0000000000,CN=203.0.113.5"
 force
```

> **NOTE**
> For more information on the ssl command, refer to ssl.

PDM Data Collection

If you are using PDM data collection, specify a hostname in the Device Communications option (**Administration > Settings > Device Communications**). If no hostname is specified, PDM data collection may fail.

Web VPM Usage with SGOS Devices

Advanced Secure Gateway (ASG) version 6.7.4.2, ProxySG version 6.7.4.2, and Reverse Proxy (RP) version 6.7.4.2 have been removed from general availability on the customer download site but is available upon request in Limited Availability (LA). SGOS Release 6.7.4.2 contained an issue in the Web Visual Policy Manager (web VPM) that could result in changes to the installed policy with no warning displayed.

The new web VPM should NOT be used in ASG/SG/RP 6.7.4.2. If it has already been used, Symantec recommends that proxy administrators verify their existing policy and then download ASG/SG/RP version 6.7.4.3 which contains a fix for this issue.

For more details, refer to: https://support.symantec.com/en_US/article.TECH253006.html

Refer to Federal Information Processing Standards (FIPS) Mode for more information.

New Features and Feature Enhancements

- This release of Management Center introduces numerous new features and enhancements to existing features. See New Features in Management Center 3.2.1.1.

Limitations

- See Limitations.

Known Issues and Fixes

- See Management Center Known Issues and Fixes for a list of known issues and fixes that Symantec is aware of for Management Center.
- In rare instances, the web User Interface (UI) does not load immediately following an upgrade to this release. The upgrade process takes longer to upgrade the system database than the core system, and that can lead to the system not being ready following the OS upgrade. Symantec recommends that if you experience this issue, to wait an additional 5 minutes following the system upgrade before attempting to access the web user interface. If the service does not come up after 5 minutes, restart the management center service from the CLI. From the CLI privileged mode, type `system-services stop management-center` and then `system-services start management-center`.

Security Announcements

This release does not resolve any vulnerability issues:

Privacy Statement

This Product collects certain information, including personal data, in system logs regarding administrators who log in to configure the appliance. For support purposes, this information is uploaded to Symantec using a secure connection through a periodic “heartbeat." Customers can optionally upload additional data to Symantec using the “sosreport” feature to help Customer Support debug issues they are having. The personal data contained in “heartbeat” or “sosreport” includes user name and IP address of client machines.

New Features in Management Center 3.2.1.1

3.2.1.1 Includes the following new features:

- Zero Touch Provisioning Support
- Support for Content Analysis Admin Console
- Statistics Monitoring Support for Content Analysis
- Device Admin Console Audit Logging
- Activate Extra Disk Space on Existing Management Center Virtual Appliance (VA)
- Additional Host Key Validation Support
- Okta Authentication Support
- Retrieve Blue Coat ProxySG/ASG Policy Coverage Data
- Analyze ProxySG/ASG Policy Hit Counts
- View Formatted Policy Trace Report
- SSL Visibility (SSLV) License Management Support
- Role Support for Web-Based VPM Editor
- Configure a Device to Trust Management Center
- View Device Certificate Data for All Devices
- Enable Device Certificate Expiration Alerts
- New Policy Permission Specific Property Filter
- Backup Management Center Using the UI
- Device Type Detection for System Image Files
- Ability to Delete Logs
- Management Center Health Widget
- Management Center Failover Enhancements
- Management Center CLI Enhancements
- Management Center API Enhancements
- Documentation Enhancements

Zero Touch Provisioning Support

Management Center 3.2 enables you to create Zero Touch Provisioning policy objects. A Zero Touch Provisioning (ZTP) policy object enables you to create templates for quickly deploying virtual machines on Integrated Secure Gateway (ISG) devices.

Using the Zero Touch Provisioning feature, you can:

- Create and modify Zero Touch Provisioning (ZTP) files
- Preview Zero Touch Provisioning Policy (ZTP) files
- Import Zero Touch Provisioning (ZTP) files
- Export Zero Touch Provisioning (ZTP) files
- Install Zero Touch Provisioning (ZTP) files

You can also view and manage the ZTP packages installed on managed ISG devices.

For more information, refer to Create a Zero Touch Provisioning (ZTP) Policy Object.

Content Analysis Admin Console Support

Management Center 3.2 includes support for the Content Analysis Admin Console. To use the Admin Console, you must obtain the CA Admin Console package from the Broadcom download site. Then, upload the package to Management Center (**Administration** > **Packages**).

Ensure that you meet the following Content Analysis Admin Console requirements:

- The Content Analysis Admin Console is only available on appliances running CA 3.2.x or later.
- Management Center must be running 3.2.x or later.
- To use an Admin Console, you must first download the installation package from the product download area on the Broadcom support site. The packages are signed to ensure their integrity. Management Center validates the package signature when you install the package. See Add Packages to Management Center for more information.
- To log in 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 for more information.

For more information, refer to About Admin Consoles.

Statistics Monitoring Support for Content Analysis

You can now enable statistics monitoring for Content Analysis devices and extract monitoring data for use in statistics monitoring reports.

Device Admin Console Audit Logging

You can now enable audit logging for device administration console activity. When logging, the system records only the user's actions during the admin console session, not the device replies. To hide sensitive information in the log, Management Center masks passwords and other secrets. You can specify more REGEX expressions to mask other information as needed (one per line).

Device admin console audit logging is disabled by default.

1. Select **Administration** > **Settings** > **Console Audit**.
2. Optional: Enter a REGEX to mask information in the log. Enter a REGEX expression to match, followed by a tab and the replacement text. You can add multiple REGEX statements—one per line.

   ```
   password ([^" ]+|[""]+|([^"]|"")*")+   password *******
   ```

   In the preceding example, the white space between `+` and `password` is a tab character.
3. Click **Save**, then **Activate**.
4. After one or more users access the admin console, you can view the log. The admin console audit log is not viewable until a user accesses the admin console.
5. To view the log, go to **Administration** > **Logs**. Each device admin console has a separate log. The log name is in the following format:

   `ac_`*`deviceIP`*`.log`

   For example: `ac_198.51.100.17.log`
6. Select the log and click **Preview** (or download the log) to view the contents of the log.

   The admin console audit logs can be up to 10MB. You can have up to four rollover logs (50MB per device). The log data is also exported to the `syslog` .

For more information, refer to Enable Device Admin Console Audit Logging.

Activate Extra Disk Space on Existing Management Center Virtual Appliance (VA)

In earlier releases, if you increased the disk space on an existing MC VA, you had to restore defaults on the appliance to activate the new storage. In Management Center 3.2.x and later, use the `storage` command to activate the new configuration without restoring defaults.

> **NOTE**
> The `storage` command is used to activate new disk space only. If you intend to decrease the disk size, you must take a backup, export the backup to another device, shut down the VA, configure the VA disk space, power on the VA and restore defaults, re-configure the appliance, and restore the backup.

1. Access the Management Center CLI and shutdown the Management Center VA using the `# shutdown` privileged mode command.
2. Adjust your hardware requirements to better match your VA configuration.
3. Power on the VA.
4. Use the `storage` command to review and activate newly available disk space.

For more information, refer to Activate Extra Disk Space on Existing Management Center Virtual Appliance (VA).

Additional Host Key Validation Support

Management Center 3.2 introduces host key validation support for the following appliances:

- Content Analysis
- Reporter
- SSL Visibility

Host key validation is a feature of the SSH protocol. Host key validation is designed to prevent devices from impersonating legitimate servers in an attempt to steal credentials and data (man-in-the-middle attack). To prevent such attacks, each device has a unique host key that can be used to establish the identity of the host.

For more information, refer to Add a Device.

Okta Authentication Support

Use this procedure to enable Okta authentication. Before starting this procedure, gather the following information from your Okta administrator:

- The Okta domain for this authentication instance.
- The Okta API key. The Okta administrator provides you with this API key. Management Center requires only a read-only Okta API key.

1. Go to **Administration > Settings > Okta**.
2. Enable Okta authentication by selecting **Is the Authenticator Enabled?**
3. Enter the **Okta Domain**, as supplied by your Okta administrator.
4. Enter the **Okta API Key**, as supplied by your Okta administrator.
5. **Test** the connection.
   You can test the domain or individual users.
6. Configure the **General Settings**.
   Use these settings to sync role and group membership settings. When a user uses Okta to authenticate, Okta creates a user account. However, users cannot perform tasks in Management Center unless their accounts are associated with the Management Center roles and group memberships.

- **Sync the Role Membership**: Sync the Okta role with the user's roles on Management Center.
- **Sync the Group Membership**: Sync the Okta group with the user's groups on Management Center.
- **User Must Have Permission**: If you select this option, the user must be associated to an existing group or role within Management Center to gain access. If you do not select this option, an authenticated user is granted basic read-only access to Management Center.
- **Role Attribute**: Okta uses the attribute that is entered in this field to identify the user's role.

For more information, refer to Use Okta Authentication.

Retrieve Blue Coat ProxySG/ASG Policy Coverage Data

The **Retrieve Policy Coverage** job enables you to collect policy hit count statistics from your managed Blue Coat ProxySG and Advanced Secure Gateway (ASG) devices. These statistics are then used to create **Policy Coverage** reports that can be used to determine the efficacy of policy.

When you run the **Retrieve Policy Coverage** job, the system saves the raw data so you can analyze it using the **Policy Coverage** report. The system processes the policy coverage data every 30 minutes. Therefore, you cannot view the resulting **Policy Coverage** report for that data until at least 30 minutes after the job has completed.Usage tips:

- Collect policy coverage data at least twice a day (at the beginning of the day and at the end of the day) to cover the full day of usage.
- Collecting hit counts more frequently than twice a day can help with ProxySG resetting hit counts on restarts
- Do not run the coverage collection job more frequently than once an hour to keep processing and reports performance reasonable

For more information, refer to Retrieve Policy Coverage Data.

Analyze ProxySG/ASG Policy Hit Counts

The new **Policy Coverage** report provides insight into the CPL policy usage for ProxySG and Advanced Secure Gateway appliances running SGOS 6.7.x and later. You can aggregate the data for one or many devices, and you can filter the data to show hit counts during a selected time frame. The data "hit counts" reflect only the number of times the policy was matched during the selected time frame. For example, if the hit count for a policy was 3 at the beginning of the start time and 9 at the end time, the policy hit count usage will be reported 6.

> **NOTE**
> Use the `policy-coverage` CLI command to manage policy coverage data retention.
>
> **NOTE**
> The ProxySG appliance resets the condition policy hit counts to zero (or some other number representing the hit count on the last policy revision) after an appliance restart. If the new hit count number is smaller than the previous number, Management Center discards the difference when presenting usage on the report.

Requirements

- To add the **Retrieve Policy Coverage** job, you must have **Device Manage** permissions.
- The **Retrieve Policy Coverage** job can only be run on ProxySG and ASG devices running SGOS 6.7.x and later.
- The ProxySG `policy coverage` command must be enabled. (The `policy coverage` command is enabled by default.)

For more information, refer to Analyze ProxySG/ASG Policy Hit Counts.

View Formatted Policy Trace Report

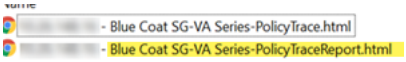
Management Center 3.2 provides the ability to download and view a report that provides a formatted view of your policy traces. To view the Policy Trace Report, you must first run a policy trace on one or more devices. Then, go to **Jobs > Archived Files** and download the policy trace to view the files.

The policy trace file is a compressed file that contains two files for each traced device:

- An unformatted dump of the policy trace.
- A formatted HTML policy trace report, as shown in the following example.

To view the Policy Trace Report, open the compressed file and double-click the file that ends with `PolicyTraceReport.html` .

For example: `198.51.100.17 - Blue Coat SG-VA Series-PolicyTraceReport.html`



You can filter the report and you can receive more detail about individual transactions.

For more information, refer to View ProxySG/ASG Policy Trace Report.

SSL Visibility (SSLV) License Management Support

You can now download SSLV licenses to Management Center (**Configuration** > **Files**) and install them on SSLV appliances. Use the **Install License** job (**Jobs** > **Add** > **New Job** > **Install License** to install the license to the SSLV appliance. You can also retrieve SSLV licenses files from the license server. **Jobs** > **Add** > **New Job** > **File Transfer**.

Role Support for Web-Based VPM Editor

Management Center 3.2.x and later include a new **VPM Policy Edit** permission. Use the **VPM Policy Edit** permission to limit the operations that a user can perform in the VPM Web Editor. For example, you can assign permissions to limit the VPM sections a user can edit, or you can limit a user to viewing only specific policy, rules, layers, or objects.

The **VPM Policy Edit** permission works in sync with the **Policy** permission. When using the **VPM Policy Edit** permission, make sure that the **VPM Policy Edit** and **Policy** permissions have equivalent settings.

On upgrade to Management Center 3.2, Management Center adds **VPM Policy Edit** permissions to match existing **Policy** permissions applied to roles.

> **NOTE**
> The permissions that you assign apply only to the VPM web editor. The permissions do not apply to the Java VPM editor.

For more information, refer to About Web VPM Policy Editor Permissions.

Configure a Device to Trust Management Center

A new feature in Management Center 3.2 enables you to configure devices to "trust" Management Center. Devices must sometimes establish certificate trust with Management Center to perform operations. For example, downloading images or uploading statistics. The **Trust MC** operation creates a job that installs the Management Center certificate onto the target devices. Each device determines where the Management Center certificate is saved and what its name should be.The **Trust MC** operation is supported for Blue Coat ProxySG (SG), Advanced Secure Gateway (ASG), and Integrated Secure Gateway (ISG) devices.

1. Select **Network** and highlight a device that you want to trust Management Center.

2. Select **Operations** > **Trust MC**.
   The system displays the Trust MC Certificate dialog.
3. Select the devices that you want to trust Management Center:
   - 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. Select **Create Job** or **Run Now**.
   The system installs the Management Center certificate on the selected devices.

For more information, refer to Configure A Device To Trust Management Center.

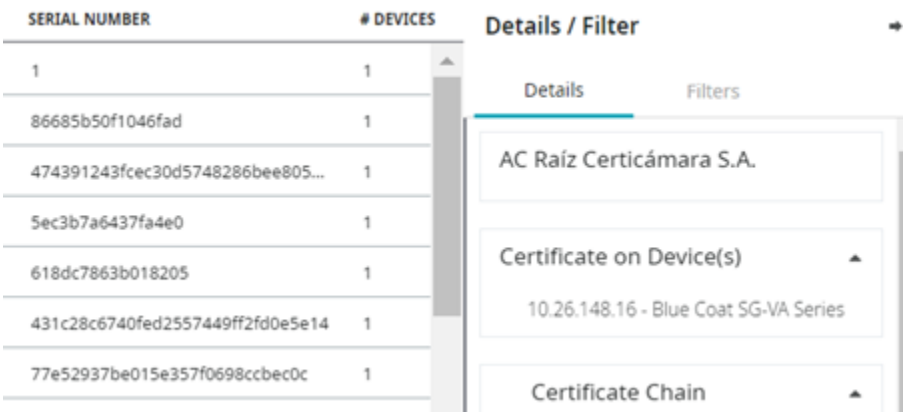
View Device Certificate Data for All Devices

You can now use the new **Configuration > Certificates** page to view all certificates that are installed on the managed devices you have collected certificates from. To view certificate data on this page, you must first run the **Collect Certificates** job on those devices. To refresh the certificate data, schedule a recurring **Collect Certificates** job to extract the certificate data regularly.

> **NOTE**
> To view the device certificates for a single device, go the Device Details page (Edit the appliance).

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

Highlight a certificate row and click the **Details** tab in the **Filter/Details** panel (on the right) to view certificate details. If necessary, expand the **Filter/Details** panel to better view the text.



Click the **Filters** tab to add filters or to refine the results.

For more information, refer to View Device Certificate Data for All Devices.

Enable Device Certificate Expiration Alerts

You can now configure Management Center to raise alerts when one or more device certificates have expired or will expire soon. Go to **Administration** > **Settings** > **Alerts** to configure the **Expiring Certificate Alert**. To receive these alerts, you must first set up a recurring **Collect Certificates** job on your managed devices.

Administrators can control the format of the messages by using the following replacement variables:

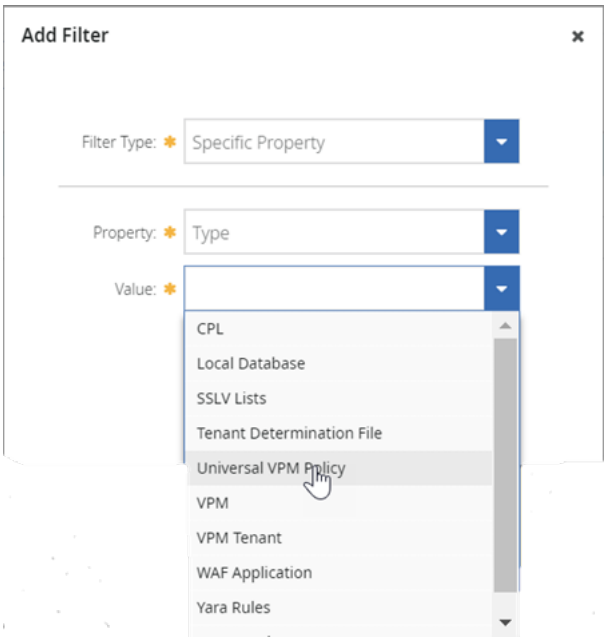
- `${subject}` - Certificate subject CN.
- `$issuer}` - Certificate CN.
- `${expiredOn}` - Certificate expiration date.
- `${issuedOn}` - Certificate issue date.
- `${deviceNames}` - Bullet list of the devices that this certificate is on.

You can also use HTML to format the email.

For more information, refer to Enable Device Certificate Expiration Alerts.

New Policy Permission Specific Property Filter

Management Center 3.2 includes a new Specific Property filter for the Policy permission. You can now restrict users to a specific type of policy, as shown in the following example.



Backup Management Center Using the UI

You can now use the new **Administration** > **Backup Management** page to immediately back up Management Center. (Previously, you could only use the CLI to backup Management Center immediately.) The options on the **Backup Management** page also allow you to:

- Take an immediate Management Center backup.
- Upload backups.
- Download backups.
- Delete backups.
- Restore backups.

The following operation creates a **Backup Management** Center job that executes immediately.

1. Go to **Administration > Backup Management**.
2. Click **Take Backup**
   The system displays the Backup Management Center window.
3. (Optional) Select the **Exclude Statistics Monitoring Trend Data** check box to exclude device reporting statistics. By excluding these statistics, the backup is substantially smaller (perhaps by hundreds of gigabytes). Keep in mind, however, that the restored backup does not have any statistics data.
4. **Email**:
   – (Optional)—Click **Email results** and select the condition. Then, enter the email address of one or more recipients.
5. Click **Create**.

For more information, refer to Manage Management Center Backups.

Device Type Detection for System Image Files

When you upload a system image (.bcsi) using **Configuration** > **Files**, the system now automatically detects the device type.

Ability to Delete Logs

Management Center 3.2.x enables users to delete logs if they have the correct permissions. A new Logs permission has been added to **Roles**. The following list describes the new permissions:

- **Logs - All Operations**
- **Logs - View**
- **Logs - Delete**

Upon upgrade to 3.2.x, the system automatically assigns **Logs - View** to users who have the **Settings - Update** permission. You must explicitly assign the **Logs - Delete** permission to enable that functionality.

To delete a log, select the log and click **Delete**. Some logs cannot be deleted. If a log cannot be deleted, the **Delete** button is disabled.

Management Center Health Widget

Management Center 3.2.x includes a new widget for monitoring MC health. The new **Management Center Health** widget includes the following data:

- CPU
- Physical Memory Total
- Physical Memory Used
- Active User Sessions
- Disk Space Total
- Used Disk Space Total

Go to **Dashboard > Home > Add Widget** to add the widget.

Management Center Failover Enhancements

Management Center 3.2.x introduces the following failover enhancements:

- Statistics monitoring historical data is replicated as a separate stream, improving health stability throughout replication. The separate stream also allows for failover to occur:
  - After initial core data and configuration is synced.
  - Before historical statistics monitoring data sync is complete.
- Management Center now issues a warning when:
  - Replication for non-essential historical data has errors.
  - The Primary partner is using 50% to 100% of allowed disk space for replication lag.

Management Center CLI Enhancements

Management Center 3.2.x introduces the following CLI enhancements:

- The `installed-systems view` command now displays the boot status:

  - `Unknown` (not booted yet)
  - `Last boot succeeded`
  - `Last boot failed`
- New `storage` command for activating extra storage on Management Center.
- The ABRCA root CA certificate now attempts to auto-renew.
- Improved the automatic trust package update process.
- The `licensing auto-update` command now works for licenses with multiple license IDs.
- License suspension warning added to `health-monitoring view` output.
- The `HOST-RESOURCES-MIB` now provides access to physical memory, data, encrypted-data, and swap space:
  - `hrStorageIndex`
  - `hrStorageDescr`
  - `hrStorageAllocationUnits`
  - `hrStorageSize`
  - `hrStorageUsed`
  - `hrSystemNumUsers`
- SCP is now supported for image installation: `installed-systems load  scp://<host>:<port>/<path>`
- Removed support for the following ciphers in SSL contexts:
  - DES and RC4 cipher suites
  - SSLv3
- Added support for the following ciphers in SSL contexts:
  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - DHE-RSA-AES256-GCM-SHA384
  - DHE-RSA-AES128-GCM-SHA256
  - DHE-RSA-AES256-SHA256
  - DHE-RSA-AES128-SHA256
  - AES256-GCM-SHA384
  - AES128-GCM-SHA256
- The `#show ssl ca-certificate` command has been modified to list all certificates:
  ```
  #show ssl ca-certificate ?
  ```
- Improved the error report when the SOS report fails to upload.

Management Center API Enhancements

Management Center 3.2.x includes the following API enhancements:

- REST API for changing the standard and enable password for the Admin account.
  You can change the enable password by specifying `ENABLE_PASSWORD` as the type.

  > **NOTE**
  > The `currentPassword` is always the Admin account password, even if you are changing the enable password.
- REST API for managing Management Center system images: `/system/images`
- REST API for managing the folder structures used to organize scripts, folders, and so on. You can also manage the entities in those folders: `/folders`
- New `system/restart` API to restart the system. You can specify a delay in restart between 0 and 60 seconds. The default is 5 seconds.
- REST API to move device groups. Example:
  ```
  PUT /groups/{uuid}/move?toGroup={toGroupUUID}
  ```

In the preceding example, the variables are explained as follows:

- `uuid` is the group to move.
- `toGroupUUID` is the folder to move the group to.

> **NOTE**
> A group may not be moved to root. Root groups may not be moved. A group may not be moved to another group in a different hierarchy.

- Enhancement: You can now retrieve a complete list of the content type values for creating policy.
  - `GET /api/policies/types` : Returns a complete list of valid content types supported
  - `GET /api/policies/types/{type}` : Returns an outline of the content (JSON) used in the POST `/api/polices/{uuid}/content` call.
- `GET /api/system/usage` returns the Management Center heartbeat data as JSON.
- The documentation for `GET /devices` now explains filters.

For more information, refer to the API help: `https://MC_IP:8082/help/api`

Documentation Enhancements

The following documentation enhancements are included in Management Center 3.2:

- Added documentation describing how the system treats special characters in CLI text input fields.
- Edited and cleaned up the API help documentation.

Management Center 3.1.3.1 (ABRCA Root CA Update Patch)

Release Information

- Release Date: 3/18/21
- Build Number: 260572
- Document Revision: 1.0

Compatible With

See Third-Party Compatibility and Cross Product Support for information.

Deploying Management Center on Virtual Appliances

You can deploy Management Center virtual appliances on the following platforms:

- VMware® ESX Server 5.5, 6.5, and 6.7
- KVM 1.5.3 on CentOS 7.3
- Xen Hypervisor in Amazon Web Services (AWS)

  NOTE
  Use only `aws.bcsi` images to install or upgrade Management Center on AWS.
- Microsoft® Hyper-V Hypervisor

Refer to the following documents for deployment information:

- *Management Center VA Initial Configuration Guide*

Supported Upgrade Paths

Management Center 3.1.3.1 supports the following upgrade paths:

- 3.1.1.1 to 3.1.3.1
- 3.0.x to 3.1.3.1

Important Notes

Updated ABRCA Root CA Certificate

This release updates the ABRCA root CA certificate. The Appliance Birth Registration Certificate Authority (ABRCA) root CA certificate is the ultimate root of trust for all appliance certificates that Symantec products use. The new certificate has an expiration date of Dec 31 00:04:16 2037 GMT.

PDM Data Collection

If you are using PDM data collection, specify a hostname in the Device Communications option (**Administration > Settings > Device Communications**). If no hostname is specified, PDM data collection may fail.

Web VPM Usage with SGOS Devices

Advanced Secure Gateway (ASG) version 6.7.4.2, ProxySG version 6.7.4.2, and Reverse Proxy (RP) version 6.7.4.2 have been removed from general availability on the customer download site but is available upon request in Limited Availability (LA). SGOS Release 6.7.4.2 contained an issue in the Web Visual Policy Manager (web VPM) that could result in changes to the installed policy with no warning displayed.

The new web VPM should NOT be used in ASG/SG/RP 6.7.4.2. If it has already been used, Symantec recommends that proxy administrators verify their existing policy and then download ASG/SG/RP version 6.7.4.3 which contains a fix for this issue.

For more details, refer to: https://support.symantec.com/en_US/article.TECH253006.html

Refer to Federal Information Processing Standards (FIPS) Mode for more information.

New Features and Feature Enhancements

- This release updates the ABRCA root CA certificate. The Appliance Birth Registration Certificate Authority (ABRCA) root CA certificate is the ultimate root of trust for all appliance certificates that Symantec products use. The new certificate has an expiration date of Dec 31 00:04:16 2037 GMT. For more information, refer to the following article: https://knowledge.broadcom.com/external/article/207144

Limitations

- See Limitations.

Known Issues and Fixes

- See Management Center Known Issues and Fixes for a list of known issues and fixes that Symantec is aware of for Management Center.
- In rare instances, the web User Interface (UI) does not load immediately following an upgrade to this release. The upgrade process takes longer to upgrade the system database than the core system, and that can lead to the system not being ready following the OS upgrade. Symantec recommends that if you experience this issue, to wait an additional 5 minutes following the system upgrade before attempting to access the web user interface. If the service does not come up after 5 minutes, restart the management center service from the CLI. From the CLI privileged mode, type `system-services stop management-center` and then `system-services start management-center`.

Security Announcements

This release does not resolve any vulnerability issues.

Privacy Statement

This Product collects certain information, including personal data, in system logs regarding administrators who log in to configure the appliance. For support purposes, this information is uploaded to Symantec using a secure connection through a periodic “heartbeat." Customers can optionally upload additional data to Symantec using the “sosreport” feature to help Customer Support debug issues they are having. The personal data contained in “heartbeat” or “sosreport” includes user name and IP address of client machines.

Management Center 3.1.1.1

Release Information

- Release Date: 11/23/20
- Build Number: 257356
- Document Revision: 1.0

Compatible With

See Third-Party Compatibility and Cross Product Support for information.

Deploying Management Center on Virtual Appliances

You can deploy Management Center virtual appliances on the following platforms:

- VMware® ESX Server 5.5, 6.5, and 6.7
- KVM 1.5.3 on CentOS 7.3
- Xen Hypervisor in Amazon Web Services (AWS)

  NOTE
  Use only `aws.bcsi` images to install or upgrade Management Center on AWS.
- Microsoft® Hyper-V Hypervisor

Refer to the following documents for deployment information:

- *Management Center VA Initial Configuration Guide*

Supported Upgrade Paths

Management Center 3.1.1.1 supports the following upgrade paths:

- 3.0.x to 3.1.1.1
- 2.4.x to 3.1.1.1

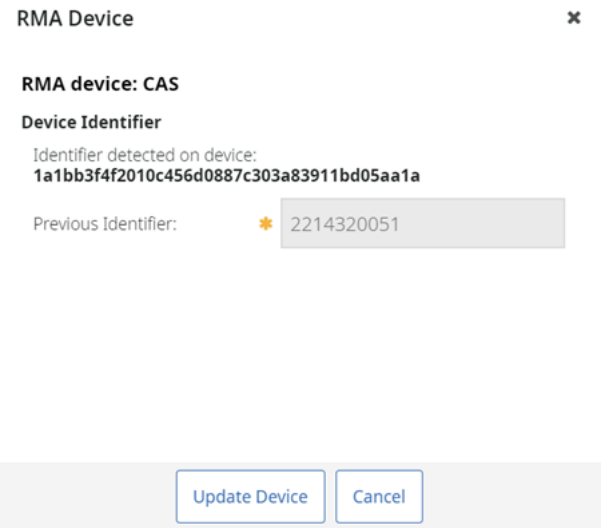
Important Changes in 3.1.1.1

Appliance ID Support

Content Analysis (CA) devices now support providing the appliance ID to Management Center. If Management Center previously used the device serial number to register the CA device, it issues the following warning noting that the device identifier has changed:

```
The internal device ID has unexpectedly changed
```

The message is informational only and does not indicate any behavior change. To clear this message, use the **RMA Device** operation feature located on the **Operations** menu. Go to the **Network** tab and select **Operations > RMA Device**.



Provide the required information and click **Update Device** to save the changes. For more information, refer to RMA a Device.

splunkforwarder Command Removed

The `splunkforwarder` command has been deleted from Management Center 3.1.1.1.

Downgrades From 3x to 2x are not Supported

You cannot downgrade from Management Center 3.x. For example, if you attempt to downgrade a full version (3x to 2x, 2x to 1x, and 3x to 1x.), the downgrade fails.

Reporter and Integrated Secure Gateway Admin Console Support

Management Center 3.1 includes support for the Reporter and Integrated Secure Gateway (ISG) Admin Consoles. You can also use Management Center to install ISG application images and complete application initial configuration. For more information, see New Features in Management Center 3.1.1.1.

Important Notes

PDM Data Collection

If you are using PDM data collection, specify a hostname in the Device Communications option (**Administration > Settings > Device Communications**). If no hostname is specified, PDM data collection may fail.

Web VPM Usage with SGOS Devices

Advanced Secure Gateway (ASG) version 6.7.4.2, ProxySG version 6.7.4.2, and Reverse Proxy (RP) version 6.7.4.2 have been removed from general availability on the customer download site but is available upon request in Limited Availability (LA). SGOS Release 6.7.4.2 contained an issue in the Web Visual Policy Manager (web VPM) that could result in changes to the installed policy with no warning displayed.

The new web VPM should NOT be used in ASG/SG/RP 6.7.4.2. If it has already been used, Symantec recommends that proxy administrators verify their existing policy and then download ASG/SG/RP version 6.7.4.3 which contains a fix for this issue.

For more details, refer to: https://support.symantec.com/en_US/article.TECH253006.html

Refer to Federal Information Processing Standards (FIPS) Mode for more information.

New Features and Feature Enhancements

- This release of Management Center introduces numerous new features and enhancements to existing features. See New Features in Management Center 3.1.1.1.

Limitations

- See Limitations.

Known Issues and Fixes

- See Management Center Known Issues and Fixes for a list of known issues and fixes that Symantec is aware of for Management Center.
- In rare instances, the web User Interface (UI) does not load immediately following an upgrade to this release. The upgrade process takes longer to upgrade the system database than the core system, and that can lead to the system not being ready following the OS upgrade. Symantec recommends that if you experience this issue, to wait an additional 5 minutes following the system upgrade before attempting to access the web user interface. If the service does not come up after 5 minutes, restart the management center service from the CLI. From the CLI privileged mode, type `system-services stop management-center` and then `system-services start management-center`.

Security Announcements

This release resolves the following vulnerability issues:

- SYMSA1469
- SYMSA1756

Documentation Errata

Inaccurate Sizing Guidelines in Online Help

A late change was introduced to increase the recommendations for CPU and RAM for VA support of 500+ devices. The change is not reflected in the help called from the appliance. The correct values are shown in the following paragraph.

To support between 501 and 1000 devices, configure the Management Center VA with the following:

- CPU: 16 Cores
- RAM: 64 GB
- Disk 1: 4 GB
- Disk 2: 1000 GB

Management Center Failover Documentation Error

The following paragraph in the online help topic *Configure Management Center Failover* contains an error:

"Determine whether to use a virtual IP address in your manual or automatic failover configuration. If you want to use a virtual IP address, obtain an unused IP address within the primary subnet of the failover partner. Use the virtual-ip command to create a virtual IP address on the primary failover partner. **Then, assign that same virtual IP address as the primary IP address of the secondary failover partner.**"

Do not assign the same virtual IP address as the primary IP address of the secondary failover partner. That is incorrect. The online documentation has been updated to correct the issue.

Reporter Report Job Permissions

Reporter report jobs require that the user has permission to view the Reporter device. If the user does not have **View** permissions for the Reporter device, the **Run Now** job fails. The online help does not indicate this.

Documentation Formatting Errors

Some of the Symantec documentation on techdocs.broadcom.com includes formatting errors in user interface paths. For example:

"This topic describes options on the **AdministrationSettings Usage Data** page."

The preceding example should display as:

"This topic describes options on the **Administration > Settings > Usage Data** page."

The issue is due to a back-end transformation error that is scheduled to be fixed in the coming weeks.

Privacy Statement

This Product collects certain information, including personal data, in system logs regarding administrators who log in to configure the appliance. For support purposes, this information is uploaded to Symantec using a secure connection through a periodic “heartbeat." Customers can optionally upload additional data to Symantec using the “sosreport” feature to help Customer Support debug issues they are having. The personal data contained in “heartbeat” or “sosreport” includes user name and IP address of client machines.

New Features in Management Center 3.1.1.1

Management Center 3.1.1.1 introduces the following new features:

- Support for Reporter and Integrated Secure Gateway (ISG) Admin Consoles
- ISG Application Support
- Open ProxySG Web-Based VPM from Software Package
- Appliance ID Support
- Support for Reporting Content Analysis (CA) Capabilities
- Device License Management
- Manage MC System Image
- Blue Coat ProxySG Appliance Policy Trace
- Execute Packet Capture (PCAP) from Management Center
- Authentication Connection and User Testing
- Content Analysis YARA Policy Object
- Show CPU Command
- SMTP Secure Email Alert Settings
- API Enhancements

Support for Reporter and Integrated Secure Gateway (ISG) Admin Consoles

Management Center 3.1 supports the new Reporter and ISG admin consoles. The consoles are designed to help you manage and monitor your appliances more efficiently. The consoles are delivered as a software package on the Reporter or ISG download area of the Broadcom Support site.

This early release of the admin consoles is a preview of the new design and functionality. As such does not include all areas of a product's user interface. Some features can't be configured in the admin console; you must use the user interface or the CLI to complete some tasks.

ISG admin console requirements:

- The ISG admin console is only available on ISG 2.2.1.1 and later.
- Management Center must be running 3.1.1.1 or later.

Reporter admin console requirements:

- Reporter 10.6.1.1 and later
- Management Center version 3.1.1.1 and later

> **NOTE**
> Users require appropriate read/write permissions to view and work in Management Center. For information on role-based administration in Management Center, and to download the Admin Console installation package, refer to the Management Center documentation.

For more information, refer to About Admin Consoles.

ISG Application Support

You can now create a Management Center job to install ISG application images to Integrated Secure Gateway appliances running ISG 2.1.x or later. (You must first upload the image to Management Center.)

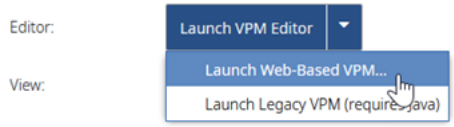
After installing an ISG image, you can then use Management Center to perform initial configuration on the ISG applications (**Network >** *`edit device`* **> Applications**). When initial configuration is complete, use the network and password information to add the application as a managed device on Management Center.

For more information, refer to Install Integrated Secure Gateway (ISG) Application Image and Perform Initial Configuration on ISG Applications.

Open ProxySG Web-Based VPM from Software Package

You now have the choice of opening the ProxySG web-based VPM from a reference device, or from a VPM software package that is uploaded to Management Center. To use the package, you must download the VPM package from the ProxySG (SGOS) download site.

To open the web-based VPM, edit the desired VPM policy and select **Launch VPM Editor**.



For more information, refer to Launch Web-Based VPM.

Appliance ID Support

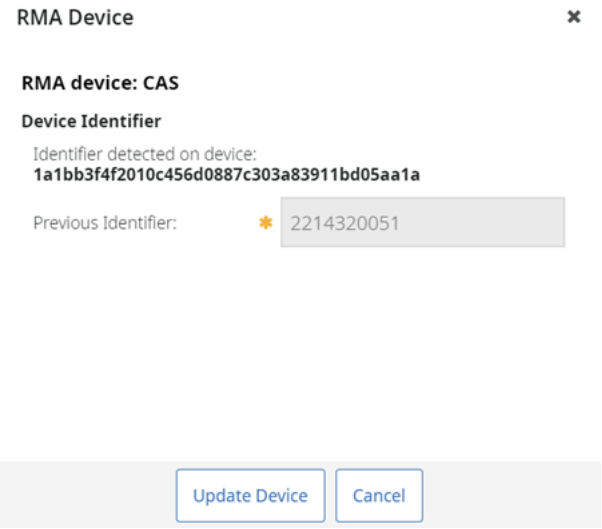
Management Center 3.1 displays the appliance ID for the following devices:

- Blue Coat ProxySG appliance
- Advanced Secure Gateway (ASG)
- Integrated Secure Gateway (ISG)
- Content Analysis (CA)

If Management Center previously used the device serial number to register the device, it issues a warning noting that the device identifier has changed:

```
The internal device ID has unexpectedly changed
```

The message is informational only and does not indicate any behavior change. To clear this message, use the **RMA Device** operation feature located on the **Operations** menu. Go to the **Network** tab and select **Operations > RMA Device**.



Provide the required information and click **Update Device** to save the changes. For more information, refer to RMA a Device.

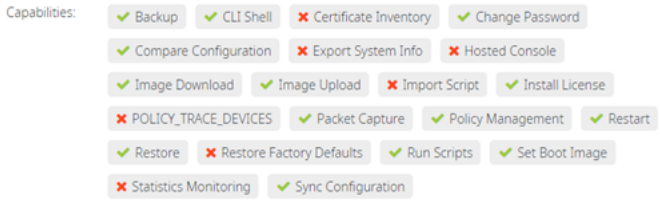
To view the appliance ID, go to the **Settings** tab in the device details page (**Network** > edit device) or use the CLI `show` command. You can also retrieve the appliance ID using the Devices REST API.

For more information, refer to View and Edit Device Information.

Support for Reporting Content Analysis (CA) Capabilities

Content Analysis devices now report their capabilities to Management Center. These capabilities are reported in the **Settings** tab in the device details page (**Network** > **Edit** > *`device`*).

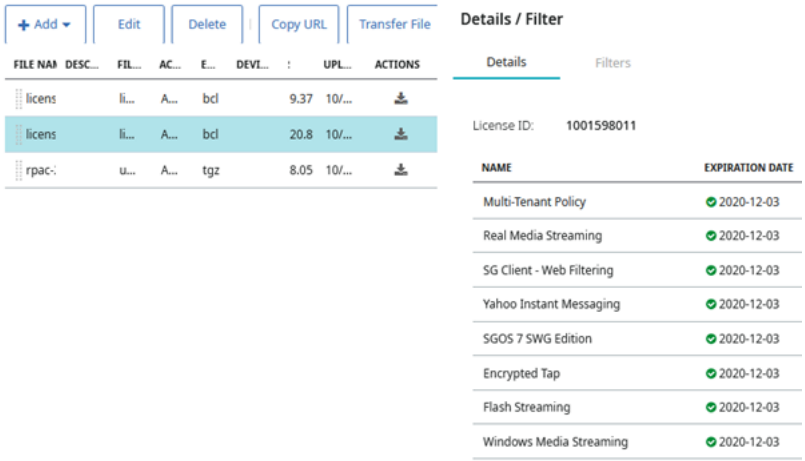
Content Analysis devices that are installed as ISG applications do not support certain features that are available in standard CA devices. The unsupported features contain a red X, as shown in the following image (ProxySG example).



Device License Management

You can now manage your device licenses directly from Management Center. The license management features include the ability to:

- The **File Transfer** job has been modified to allow you to retrieve device licenses from the Broadcom licensing server. To view the downloaded file, go to **Configuration > Files**. To view license details, select the row with the license.



- Use the **Install License** job to install device licenses on your managed devices.
  This job requires that the license is available in the Management Center file store. The Install License job is supported only for Blue Coat ProxySG appliances, Integrated Secure Gateways, and Content Analysis devices.
- View device license information in the following places:
  - **Network > Licensing** tab
  - **Network > *`edit_devicename`* > License tab**

For more information, refer to Retrieve License File from Broadcom License Server.

Manage MC System Image

Management Center 3.1 includes a new **Image Management** user interface. This interface enables you to make system images default, lock, and delete them. You can also add system images to Management Center.

1. Select **Administration > Image Management**.
2. To make an image the default, select the checkbox in the **Default** column.
3. To keep the image from being deleted when other images are added, select the checkbox in the **Locked** column.
4. To delete an image, click the "garbage can" icon in the **Action** column, then click **Yes** to confirm deletion.
5. To add an image to Management Center, click **Add Image**.
6. To reboot Management Center to load the default image, click **Reboot Default Image**, then click **Yes** to confirm the reboot.

For more information, refer to Manage MC System Images.

Blue Coat ProxySG Appliance Policy Trace

You can now run an immediate policy trace on a ProxySG appliance or schedule a policy trace using the new **Policy Trace Device** job. The policy trace options are the same as the options found on the ProxySG appliance.

CAUTION
Tracing records every policy-related event in every layer. Tracing should be used only while troubleshooting. Tracing all policy execution requires heavy CPU resources, and also generates a large trace file. Policy tracing also slows down the appliance's ability to handle traffic. Using policy tracing in production environments is unwise.

Execute policy trace:

- Run immediate policy trace: **Network > *select_device* > Operations > Policy Trace**
- Schedule policy trace: **Jobs > Add > New Job > Policy Trace Device**

For more information, refer to Run ProxySG/ASG Policy Trace.

Execute Packet Capture (PCAP) from Management Center

Management Center 3.1 includes a new operation that allows you to run a packet capture on ProxySG/ASG or CA devices.

1. Select the **Network** tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. Perform one of the following actions:
   – Select the device row. Then click the **Operations** drop-down list, and select **Packet Capture**.
   – Click the device link to edit the device. Then click the **Operations** drop-down list, and select **Packet Capture**.
   – Right click the device and select **Packet Capture**.
   The system opens the **Packet Capture** configuration dialog.
4. Take one of the following actions:
   – ProxySG/ASG: Select the direction and interface. Provide a filter if desired and click **Start Capture**.
   NOTE
   For more information on ProxySG packet capturing, refer to Packet Capturing (PCAP—the Job Utility) in the SGOS Administration Guide.
   – Content Analysis: Provide a filter if desired and set the duration. Then click **Start Capture.**
   The packet capture begins. The system displays the progress of the capture.
5. To download the packet capture, click **Download**.
6. To refresh the data in the packet capture window, click **Refresh**.
7. To stop the capture, click **Stop Capture**.

For more information, refer to Initiate Packet Capture on SG/ASG or CA Device.

Authentication Connection and User Testing

When configuring LDAP, Active Directory LDAP, or RADIUS authentication, you can now verify that your settings are correct by testing the connection.

Test LDAP and RADIUS Connection

1. Select **Administration > Settings**.
2. Click **LDAP** or **RADIUS**.
3. Configure the primary or secondary server settings and click **Test**.
4. If the shared secret field is not populated, you must enter it. The system does not make the shared secret available after it is saved. If you have entered the shared secret in the settings but have not yet saved your settings, the system auto-populates that field.
5. Click **Test**.
   The system reports a connection success or failure.

Test Active Directory LDAP Connection

Active Directory LDAP does not use a shared secret. To test the connection, enter the user name and password.

1. Select **Administration > Settings**.
2. Click **Active Directory LDAP**.
3. Configure the primary or secondary server settings and click **Test**.
4. Enter the Active Directory user name and password
5. Click **Test**.
   The systems reports connection success or failure.

Test Authentication User

To test a specific user, or to validate that you have assigned them to the correct groups or roles, complete the following steps:

1. Select **Administration > Settings**.
2. Click **LDAP**, or **RADIUS**.
3. Configure the primary or secondary server settings, and **General** and **Search** settings as appropriate.
4. Click **Test**.
5. Enter the shared secret.
6. Enter the user's user name and password.

For more information, refer to Test Management Center Authentication Connection or Users.

Content Analysis YARA Policy Object

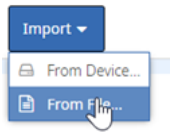
Administrators can now add YARA policy as a Management Center policy object. A YARA policy object allows administrators to manage the YARA rules on any managed Content Analysis device. This operation is only supported for Content Analysis devices running 2.1 and later.

To add a YARA Rule policy object, complete the following steps.

1. Select **Configuration > Policy**.
2. Click **Add > Add Policy**.
3. Enter a name for the policy object.
4. Select **YARA Rules** 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. Optional—Identify this policy with a **Tenant**.
7. Enter a description in the **Description** field. Although entering a description is not required, the description helps differentiate versions of the same policy.
8. Indicate whether to **Replace Substitution Variables**. See Use Substitution Variables in Policies and Scripts for more information.
9. Click **Next**.
10. Enter or select values for the defined attributes.
11. Click **Finish**.
    The system displays the empty YARA Rules policy object.
12. Edit the file to enter your YARA rule content.
13. Alternatively, click **Import** to add content to the YARA Rule policy object. You can import data from a Content Analysis device or from a local file. Accepted file extensions include `.json` ,`.yar` , and `.txt` .



.

For more information, refer to Add a Yara Rule Policy Object.

Show CPU Command

The `show` command now allows you to view CPU data.

```
# show cpu all | debug | extended
# show cpu all Current CPU usage (%): CPU 0: 9.9 CPU 1: 4.0
```

The command options can be combined.

```
 show cpu all extended
Current CPU usage (%):
1 sec 5 sec 30sec 60sec
CPU 0: 12.2 12.3 7.6 7.1
CPU 1: 5.0 10.1 5.7 4.9
```

SMTP Secure Email Alert Settings

You can now configure a secure connection for SMTP email alerts.

Port	SMTP port number
Username	SMTP username
Password	SMTP password
Protocol	SMTP protocol
SSL Context	SSL context used to communicate with SMTP gateway.

For more information, refer to smtp.

API Enhancements

The Management Center REST API includes the following enhancements:

- The hardware serial number and appliance ID are now included in the API.
- Introduction of new Devices end point, which allows you to query for devices and associated capabilities. ISG devices are now properly recognized.

Management Center 3.0.1.1

Release Information

- Release Date: 08/17/20
- Build Number: 253769
- Document Revision: 1.0

Compatible With

See Third-Party Compatibility and Cross Product Support for information.

Deploying Management Center on Virtual Appliances

You can deploy Management Center virtual appliances on the following platforms:

- VMware® ESX Server 5.5, 6.5, and 6.7
- KVM 1.5.3 on CentOS 7.3
- Xen Hypervisor in Amazon Web Services (AWS)

  NOTE
  Use only aws.bcsi images to install or upgrade Management Center on AWS.
- Microsoft® Hyper-V Hypervisor

Refer to the following documents for deployment information:

- *Management Center VA Initial Configuration Guide*

Supported Upgrade Paths

Management Center 3.0.1.1 supports the following upgrade paths:

- 2.3.x to 3.0.1.1
- 2.4.x to 3.0.1.1

Important Changes in 3.0.1.1

Downgrades From 3x to 2x are not Supported

You cannot downgrade from Management Center 3.0. For example, if you attempt to downgrade a full version (3x to 2x, 2x to 1x, and 3x to 1x.), the downgrade fails.

Integrated Secure Gateway Support

Management Center 3.0 includes support for managing Integrated Secure Gateway appliances. See New Features in Management Center 3.0.1.1.

Important Notes

PDM Data Collection

If you are using PDM data collection, specify a hostname in the Device Communications option (**Administration > Settings > Device Communications**). If no hostname is specified, PDM data collection may fail.

Web VPM Usage with SGOS Devices

Advanced Secure Gateway (ASG) version 6.7.4.2, ProxySG version 6.7.4.2, and Reverse Proxy (RP) version 6.7.4.2 have been removed from general availability on the customer download site but is available upon request in Limited Availability (LA). SGOS Release 6.7.4.2 contained an issue in the Web Visual Policy Manager (web VPM) that could result in changes to the installed policy with no warning displayed.

The new web VPM should NOT be used in ASG/SG/RP 6.7.4.2. If it has already been used, Symantec recommends that proxy administrators verify their existing policy and then download ASG/SG/RP version 6.7.4.3 which contains a fix for this issue.

For more details, refer to: https://support.symantec.com/en_US/article.TECH253006.html

Refer to Federal Information Processing Standards (FIPS) Mode for more information.

New Features and Feature Enhancements

- This release of Management Center introduces numerous new features and enhancements to existing features. See New Features in Management Center 3.0.1.1.

Limitations

- See Limitations.

Known Issues and Fixes

- See Management Center Known Issues and Fixes for a list of known issues and fixes that Symantec is aware of for Management Center.
- In rare instances, the web User Interface (UI) does not load immediately following an upgrade to this release. The upgrade process takes longer to upgrade the system database than the core system, and that can lead to the system not being ready following the OS upgrade. Symantec recommends that if you experience this issue, to wait an additional 5 minutes following the system upgrade before attempting to access the web user interface. If the service does not come up after 5 minutes, restart the management center service from the CLI. From the CLI privileged mode, type `system-services stop management-center` and then `system-services start management-center`.

Security Announcements

This release resolves the following vulnerability issues:

- SYMSA1760 - Nginx Vulnerabilities Jul 2017 - Oct 2019
- SYMSA1765 - Apache Tomcat Vulnerabilities Oct 2018 – Feb 2020
- SYMSA1492 - Linux Kernel Vulnerabilities May-June 2019
- SYMSA1467- Linux Kernel Aug 2017 - (Sep 2018 Vulnerabilities) CVE-2018-5390 and CVE-2018-5391
- SYMSA1462 (OpenSSL) - Vulnerabilities 16-Apr-2018 and 12-Jun-2018
- SYSMA1443 (SA166) - OpenSSL Vulnerabilities 27-Mar-2018
- SYMSA1423 (SA157) - OpenSSL Vulnerabilities 28-Aug-2017 and 2-Nov-2017
- SYMSA1397 (SA144) - OpenSSH Vulnerabilities January 2017.

Documentation Errata

Some of the Symantec documentation on techdocs.broadcom.com includes formatting errors in user interface paths. For example:

"This topic describes options on the **AdministrationSettings Usage Data** page."

The preceding example should display as:

"This topic describes options on the **Administration > Settings > Usage Data** page."

The issue is due to a back-end transformation error that is scheduled to be fixed in the coming weeks.

Privacy Statement

This Product collects certain information, including personal data, in system logs regarding administrators who log in to configure the appliance. For support purposes, this information is uploaded to Symantec using a secure connection through a periodic “heartbeat." Customers can optionally upload additional data to Symantec using the “sosreport” feature to help Customer Support debug issues they are having. The personal data contained in “heartbeat” or “sosreport” includes user name and IP address of client machines.

New Features in Management Center 3.0.1.1

This topic describes the features that are introduced in the Management Center 3.0 release.

Management Center 3.0 introduces the following new features:

- Obfuscate Reporter Fields
- Integrated Secure Gateway Support
- Microsoft® Hyper-V Hypervisor Support for Virtual Appliances
- Automatic Failover Support
- Virtual IP Address Support
- User Interface Usability Update
- Send Usage Data
- Use Public Key Authentication for CLI Access
- Ability to Use Certificate Revocation Lists (CRL) with SSL Mutual Authentication
- Improved Reporting for Device Certificates
- Ability to Regenerate the Management Center Public Key
- Ability to Set File Access Control
- Automatic Notification of Policy Changes
- CPL Fragments Can Now Contain Shared Objects
- VPM Diff Improvements
- Local Database Improvements
- Ability to Add Second SNMP Trap Notification Target
- SNMP Agent Support for SNMPv3
- Show Reporter CPU Status
- Ability to Take and Collect Memory Dumps for Management Center Services
- Revision Date Now Shown on the Script Grid
- Insert Local Variables in Scripts for Use with the Management Center API
- Remove Default CCLs From Scripts
- New File Store API
- API Enhancement: Access Archived files in Job History

Obfuscate Reporter Fields

When creating or editing roles, you can set permissions to obfuscate the Reporter report fields the role has access to. When you obfuscate a report field, the user can still view reports containing that field but cannot view the data in the obfuscated fields. Note the following information:

- You cannot obfuscate a field that has already been restricted.
- Obfuscation persists through sorting and paging. Obfuscation also persists through filtering except for **Full Log Detail** reports, where any deobfuscation is lost when filtering.
- Users cannot filter on any obfuscated field. Only canned filters are permitted.
- To allow a user to view the data in obfuscated fields, you must assign the **Deobfuscate** permission to one of the user's roles.
- Reporter Report jobs that are run with a role that is specified in the configuration:
  - If a user runs a job ad hoc or triggers a job with an event, that user must have the specified role or the job will fail.
  - If a Reporter report job runs as a scheduled Job, it runs using the specified role. If this role includes obfuscation relevant to the report specified in the job configuration, then the report is obfuscated.

For more information, refer to About Reporter Obfuscation.

Integrated Secure Gateway Support

Management Center 3.0 includes support for managing Integrated Secure Gateway appliances.
Support for ISG appliances includes:

- Basic metrics, for example, CPU and memory
- Image management: Download of images from Management Center; setting boot image.
- Restart
- Restore factory defaults.

  CAUTION
  Network settings are not preserved.

- Web CLI shell
- CLI scripting

  NOTE

  - Public key authentication is not supported for authenticating to ISG appliances.
  - Any applications running on the ISG can also be added to Management Center as individual devices. Those devices might not support certain features, for example, software upgrade. Refer to the appliance's **Device Details Settings** page for more information.

For more information, refer to Add a Device.

Microsoft® Hyper-V Hypervisor Support for Virtual Appliances

You can now deploy Management Center on the Hyper-V Hypervisor. For more information, refer to the *Management Center Initial Configuration Guide For Virtual Appliances, Version 3.0.1.1*.

For more information, refer to Hyper-V Hypervisor Requirements.

Automatic Failover Support

Management Center 3.0 now supports automatic failover. In this mode, failover automatically occurs after the timeout value (set during failover configuration) expires. You set the timeout value during configuration of the secondary failover partner.

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.
- 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. Failover partners should 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.

For more information, refer to About Management Center Failover.

Virtual IP Address Support

Management Center 3.0 includes support for using on a virtual IP address on one of Management Center's interfaces. Using a virtual IP address allows users and devices to access the correct Management Center appliance in all cases. A common use case is statistics monitoring, in which devices are configured with a virtual IP address to send data back to Management Center. Assigning a virtual IP address is not required for failover. However, using a virtual IP address enables the secondary failover partner to accept requests on that virtual IP-address when the primary failover partner is unresponsive.

Virtual IP address assignments are supported for on-premises and AWS deployments.

For more information, refer to virtual-ip.

User Interface Usability Update

The Management Center user interface has been updated in version 3.0. The changes include the following items:

- The look and feel of the left navigation bar has changed.
- The user interface logos, and so on, have been rebranded to reflect Broadcom corporate standards.
- The font style in the user interface has changed.
- The update includes various other minor changes to the appearance of the user interface.
- The placement of certain buttons and the filter has also changed.

The functionality of Management Center has not been impacted by these changes. The documentation has not yet been updated to reflect these changes.

Send Usage Data

Management Center 3.0 supports the option to send daily usage data to Broadcom. If you have a Portfolio License Agreement (PLA) with Broadcom, you are required to send daily usage data to Broadcom. You can do that using this option or by another means negotiated with Broadcom.

You send usage data using the options on the **Administration** > **System Settings** > **Usage Data** page.

The usage data information is securely transmitted to the Broadcom Portal. The data includes the number of devices that are being monitored. No Personally Identifiable Information (PII) covered under GDPR is transmitted. You can view the data that is sent by looking at the `usage.log`. Go to **Administration** > **Logs** to view the log.

For more information, refer to Send Usage Data to Broadcom.

Use Public Key Authentication for CLI Access

Management Center 3.0 now allows users to access the MC CLI using public key authentication.

To enable public key authentication for the SSH console, you must complete the following steps:

1. Ensure that the user has the administrator role, or a role that includes the Management Center CLI permission.
2. Generate the SSH public and private key that will be used to access Management Center.
3. Enable public key authentication.
4. Inline the user's public key.

To enable public key authentication:

```
(config)# ssh-console public-key-authentication enable
```

For more information, refer to Use Public Key Authentication for CLI Access.

Ability to Use Certificate Revocation Lists (CRL) with SSL Mutual Authentication

You can now use a Certificate Revocation List (CRL) to block users from accessing Management Center. To use this feature, you must first configure SSL Mutual Authentication for Management Center users. Then, you must add the CRL to Management Center. Finally, you must ensure that client authentication is set to mandatory:

```
(config)# security client-authentication set mandatory
```

Copy the CRL into Management Center

1. Copy your CRL.
2. Enter the following command to import the CRL into Management Center:

   ```
   (config-ssl)# inline crl crl_name
   ```

   Press `Ctrl-D` when finished Alternatively, you can specify a URL that contains your CRL data. When you enter a URL, the system periodically checks the URL to update the contents of the CRL. The refresh interval is set using the `refresh-interval` command.

Use the CRL for SSL Mutual Authentication

1. Enter the following command:

   ```
   (config)# security client-authentication crls crl_name
   ```

For more information, refer to Use Certificate Revocation Lists (CRL) with SSL Mutual Authentication.

Improved Reporting for Device Certificates

New reporting options for device certificates have been added to the **Summary Report (Jobs > Add > New Job > Summary Report.**

The following reporting categories have been added:

Certificate Status – This option lists certificates in order of expiration (expired, 30 days, 60 days).

Certificate Inventory– This option provides a full list of all certificates and the devices they are associated with. This list is helpful to use as a complete inventory of PKI. Each reporting category lists the common name of the certificate, issuer and issue date, expiration date, serial number, and the devices that are using the certificate.

API– Additionally, the Management Center API includes the following certificate-related enhancements:

- New filters for `/{uuid}/certificates` and `/certificates`
  - `keyUsageNames`
  - `fingerprint`
  - `signatureAlgorithm`
  - `selfSigned`
- New output option for `/{uuid}/certificates` and `/certificates`
- Ability to control if the output should contain a full set of certificate lists that the certificate is included in. The default is to include the list.
- A new API The `/certificates/usage` API returns a unique list of certificates. (The API uses the certificate fingerprint to determine uniqueness.) For each certificate, the API lists the devices that are using the certificate.

For more information, refer to Run a Summary Report.

Ability to Regenerate the Management Center Public Key

You can now regenerate the RSA key Management Center uses to authenticate to the ProxySG or ASG device. This key is used in the public key authentication method. In 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. Regenerate the Management Center RSA key using the device-communication CLI command.

For more information, refer to device-communication.

Ability to Set File Access Control

MC 3.0 provides a new option to control access to file downloads from the file store. Files have three types of permissions:

- **None**-This setting blocks all access to download files from /fs/download. The Copy URL setting is not available on the UI when the access is set to NONE.
- **All**-This setting allows downloading/uploading using HTTPS or HTTP without authorization. (The default setting is All.)
- **Authenticated**-This setting only allows file downloading/uploading over HTTPS. You must be authenticated to Management Center or must use your API credentials if you have generated an API token for your user ID.

For more information, refer to Set File Access Control.

Automatic Notification of Policy Changes

Management Center 3.0 now includes the ability to subscribe to an alert for a policy object that has changed. The alert is sent to an email address (or multiple email addresses) that you specify and includes:

- A diff report of the changes that includes the policy name, reference ID, previous version number, current version number, the user who modified it, the modification time, a description, and a commit comment.
- A description of the previous version
- The ability to specify the format of the diff report as HTML or PDF.

For more information, refer to Receive Notification When Policy Changes.

CPL Fragments Can Now Contain Shared Objects

You can now include shared objects in CPL fragments, not just top-level CPL files. You can include a URL list, category list, or another CPL fragment (Management Center notifies you of circular references) in a CPL fragment.

1. Select **Configuration > Shared Objects**.
2. In the **Shared Policy Objects** list, click the CPL fragment to which you want to add the shared object. The policy is displayed in the **Editor**.
3. Place the text cursor into the policy section where you want to include the shared object and select **Operations> Insert > Insert Include**. You can only place a shared object into an existing policy section. The web console displays the Select Policies dialog.
4. From the available policy fragments, select the shared object to include.
5. To commit your changes, click **Save** and enter a comment for the commit operation. The comment that you enter is saved as policy metadata.

For more information, refer to Include a Shared Policy Object in CPL or VPM Policy.

VPM Diff Improvements

Previously when a policy was saved, the diff view of the VPM changes highlighted the modification timestamp as well as any changes to rule index comments. In Management 3.0, the default view of the VPM diffs has been simplified to highlight only the actual changes that have been made. Changes to the timestamp and rule index comments have been silenced. To see a full set of comments and the timestamp for any policy changes, click on the **Generated CPL** (Verbose View) icon in the upper left corner of the window.

For more information, refer to Compare Different Versions of the Same Policy.

Local Database Improvements

Management Center 3.0 includes the following local database improvements:

- **More Permissive Processing of End Statements**
  Management Center is now more permissive when checking for end statements in local database policy. Many customers use statements like "end category." Management Center previously flagged these end statements as errors and now processes the end statement and any additional text normally.
- **Allow Category-Level Comments**
  Management Center now allows comments/descriptions at the category-level in the user interface and for import.
- **Preserve line-comments when importing Local Database from .ldb file**
  Comments above a statement are attached to the statement immediately following the comment.
- **Allow Entries to Be Disabled in Local Database**
  Management Center no longer requires users to remove entries they temporarily want to disable. If a URL is preceded by the `;` character, Management Center now interprets the statement as a disabled entry and treats it as such. For example:
  ```
  ; disabledentry.com
  ```
- **Local Database allows hosts with trailing dot**
  The ProxySG appliance allows trailing dots in hostname statements. To ensure that imported local database policy can run without errors, Management Center 3.0 now allows a trailing dot after a hostname. Previous releases of Management Center did not allow a trailing dot after a hostname and reported an error.

Ability to Add Second SNMP Trap Notification Target

Management Center 3.0 includes support for a second SNMP trap notification target. Providing a second SNMP trap notification target provides redundancy for SNMP monitoring and alerting. To add a second SNMP trap notification target, go to **Administration > Settings > SNMP Alerts**.

For more information, refer to Configure SNMP Alerts.

SNMP Agent Support for SNMPv3

In Management Center 3.0, SNMP agents can now be configured to use, SNMPv2, SNMPv3, or both. The settings on the **SNMP Agent Settings** page (**Administration** > **SNMP Agent Settings**) have been changed to reflect this change.

For more information, refer to Configure SNMP Agent Settings.

Show Reporter CPU Status

Management Center 3.0 now displays Reporter CPU usage data for Reporter appliances running Reporter 10.5.2.1 or later. View the CPU usage data in the **Network** > **Health** and **Network** > **Status** > **System Metrics**.

Ability to Take and Collect Memory Dumps for Management Center Services

The `service-action memory-dump` command now allows you to take memory dumps for the following services:

- Management Center (web UI, device management, policy management, scheduled jobs, reporting, and alerts)
- Report Generator (for offline reports)
- Statistics Monitoring

The memory dumps are saved to **Administration** > **Logs** and can be uploaded to support using the `diagnostics` command. All memory dumps are deleted whenever Management Center restarts. Deleting memory dumps on restart is done to preserve disk space.

Syntax

```
#service-action memory-dump management-center | report-generator
  | statistics-monitoring
```

For more information, refer to service-action.

Revision Date Now Shown on the Script Grid

A new field has been added to the **Script Objects** page. This column shows the date and time of most recent revision to the script.

Insert Local Variables in Scripts for Use with the Management Center API

In MC 3.0, you can use the REST API to pass local variable values into device scripts. This action is helpful when you want to change values in device scripts without editing them.

The `parameters` variable can be inserted into scripts and then modified using the Management Center API. The syntax of the `parameters` variable is:

```
parameters.property
```

The variable can be placed anywhere in the script. For example:

```
${@set-local username = $parameters.username(MY_DEFAULT)}
…
users;
logout ${@get-local username}
```

The REST API function `api/script/{uuid}/execute` is used to define the local value.

For more information, refer to Insert Local Variables in Scripts for Use with Management Center API.

Remove Default CCLs From Scripts

When you import a script, the system inserts default CA Certificate Lists (CCLs) into the script. These default certificate lists cause errors when you try to run the script again. This operation removes the following default CCLs:

- `bluecoat-appliance`
- `bluecoat-image-validation`
- `bluecoat-license`
- `bluecoat-services`

For more information, refer to Optimize a Script for Use on Other Devices.

New File Store API

A new API endpoint has been added that provides the ability to manage the contents of the file store. Using the API, you can:

- Retrieve the list of files in the store along with the associated metadata.
- Retrieve the contents of a file in the store (download the file).
- Add a new file to the file store and upload the contents.
- Replace the metadata associated with a file.
- Replace the contents of a file in the store.

API Enhancement: Access Archived files in Job History

A new set of APIs has been added to the Jobs API. The APIs allow you to access contents of job history that is stored in the job file archive. You can now:

- Retrieve the list of files in the archive.
- Retrieve the content of a file in the archive (download the file).

Management Center Known Issues and Fixes

Symantec is aware of the following issues in Management Center.

Security Issues

Issue Number	Description
MC-754	SYMSA1374 (SA128) - Multiple PCRE Vulnerabilities. Management Center includes the vulnerable library but does not have vector of attack.
MC-756	SYMSA1404 (SA148) - Linux Kernel Vulnerabilities Feb-Apr 2017.

Open Known Issues

Component	Issue #	Issue Description

Authentication	MC-2899	In some cases the Default Certificate IP may not update correctly.
		Workaround: To update the default certificate, do the following:
		1. Enter the following command and record the certificate subject distinguished name:
		`# ssl view keyring default`
		2. Regenerate the certificate, inserting the subject data you collected in step 1:
		`# ssl regenerate certificate default subject "insert subject" force`
		3. Restart MC after regenerating the default certificate. The restart is required to clear the cached copy of the old certificate:
		`# restart`

Alerts	MC-699	Management Center alert notifications still report license issue after the issue is resolved.
CLI	MC-784	You cannot download a license file if the URL contains an IPv6 address. Workaround: Use the license installation in the Management Center user interface.
CLI	MC-802	The following CLI show commands do not return results: • `show security` • `show health-monitoring` • `show notification`

Component	Issue #	Issue Description
CLI	MC-803	Diagnostics Heartbeat data does not include failure details; only **OK** and **Failed** messages are currently displayed.
Failover	MC-806	Error message in case of version-mismatch is incorrect.
Jobs	MC-807	**Export Backup** jobs fail to generate if the job name has more than 64 characters. This can occur if the job name is a duplicate of an existing job name and characters are auto appended to it.
Monitoring	MC-808	Dashboard widgets can show connection failures in certain cases involving long-running queries.
Networking	MC-3346	The Docker interface is blocking some connections to MC on the local network.
Policy	MC-2963	Certain illegal characters on URL strings are incorrectly allowed.
Policy	MC-549	Management Center does not display upload video web operation.
Reports	MC-3409	Duplicate data is included in the CSV export of the Full Log Details report.

Known Issues Now Fixed

Component	Issue #	Issue Description
Fixed in 3.3.2.1		
Policy	MC-3410	Legacy Java VPM editor is not launching.
Policy	MC-2807	Shared object version control discrepancy.
Fixed in 3.3.1.1		
Authentication	MC-2900	Unable to install certificate to the ISG appliance.
Failover	MC-2338	Management Center UI disconnects while failover shows waiting for successful subscription status.
Failover	MC-2874	Disk space on the primary partner in failover mode was consumed by the unused replication slot.
Jobs	MC-2958	The backup job timestamp did not match the system time.
Jobs	MC-2826	The jobs API did not allow users to filter by time.
Policy	MC-2470	The PCAP filter did not work for UDP traffic.

Component	Issue #	Issue Description
Security	MC-2332	SYMSA17650 Tomcat Vulnerabilities
Security	MC-2318	SYMSA17570 OpenSSL Vulnerabilities (CVE-2021-23840 and CVE-2021-23841)
Security	MC-2242	SYMSA17570 OpenSSL Vulnerabilities (CVE-2020-1968 and CVE-2020-1971)
System	MC-2792	Unexpected reboot and downgrade.
User Interface	MC-2798	Interface issues after upgrade to 3.1.x.
Fixed in 3.2.2.1		
API	MC-2742	`getCertificates` API call showed duplicate certifcates.
Jobs	MC-2741	Compare and save configuration jobs did not pull known certificates with keys from SSLV devices.
Reporting	MC-2743	Certificate inventory report did not show the subject name.
System	MC-2776	Fractional or 0 offset timezones caused a user interface error.
System	MC-2789	The user interface was sometimes inaccessible after upgrade from MC 3.1.3.1.
Fixed in 3.2.1.1		
Authentication	MC-2416	Management Center maintained old `ca-certificates abrca_root` record for managed devices.
CLI	MC-2322	`show ssl ca-certificates` did not work properly.
Failover	MC-2270	Management Center failover initial sync failure.
Failover	MC-2658	Display issue with % when there was a replication lag with the Primary failover partner.
Jobs	MC-2403	The **Save Config** and **Compare Config** jobs did not include `tcp-ip` ProxySG appliance settings.
Logs	MC-900	Eventlog/syslog lines showed duplicate date/time instead of hostname/IP address.
Logs	MC-1332	Event logs were not showing the hostname or IP address.
Monitoring	MC-1475	Statistics Monitoring data points showed a different timestamp based on the selected date filters.
Monitoring	MC-1644	Some ProxySG appliances were missing when downloading statistical reports.

Component	Issue #	Issue Description
Monitoring	MC-2226	Statistics Monitoring Report - Management Center gave an intermittent job error when generating CPU and Memory reports.
System	MC-2276	Erroneous duplicate serial number error reported soon after upgrade to 3.1.1.1.
System	MC-2286	Backup time created showed UTC with time zone.
Fixed in 3.1.4.1		
Failover	MC-2352	Disk bloat caused performance and replication issues on secondary failover node.
Failover	MC-2394	Failover now occurs once core DB completes, even if historical application statistics are still syncing.
Fixed in 3.1.3.1		
Authentication	MC-2296	Management Center failed to update ABRCA root certificate.
Authentication	MC-2335	Updated ABRCA certificate.
Failover	MC-2262	Certificate permissions caused failover to fail.
Failover	MC-2271	Failover error when syncing.
Failover	MC-2285	Improved initial sync progress status.
Fixed in 3.1.2.1		
Authentication	MC-2296	Management Center failed to update ABRCA root certificate.
CLI	MC-2150	Changing data retention policy via CLI on systems with large statistics monitoring loads can cause extended delays in responsiveness
Logs	MC-2219	Messages were not rotated in logs.
Monitoring	MC-1602	Health check statuses were inconsistent on some IP addresses.
Reporting	MC-1649	Unified reports showed incorrect timestamps in CSV export.
Policy	MC-1945	Management Center errored when the URL length exceeded 1024 characters.
Fixed in 3.1.1.2		
Failover	MC-2185	Failover failed to do initial sync.
Reporting	MC-2199	Report jobs did not recognize group role assignments.
Fixed in 3.1.1.1		

Component	Issue #	Issue Description
Authentication	MC-1321	MC 2.3.x was unable to verify the CA certificate for syslog servers using TLS. Workaround: The Syslog's SSL server certificate must be signed by Management Center's default_CA. This requires exporting the default_CA private key and certificate to openssl/syslog server. See TECH257018 - Management Center is unable to verify the CA certificate for syslog servers using TLS for more information.
Device Management	MC-2119	SG managed device showed "X" on all capabilities.
Failover	MC-2134	Primary failover incorrectly printed out "DENIED FORBIDDEN Remote Request" error.
Logging	MC-2158	Removed splunk forwarder CLI commands.
Monitoring	MC-1974	False PSU alarm status was raised.
Security	MC-763	SYMSA1469
Security	MC-1547	SYMSA1756
Statistics Monitoring	MC-1987	Statistics Monitoring Report job defaulting to average.
Fixed in 3.0.3.1		
API	MC-1999	API audit logs did not show Client IP in 'info 2' field.
Failover	MC-1973	Database sync status bar could freeze for long periods of time.
Monitoring	MC-1114	Device names did not sync with Statistic Monitoring report.
Policy	MC-2043	The Web VPM did not load application attributes in Management Center.
Policy	MC-2014	Updating policy content via API failed to release edit lock.
Fixed in 3.0.2.1		
Device Management	MC-1878	Management Center throttled concurrent connections when exporting managed device backups.
Platform	MC-1967	jQuery updated to v3.5.1.

Component	Issue #	Issue Description
Platform	MC-809	Management Center sent license server avoidance errors because it was deployed with a proxy and MC had a credential on its proxy settings. Users were not able to null the user name and password to correct the issue. **Workaround**: Null the username and password using the CLI: `# en # con t (config)# proxy-settings (config-proxy-settings)# **username** "" (config-proxy-settings)# **password** ""`
Policy	MC-1689	No warning was displayed when attempting to edit a VPM policy opened by the same user account.
Reporting	MC-1476	Report date/time field formatting was not consistent in CSV export.
Fixed in 3.0.1.1		
Authentication	MC-1195	Browser-trusted CCL reset cleared all CAs.
API	MC-1691	PUT job API returned 500 error code.
CLI	MC-1901	CLI: Non-admin users were not able to log in when CAC was set to mandatory.
Device Management	MC-1626	Management Center displayed operation timeout when attempting to add CAS.
Device Management	MC-804	Users could not enable SNMP alert when an IPv6 address was defined. Error: `Failed to save "SNMP-ALERT": Property "SNMP Destination IP or hostname" had invalid value "undefined"`
Monitoring	MC-1651	SNMP v3 traps were missing values for EngineBoots and EngineTime.
Network	MC-1149	Adding static route crashed the CLI.
Platform	MC-1298	Default Symantec NTP servers configured were not resolvable.
Scripts	MC-1702	Users with specific permissions were unable to delete script.
Security	MC-1562	SYMSA1760
Security	MC-1531	SYMSA1765
Security	MC-770	SYMSA1492
Scripts	MC-1357	Unable to send hex codes in script.
System	MC-1135	SOS diagnostics did not send in certain cases.

Component	Issue #	Issue Description
System	MC-1132	Disk filling up with PCAP dumps.

Limitations

Limitations are issues of which Symantec is aware; however, they are not fixable because of an interaction with third-party products or they work as designed but might cause an issue.

Authentication

Although, Management Center allows usernames that include a colon to be created, such usernames cannot log in to the web management or command line interfaces.

Advanced Secure Gateway (ASG)—Limited Signed Image Support

You cannot install ASG images from HTTPS servers with a certificate that is signed by private CAs or with self-signed certificates.

Install upgrade images from the Broadcom Support site, from an HTTP-based server, or from an HTTPS server with a certificate signed by a public CA.

VPM

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 must 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.

RADIUS Not Supported in FIPS Mode

RADIUS authentication is not supported when Management Center is running in FIPS modes.

Reference Information

The following sections provide reference and compatibility information for Management Center.

- Cross Product Support
- Third-Party Compatibility
- Management Center MIB Files
- Symantec Technical Support Resource
- Documentation Resource and Update Log

Cross Product Support

The following Symantec products are compatible with Management Center 3.3.1.1:

Product	Minimum Versions Required
Advanced Secure Gateway	SGOS 6.6.x
Content Analysis	1.3.x, 2.2.x
Director*	6.1.19.1 *Devices that are already managed by Director can be imported and managed by Management Center.
Malware Analysis	4.2.1
PacketShaper	PSOS 9.2.11 PS S-Series 11.2
ProxySG Appliance*	SGOS 6.2.x *SGOS 6.3.x is required for Statistics Monitoring reports and statistics collection.
Reporter	10.1.x
SSL Visibility	3.8.6, 4.x
Web Security Service	Current

Supported Platforms

Management Center 3.3.1.1 is supported on the platforms that are listed here:

- MC-S400-20
- VMware ESX 5.5, 6.5, 6.7
- KVM 1.5.3
- Xen Hypervisor AWS
- Microsoft Hyper-V Hypervisor

Third-Party Compatibility

VMware

If you are running Management Center as an ESX virtual appliance, follow these requirements to achieve satisfactory performance and operation. The virtualization environment must have, at a minimum:

- VMware ESX Server 5.5, 6.5, 6.7, and ESXi 7.0
- Dual-core processor
- 8 GB of virtual memory
- 100-GB hard disk space

- If you want to use remote serial connections, your VMware license must be Enterprise or Enterprise Plus. For more information, please refer to the VMware documentation.
- Running Management Center as a virtual appliance can be demanding for ESX server disk subsystems. Use enterprise-grade hardware RAID controllers with a dedicated write cache to satisfy IO demands.
- Because Management Center uses EFI (Extensible Firmware Interface), certain ESX hosts may require VMware tuning specific to the deployed storage type. In certain cases, you may have to reduce the ESXi parameter Disk.DiskMaxIOSize from 32 MB (32768 KB) to 4 MB (4096 KB). For example, if your VMware vSphere environment utilizes Pure Storage®, the Disk.DiskMaxIOSize must be set to 4 MB or the image fails to boot. For more information, refer to the VMware and storage vendor documentation.
- The Management Center OVF does not install correctly on vSphere 6.5. vSphere 6.5 sets the boot option to BIOS, instead of the correct setting for the Management Center OVF: EFI/UEFI. To work around this problem, take one of the following actions:
  - Deploy the OVF template with the EFI boot option using the command line: OvfTool, version 4.2.0. Refer to this page for more information: https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-esxi-vcenter-server-65-release-notes.html#vmissues.
  - Use the vSphere client to deploy the OVF, but change the Boot Options setting to EFI before starting the VM. See Management Center VM Workaround for vSphere 6.5.x for more information.

KVM

Adhere to the following requirements.

- KVM Version: KVM 1.5.3
- OS Support: The operating system must be running kernel version 3.10 or later. Refer to the CentOS documentation as needed:
  CentOS 7.3: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/
- Required Software: Confirm access to the following items in your virtualization environment:
  - KVM
  - QEMU 2.0 or later
  - Libvirt API
  - Virsh tool

For more information, refer to the *Management Center VA Initial Configuration Guide*.

Hyper-V

Management Center is compatible with the Hyper-V hypervisor on the following operating system:

- Microsoft Windows Server 2016 configured with GPT partition

Management Center does not support suspend and resume operations, or the creation of watchpoints.

Virtual Machine Sizing Guidelines

Reserving memory and a CPU core for your Management Center virtual appliance (VA) is a good idea. If the resource allocation is not sufficient to support the number of devices that your license allows, the virtual appliance might not perform optimally. For example, if the server does not have the available resources to satisfy the VA resource reservations, the MC VA might not power on.

The following recommendations do not account for tenant policies that can be configured on ProxySG 6.6.x appliances (and later releases). If Management Center is collecting statistics from ProxySG appliances that are configured with tenant policy, you must significantly increase the space requirements on MC. Every 1024 tenants require an extra 20-GB disk space on VMs Disk 2 storage. For example, if each of the 10 managed devices has 2048 tenants that are configured (bringing the total number of tenants to 20480), the space requirement on Disk 2 is increased by an extra 400 GB.

When speaking with your Management Center salesperson, consider the number of devices you plan to manage with Management Center. Then, purchase the appropriate base system license, as detailed in the following sections.

The default configuration of MC VA can support up to 10 devices. Symantec delivers the following default VA configuration:

- CPU: 2 Cores
- RAM: 8 GB
- Disk 1: 4 GB
- Disk 2: 100 GB

To support more than 10 devices on an MC VA, an administrator must increase the requirements as listed in the following sections.

To support from 11 through 250 devices, configure the MC VA with the following specifications:

- CPU: 8 Cores
- RAM: 32 GB
- Disk 1: 4 GB
- Disk 2: 400 GB

To support from 251 through 500 devices, configure the MC VA with the following specifications:

- CPU: 16 Cores
- RAM: 64 GB
- Disk 1: 4 GB
- Disk 2: 600 GB

To support from 501 through 1000 devices, configure theMC VA with the following specifications:

- CPU: 32 Cores
- RAM: 128 GB
- Disk 1: 4 GB
- Disk 2: 1000 GB

If you are installing Management Center VA for the first time, you might need to adjust your virtual machine settings to match the guidelines outlined in the previous sections. See Create the Management Center VMware Virtual Appliance, without powering on the VA (step 11).

Supported Browsers

Using unsupported browsers in your deployment might yield unexpected results. The following browsers are supported for this release of Management Center.

- Google Chrome 61.0 and later
- Mozilla Firefox 50.0 and later
- Microsoft Internet Explorer 11.x

Other Internet Explorer Requirements

Note the following information:

- You must run Internet Explorer with compatibility mode turned off. To disable compatibility mode, right-click the Internet Explorer icon and select **Properties**. Click **Compatibility**, clear the **Run this program in compatibility mode for** check box and then click **OK**.
- TLS 1.0 is disabled on Management Center. To connect securely 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**.

Java

When using the legacy VPM editor, Symantec use the recommended Java version that is listed here.

Releases earlier than 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 want to launch the VPM editor from within Management Center, you must 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 earlier than the preceding SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.

If you must use Java 7 (not recommended), you must enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command.

Reference: Management Center MIB Files

A description of the various MIBS used by Management Center.

You can set up and can receive SNMP notifications about Management Center. Download the management information bases (MIBs) that Management Center supports from: https://support.broadcom.com/security.

> **NOTE**
> If you are upgrading Management Center on AWS, use only aws.bcsi images.

For instructions on configuring SNMP, refer to Configure SNMP Alerts and Configure the SNMP Agent Password.

Management Center MIBs

Management Center uses public and private MIBs.

Private MIBs

Management Center uses the following private MIBs:

MIB	Description
BCSI-MIB	A root MIB module for Symantec. This MIB is the root MIB module for Blue Coat Systems, which was acquired by Symantec. The MIB defines the parent OID for Blue Coat products, BCSI-MANAGEMENT-CENTER-MIB requires it.
BLUECOAT-MIB	A root MIB module for Symantec. The enterprise number is that of CacheFlow, Blue Coat System's former corporate name. This MIB defines the parent OID for older Blue Coat products (SG product line).
BCSI-MANAGEMENT-CENTER -MIB	The MIB module for Management Center, which describes trap notifications that are sent from Management Center.
BLUECOAT-SG-SENSOR-MIB	The MIB module for hardware sensor data.

BLUECOAT-INFO-MIB	The INFO MIB is used to provide general information about the appliance—product information, version, serial number.
BCSI-MC-RESOURCES-MIB	The BCSI-MC-RESOURCES-MIB shows the current memory utilization.
BLUECOAT-SG-HEALTHMONITOR-MIB	Not implemented.

Standard MIBs

Management Center also supports several variables in the following standard MIBs. The suggested source for these files is http://www.ietf.org.

RFC	MIB	Description
RFC 2790	HOST-RESOURCES-MIB	Monitors the values of Management Center system resources like CPU and memory
RFC 2863	INTERFACES-GROUP-MIB (IF-MIB)	Describes network interface parameters and state.
RFC 3411	SNMP-FRAMEWORK-MIB	Standard MIB for SNMP framework definitions.
RFC 3412	SNMP-MPD-MIB	Standard MIB for Message Processing and Dispatching.
RFC 2573	SNMP-TARGET-MIB	Standard MIB describing notification objects.
RFC 3414	SNMP-USER-BASED-SM-MIB	Standard MIB describing objects for User-based Security Model.
RFC 3418	SNMPv2-MIB	Describes generic objects for a managed entity.
RFC 3415	SNMP-VIEW-BASED-ACM-MIB	Describes objects for View-based Access Control Model.

Symantec Technical Support Resource

Symantec provides various methods of Technical Support.

Symantec Support Main Page

- https://support.broadcom.com/security

Knowledge Base

- https://support.broadcom.com/security/product-catalog.html

Customer Forums

- https://community.broadcom.com/home

Documentation

- https://techdocs.broadcom.com/content/broadcom/techdocs.html

Symantec Management Center Documentation Resources

Symantec provides technical and solution documentation in different formats. This page provides a resource locator.

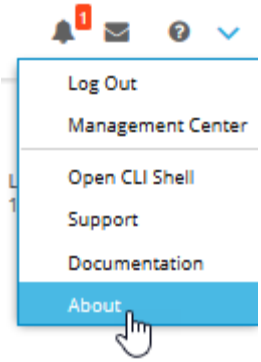
Management Center Documentation

- Access the Management Center product documentation here:
  https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/web-and-network-security.html
- Management Center *Help* (online help system)
  The online help system is intended to contain the same information as the Configuration Guide, but it is not updated as frequently. The content in the Management Center *Configuration Guide* on the Broadcom Tech Docs Portal supersedes the content in the online help.

Release Notes, Software Images, MIBs

To download software images and license keys, you need the serial number of the appliance:

- The serial number of your appliance To locate the serial number, go to the 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 more instructions, refer to the Getting Started guide.

Symantec Technical Publications documentation feedback

- documentation.inbox@broadcom.com

Symantec™
by Broadcom Software