Management Center 4.1.1.1 Release Notes

December 16, 2024

Table of Contents

Install the Management Center 4.x Upgrade....3
Management Center 4.1.1.1 Release Notes....6
New Features in Management Center 4.1.1.1....7
Fixed Issues in Management Center 4.1.1.1....8
Management Center 3.3.5.2 (Patch) Release Notes....10
Fixed Issues in Management Center 3.3.5.2....11
Management Center 3.3.5.1 (Patch) Release Notes....13
New Features in Management Center 3.3.5.1....14
Fixed Issues in Management Center 3.3.5.1....15
Management Center 3.3.4.1 (Patch) Release Notes....16
Fixed Issues in Management Center 3.3.4.1....17
Management Center 3.3.3.1 (Patch) Release Notes....19
Fixed Issues in Management Center 3.3.3.1....20
Management Center 3.3.2.1 (Patch) Release Notes....21
New Features in Management Center 3.3.2.1....22
Fixed Issues in Management Center 3.3.2.1....22
Management Center 3.3.1.1 Release Notes....24
New Features in Management Center 3.3.1.1....25
Fixed Issues in Management Center 3.3.1.1....31
Known Issues in Management Center 4.x....32
Limitations....32
Third-Party Compatibility....33
Support and Technical Documentation....36
Management Center MIB Files....37
Documentation Legal Notice....39

Install the Management Center 4.x Upgrade

Before You Upgrade Management Center

Observe the following guidelines when upgrading Management Center:

Best Practices	Description
Licenses	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 install the Management Center upgrade, 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.
Back Up the Management 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. If the upgrade fails, use the backup to restore your system. Management Center 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 Management Center configurations can be backed up 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
Back Up 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 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 CLI commands. See installed-systems for a description of the commands for adding, deleting, locking, unlocking, and viewing images.
Version Requirements	When upgrading or downgrading Management Center, you must stay within two versions of what is running. Refer to requirements for each release for more information.

Best Practices	Description
Upgrading a Failover Pair	During replication, configuration for both the primary and secondary failover partners is limited. Replication requires both the primary and secondary partners 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.
Duration of the Upgrade Process	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.

Upgrade to Management Center 4.x

To upgrade Management Center, complete the following steps:

1. Before you begin, Back Up the Management Center Configuration and export it off-box. If you must recover from a failed upgrade, 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 the Management Center appliance. 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 the 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://198.51.100.36:8082/fs/download/6c80d3a2cc124347aedb2a688da3859e
   b. Change the protocol to HTTP and the port to 8080. The URL should now look like this:
      http://198.51.100.36:8080/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. Access the web-based management console at https://*management_center_ip*/8082
7. Access the CLI using an SSH client.
8. 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
```

Management Center 4.1.1.1 Release Notes

Release Information

- **Product Version:** 4.1.1.1
- **Build Number:** 299429
- **Release Date:** December 16, 2024
- **Document Date:** December 16, 2024

Management Center Appliances

- Management Center MC-400-20
- Symantec Security Platform SSP-S210-10
- Symantec Security Platform SSP-S410-10, SSP-S410-20, SSP-410-30, SSP-S410-40
- Symantec Security Platform SSP-S410-20B, SSP-S410-40B

Compatible Symantec Products

The following products are compatible with Management Center 4.1.1.1:

Symantec Product	Minimum Version Required
Advanced Secure Gateway	SGOS 6.6
Content Analysis	1.3.x, 2.2.x
Director	6.1.19.1 Devices that are already being 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

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 4.1.1.1 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Symantec Integrated Secure Gateway (SSP appliances)

  NOTE
  You must have a Management Center Enterprise License to deploy Management Center on ISG.
- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0, 8.0
- Xen Hypervisor in Amazon Web Services (AWS)

NOTE
Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

Supported Upgrade Paths

Management Center 4.1.1.1 supports the following upgrade paths:

- 3.3.x to 4.1.1.1
- 3.2.x to 4.1.1.1

Supported Downgrades

- Downgrades from Management Center 4.1.x to 3.3.x and earlier are not supported.

The database structure in Management Center 4.1.1.1 has been updated, and cannot be reconstructed with earlier versions of Management Center.

New Features in Management Center 4.1.1.1

Management Center 4.1.1.1 includes the following new features and changes.

Core Operating System Updates

This release includes the most recent O.S. updates and third-party software libraries. The enhancements represent a modernization of the platform, ensuring maximum security and continued performance for deployed systems.

Password Expiration

Passwords for local users can now be set to expire with the **`max-password-age`** command. The password expires after a specified number of days (0-365). If the password expiration is set to 0 days, the password never expires.

The number of days, or grace period, the user has to reset an expired password is configured with the **`expiration-lockout`** command. The grace period can be set to a specified number of days (0-30). If the grace period is set to 0 days, there is no time limit for the period.

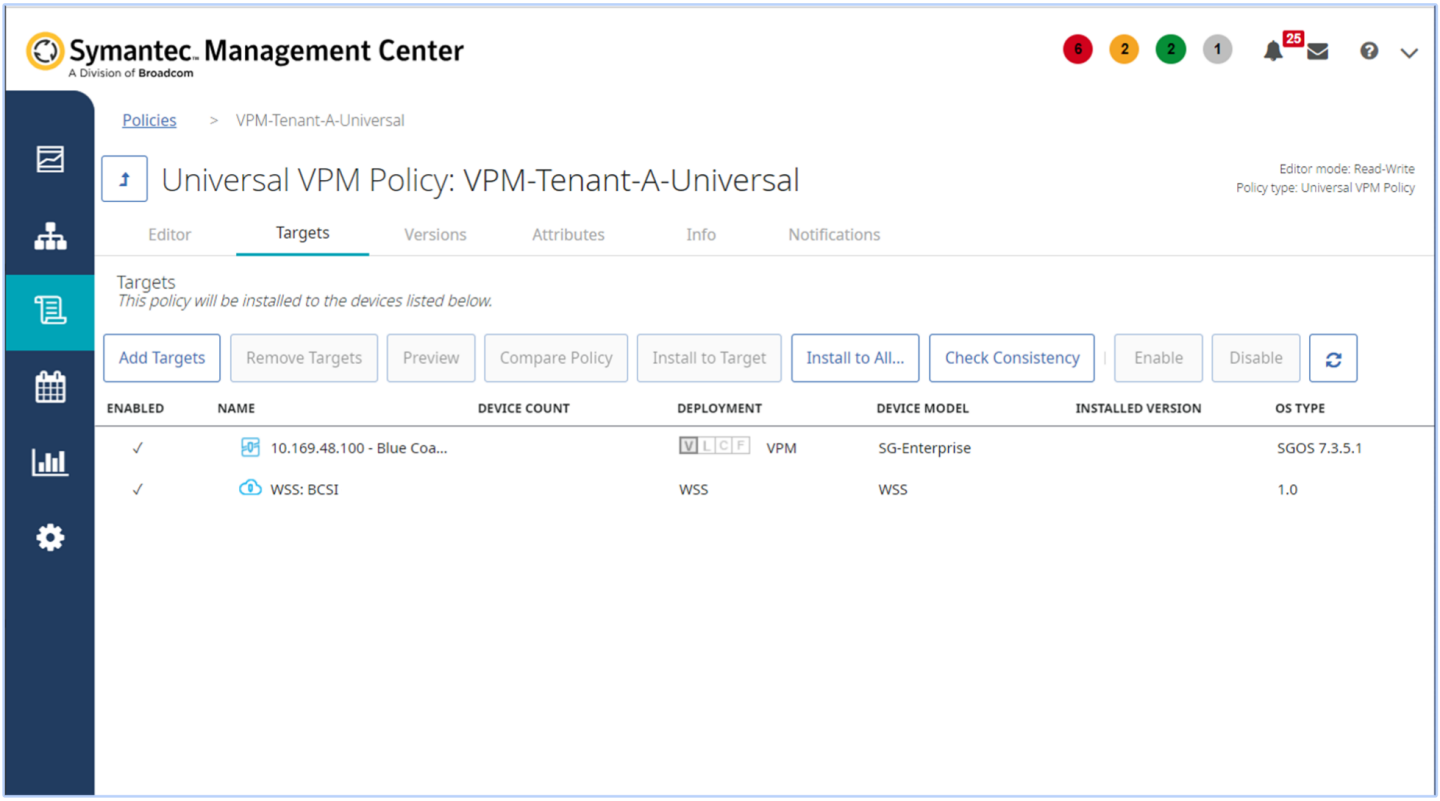
VMware ESXi 8.0 Support

Management Center 4.1.1.1 is compatible with VMware ESXi 8.0. Supported VMware servers now include:

- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0, 8.0

UPE Multitenant Feature

Universal Policy tenants in Management Center can now be associated with Cloud SWG (WSS) tenants, which allows a policy to be simultaneously enforced for both cloud and on-premise. When editing the Universal Policy in Management Center, the associated WSS tenant can now be selected as a target of the policy.



Changes to SSH Console

Changes to the SSH console include:

- Support for ssh-ed25519 as a public key and host key algorithm.
- The SSH console public key and host key algorithms can be configured.

See the *CLI Command Reference* for more information.

Microsoft Hyper-V Not Supported

Management Center 4.1.1.1 does not support Microsoft Hyper-V hypervisor.

Fixed Issues in Management Center 4.1.1.1

Management Center 4.1.1.1 includes the following fixes.

Issue	Description
SWGMGT-10334	Large policy installations to WSS can time out after 2 minutes.
SWGMGT-10303	Install policy job can sporadically fail on large list of target devices.
SWGMGT-10217	Certain EOF markers can cause policy install failures.
SWGMGT-10129	Proxy settings not working correctly with Okta authentication.
SWGMGT-10095	Default maximum revision storage can cause database bloating.
SWGMGT-9682	Download Backup operation with GUI does not support large backup files.
SWGMGT-9605	Inconsistencies between SNMP System settings in the CLI and the GUI.

Issue	Description
SWGMGT-9604	Certain reporter widgets are not loading properly.
SWGMGT-9566	Intermittent device connectivity problems as file handler limit reached.
SWGMGT-9529	Cleanup of device backups not working on automated jobs.
SWGMGT-9524	Unable to filter Alerts with the API.
SWGMGT-9513	Comments are not functioning properly in CPL fragments.
SWGMGT-9496	Some failed scripts incorrectly reporting as Successful.
SWGMGT-9432	Shared Policy Objects not keeping folder grouping after editing.
SWGMGT-9371	Management center policy import from file not validating file type meta.
SWGMGT-9304	Management Center REST API "jobs/result" queries: slow responses and high CPU usage.
SWGMGT-9303	VPM Policy edit lock not functioning.
SWGMGT-9191	Restore Configuration - Factory Default does not properly regenerate default certificate.
SWGMGT-9135	Check Consistency and Compare Policy mismatch for exception lists.
SWGMGT-9133	Importing exception pages from device does not always import all exception pages.
SWGMGT-9087	Restore Backup operation in the GUI does not support large backup files.
SWGMGT-8740	Management Center does not correctly clear temporary files after creating reports.
SWGMGT-8394	The Docker interface is blocking some connections to MC on the local network.
SWGMGT-2930	SYMSA1404 (SA148) - Linux Kernel Vulnerabilities Feb-Apr 2017
SWGMGT-2928	SYMSA1374 (SA128) - Multiple PCRE Vulnerabilities. Management Center includes the vulnerable library but does not have a vector of attack.

Management Center 3.3.5.2 (Patch) Release Notes

Release Information

- **Product Version:** 3.3.5.2
- **Build Number:** 294332
- **Release Date:** March 4, 2024
- **Document Date:** June 17, 2024

Management Center Appliances

- Management Center MC-400-20
- Symantec Security Platform SSP-S210-10
- Symantec Security Platform SSP-S410-10, SSP-S410-20, SSP-410-30, SSP-S410-40
- Symantec Security Platform SSP-S410-20B, SSP-S410-40B

Compatible Symantec Products

The following products are compatible with Management Center 3.3.5.2:

Symantec Product	Minimum Version Required
Advanced Secure Gateway	SGOS 6.6
Content Analysis	1.3.x, 2.2.x
Director	6.1.19.1 Devices that are already being 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

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 3.3.5.2 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Microsoft Hyper-V Hypervisor
- Symantec Integrated Secure Gateway (SSP appliances)

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

- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0
- Xen Hypervisor in Amazon Web Services (AWS)

NOTE
Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

Supported Upgrade Paths

Management Center 3.3.5.2 supports the following upgrade paths:

- 3.3.x to 3.3.5.2
- 3.2.x to 3.3.5.2
- 3.1.x to 3.3.5.2

Supported Downgrades

- Downgrades from Management Center 3.3.x to 3.2.x and earlier are not supported.

The database structure in Management Center 3.3.x has been updated, and cannot be reconstructed with earlier versions of Management Center.

Fixed Issues in Management Center 3.3.5.2

Management Center 3.3.5.2 includes the following fixes:

Issue	Description
SWGMGT-9599	External authorization logins fail.
SWGMGT-9394	A certificate warning is encountered when installing or opening UI packages.
SWGMGT-9359	Permissions error does not include details.
SWGMGT-9322	The Collect Certificates job for a large number of devices can hang.
SWGMGT-9272	Some ZTP payloads are created with an empty name.
SWGMGT-9222	DNS entries can revert to DHCP when deployed in GCP.
SWGMGT-9213	Full log details report not loading after upgrading to MC 3.3.4.1.
SWGMGT-9202	Proxy devices running on SSP hardware may not start up after issuing a restart command.
SWGMGT-9193	Configuring failover with an empty "security allowed-hosts" list may fail.
SWGMGT-9177	The system displays duplicate entries after 1000 rows when exporting full log details. The CSV report export limit has been updated to 50,000 rows. Reporter must be running version 11.0.2 to use this fix.
SWGMGT-9173	First-time installations of the exception page can fail.
SWGMGT-9153	The default admin account can be temporarily deleted.
SWGMGT-9146	Some scripts can trigger a false warning about affecting an ISG host.
SWGMGT-9126	The Device Inventory widget is automatically closing.
SWGMGT-9111	The name is not populating when creating a shared exception page object.
SWGMGT-9108	Users with read permissions are unable to view VPM objects and backup images.
SWGMGT-9082	Device status for the API does not return the last boot data for ISG devices.

Issue	Description
SWGMGT-8634	DNS entries can revert to DHCP when deployed in AWS.
SWGMGT-8510	Running a policy trace from MC can remove existing forward policy in SG.

Management Center 3.3.5.1 (Patch) Release Notes

Release Information

- **Product Version:** 3.3.5.1
- **Build Number:** 293194
- **Release Date:** February 20, 2024
- **Document Date:** February 22, 2024

Management Center Appliances

- Management Center MC-400-20
- Symantec Security Platform SSP-S210-10
- Symantec Security Platform SSP-S410-10, SSP-S410-20, SSP-410-30, SSP-S410-40
- Symantec Security Platform SSP-S410-20B, SSP-S410-40B

Compatible Symantec Products

The following products are compatible with Management Center 3.3.5.1:

Symantec Product	Minimum Version Required
Advanced Secure Gateway	SGOS 6.6
Content Analysis	1.3.x, 2.2.x
Director	6.1.19.1 Devices that are already being 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

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 3.3.5.1 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Microsoft Hyper-V Hypervisor
- Symantec Integrated Secure Gateway (SSP appliances)

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

- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0
- Xen Hypervisor in Amazon Web Services (AWS)

NOTE
Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

Supported Upgrade Paths

Management Center 3.3.5.1 supports the following upgrade paths:

- 3.3.x to 3.3.5.1
- 3.2.x to 3.3.5.1
- 3.1.x to 3.3.5.1

Supported Downgrades

- Downgrades from Management Center 3.3.x to 3.2.x and earlier are not supported.

The database structure in Management Center 3.3.x has been updated, and cannot be reconstructed with earlier versions of Management Center.

New Features in Management Center 3.3.5.1

Reporter Enterprise Licensing Support

MC 3.3.5.1 supports Reporter Enterprise licensing. This means that you can now add multiple Reporter devices that share a single serial number. MC 3.3.5.x and later use the Reporter appliance ID to track individual devices. After you upgrade to 3.3.5.x, the system displays a warning on Reporter devices that were present in MC before the upgrade. The warning states that the appliance ID has changed. The warning does not cause any functional issues. You can eliminate the error by deleting and then re-adding those devices. If you are running an MC release earlier than 3.3.5.1, you can add *one* Reporter that has an Enterprise license. You cannot add more than one Reporter device that has the same serial number in releases before 3.3.5.1. If you want to do that, you must upgrade to Management Center 3.3.5.x. For more information about Reporter Enterprise licensing, see the *New Features in Reporter 11.0.2.1* in the Reporter documentation.

Fractional Time Zone Support

MC 3.3.5.1 includes support for fractional time zones. You can set the Reporter Time Zone in Management Center to these additional time zones. Also, CSV reports now reflect the time zone that is specified in the Reporter Time Zone option. For more information, see the Admin Guide in the Management Center documentation.

NOTE
While Management Center supports fractional time zones, Reporter does not. When you create a Reporter report for a fractional time zone, MC uses the nearest normalized time zone to obtain the data. The system then provides results that reflect the fractional time zone.

Password Lockout

MC 3.3.5.1 includes a password lockout feature. The **`lockout`** setting determines the number of times a local user can enter a failed login password before being locked out of their account. The lockout applies to both the user interface and SSH sessions. For more information lockout settings, see the *CLI Command Reference* in the Management Center documentation.

Absolute Timeout

This option specifies the number of minutes that a local user can stay logged in without re-authenticating. When the specified number of minutes elapse after login, the user is automatically logged out. Users are logged out after this time even if they are active. The default setting is 60 minutes. 60 minutes is also the lower limit for this option. The maximum limit is 2880 minutes (48 hours). For more information about the Absolute Timeout settings, see the *Admin Guide* in the Management Center documentation.

Fixed Issues in Management Center 3.3.5.1

Management Center 3.3.5.1 includes the following fixes:

Issue	Description
SWGMGT-9394	A certificate warning is encountered when installing or opening UI packages.
SWGMGT-9359	Permissions error does not include details.
SWGMGT-9322	The Collect Certificates job for a large number of devices can hang.
SWGMGT-9272	Some ZTP payloads are created with an empty name.
SWGMGT-9222	DNS entries can revert to DHCP when deployed in GCP.
SWGMGT-9213	Full log details report not loading after upgrading to MC 3.3.4.1.
SWGMGT-9202	Proxy devices running on SSP hardware may not start up after issuing a restart command.
SWGMGT-9193	Configuring failover with an empty "security allowed-hosts" list may fail.
SWGMGT-9177	The system displays duplicate entries after 1000 rows when exporting full log details. The CSV report export limit has been updated to 50,000 rows. Reporter must be running version 11.0.2 to use this fix.
SWGMGT-9173	First-time installations of the exception page can fail.
SWGMGT-9153	The default admin account can be temporarily deleted.
SWGMGT-9146	Some scripts can trigger a false warning about affecting an ISG host.
SWGMGT-9126	The Device Inventory widget is automatically closing.
SWGMGT-9111	The name is not populating when creating a shared exception page object.
SWGMGT-9108	Users with read permissions are unable to view VPM objects and backup images.
SWGMGT-9082	Device status for the API does not return the last boot data for ISG devices.
SWGMGT-8634	DNS entries can revert to DHCP when deployed in AWS.
SWGMGT-8510	Running a policy trace from MC can remove existing forward policy in SG.

Management Center 3.3.4.1 (Patch) Release Notes

Release Information

- **Product Version:** 3.3.4.1
- **Build Number:** 287435
- **Release Date:** August 15, 2023
- **Document Date:** August 15, 2023

Management Center Appliances

- Management Center MC-400-20
- Symantec Security Platform SSP-S210-10
- Symantec Security Platform SSP-S410-10, SSP-S410-20, SSP-410-30, SSP-S410-40
- Symantec Security Platform SSP-S410-20B, SSP-S410-40B

Compatible Symantec Products

The following products are compatible with Management Center 3.3.4.1:

Symantec Product	Minimum Version Required
Advanced Secure Gateway	SGOS 6.6
Content Analysis	1.3.x, 2.2.x
Director	6.1.19.1 Devices that are already being 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

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 3.3.4.1 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Microsoft Hyper-V Hypervisor
- Symantec Integrated Secure Gateway (SSP appliances)

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

- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0
- Xen Hypervisor in Amazon Web Services (AWS)

NOTE
Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

Supported Upgrade Paths

Management Center 3.3.4.1 supports the following upgrade paths:

- 3.3.x to 3.3.4.1
- 3.2.x to 3.3.4.1
- 3.1.x to 3.3.4.1

Supported Downgrades

- Downgrades from Management Center 3.3.x to 3.2.x and earlier are not supported.

The database structure in Management Center 3.3.x has been updated, and cannot be reconstructed with earlier versions of Management Center.

Fixed Issues in Management Center 3.3.4.1

Management Center 3.3.4.1 includes the following fixes:

Issue	Description
SWGMGT-9105	SSH sessions on devices did not close after running MC scripts.
SWGMGT-9088	Backups that are downloaded from the UI are missing the correct file extension.
SWGMGT-9049	The wrong version of Reporter displays when databases are unloaded or there is a connection error.
SWGMGT-9021	The admin logins are missing from audit log.
SWGMGT-8955	Reports for <= 24hrs show the previous day instead of the current day in the filter.
SWGMGT-8951	Unable to start Statistics Monitoring Service.
SWGMGT-8947	The coe_isec.service watchdog timeout causing MC crashes.
SWGMGT-8884	Object and Operation types are not included in SMC Audit log.
SWGMGT-8874	Issuing the command diagnostics service-info send <case_number> can cause unexpected reboot/downgrade.
SWGMGT-8867	The Collect Certificates Job for ProxySG is failing.
SWGMGT-8866	Unable to add SGAC package to fresh installation.
SWGMGT-8843	The Operations button does not do anything when viewing older version of CPL policy.
SWGMGT-8819	After you upgrade to 3.3.2.1, the network devices view does not show all devices.
SWGMGT-8802	The Add Role wizard for Reporter permissions gets stuck after selecting a database.
SWGMGT-8757	The Export Backup job should not require the protocol to be lowercase.
SWGMGT-8745	Incorrect expired license warning on some Content Analysis devices.
SWGMGT-8741	Discrepancy in ISG resource usage.
SWGMGT-8731	Some reports grouped by Client IP address return error.

Issue	Description
SWGMGT-8726	The Previous Page Button does not display in "Full Log Details."
SWGMGT-8716	SGAC reports an error when Specify Credentials authentication is used.
SWGMGT-8698	Policy coverage report fails to load with large policy objects.
SWGMGT-8677	Policy/object version history does not support more than three digits.
SWGMGT-8658	False urgent alarm for Proxy License expiration.
SWGMGT-8460	MC sends alert that does not include the device identity.
SWGMGT-8405	OutOfMemoryError occurred when the REST API was used to update a Shared Object.

Management Center 3.3.3.1 (Patch) Release Notes

Release Information

- **Product Version:** 3.3.3.1
- **Build Number:** 281216
- **Release Date:** January 23, 2023
- **Document Date:** January 24, 2023

Management Center Appliances

- Management Center MC-400-20
- Symantec Security Platform SSP-S210-10
- Symantec Security Platform SSP-S410-10, SSP-S410-20, SSP-410-30, SSP-S410-40
- Symantec Security Platform SSP-S410-20B, SSP-S410-40B

Compatible Symantec Products

The following products are compatible with Management Center 3.3.3.1:

Symantec Product	Minimum Version Required
Advanced Secure Gateway	SGOS 6.6
Content Analysis	1.3.x, 2.2.x
Director	6.1.19.1 Devices that are already being 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

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 3.3.3.1 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Microsoft Hyper-V Hypervisor
- Symantec Integrated Secure Gateway (SSP appliances)

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

- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0
- Xen Hypervisor in Amazon Web Services (AWS)

NOTE
Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

Supported Upgrade Paths

Management Center 3.3.3.1 supports the following upgrade paths:

- 3.2.x to 3.3.3.1
- 3.1.x to 3.3.3.1

Supported Downgrades

- Downgrades from Management Center 3.3.x to 3.2.x and earlier are not supported.

The database structure in Management Center 3.3.x has been updated, and cannot be reconstructed with earlier versions of Management Center.

Fixed Issues in Management Center 3.3.3.1

Management Center 3.3.3.1 includes the following fixes:

Issue	Description
SWGMGT-2426	Invalid Credentials issue with connected devices due to exceeding underlying file handler limit.
SWGMGT-2386	Compare config job ip parameter discrepancy.

Management Center 3.3.2.1 (Patch) Release Notes

Release Information

- **Product Version:** 3.3.2.1
- **Build Number:** 276444
- **Release Date:** November 4, 2022
- **Document Date:** November 4, 2022

Management Center Appliances

- Management Center MC-400-20
- Symantec Security Platform SSP-S210-10
- Symantec Security Platform SSP-S410-10, SSP-S410-20, SSP-410-30, SSP-S410-40
- Symantec Security Platform SSP-S410-20B, SSP-S410-40B

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 3.3.3.1 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Microsoft Hyper-V Hypervisor
- VMware ESX Server 5.5, 6.5, 6.7
- Symantec Integrated Secure Gateway

  NOTE
  You must have a Management Center Enterprise License to deploy Management Center on ISG.
- Xen Hypervisor in Amazon Web Services (AWS)

  NOTE
  Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

Compatible Symantec Products

The following products are compatible with Management Center 3.3.2.1:

Symantec Product	Minimum Version Required
Advanced Secure Gateway	SGOS 6.6
Content Analysis	1.3.x, 2.2.x
Director	6.1.19.1 Devices that are already being 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

Symantec Product	Minimum Version Required
SSL Visibility	3.8.6, 4.x
Web Security Service	Current

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 3.3.2.1 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Microsoft Hyper-V Hypervisor
- Symantec Integrated Secure Gateway (SSP appliances)

  NOTE
  You must have a Management Center Enterprise License to deploy Management Center on ISG.
- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0
- Xen Hypervisor in Amazon Web Services (AWS)

  NOTE
  Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

Supported Upgrade Paths

Management Center 3.3.2.1 supports the following upgrade paths:

- 3.2.x to 3.3.2.1
- 3.1.x to 3.3.2.1

Supported Downgrades

- Downgrades from Management Center 3.3.x to 3.2.x and earlier are not supported.

The database structure in Management Center 3.3.x has been updated, and cannot be reconstructed with earlier versions of Management Center.

New Features in Management Center 3.3.2.1

Management Center is Now Preloaded with the Admin Console and VPM Packages

- SWGMGT-2525: Device admin console packages are now included in the Management Center software.
- SWGMGT-2525: The latest versions of web VPM packages are now included in the Management Center software.

Downloading the admin console and VPM packages from Broadcom is only necessary if:

- You are running an MC release earlier than 3.3.2.1.
- You want a package version that is released in between MC versions.

Fixed Issues in Management Center 3.3.2.1

Management Center 3.3.2.1 includes the following fixes:

Issue	Description
SWGMGT-2525	Preload MC with latest version of Admin Consoles and VPM.
SWGMGT-2494	Policy level version control.

Issue	Description
SWGMGT-2481	Execute a script against a group with the API.
SWGMGT-2453	Search device API by connection info.
SWGMGT-2377	Support for FedRamp WSS instance.
SWGMGT-2348	Legacy Java VPM editor unable to launch.
SWGMGT-2318	SMTP support over TLS.
SWGMGT-2281	AWS unexpectedly reverts to an older version of MC.
SWGMGT-1936	Shared object version control inconsistency.
SWGMGT-1712	Policy version does not match between S500 and VA.
SWGMGT-1575	Support for ZTP deployments.
SWGMGT-1549	Support for ESXi 7.0.
SWGMGT-1161	Support for Azure.
SWGMGT-1077	Support for GCP.

Management Center 3.3.1.1 Release Notes

Release Information

- **Product Version:** 3.3.1.1
- **Build Number:** 271087
- **Release Date:** February 16, 2022
- **Document Date:** February 16, 2022

Management Center Appliances

- Management Center MC-400-20
- Symantec Security Platform SSP-S210-10
- Symantec Security Platform SSP-S410-10, SSP-S410-20, SSP-410-30, SSP-S410-40
- Symantec Security Platform SSP-S410-20B, SSP-S410-40B

Compatible Symantec Products

The following products are compatible with Management Center 3.3.1.1:

Symantec Product	Minimum Version Required
Advanced Secure Gateway	SGOS 6.6
Content Analysis	1.3.x, 2.2.x
Director	6.1.19.1 Devices that are already being 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

Compatible Platforms for Deploying Management Center Virtual Appliances

You can deploy Management Center 3.3.1.1 virtual appliances on the following platforms:

- KVM 1.5.3 on CentOS 7.3
- Microsoft Hyper-V Hypervisor
- Symantec Integrated Secure Gateway (SSP appliances)

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

- VMware ESX Server 5.5, 6.5, 6.7
- VMware ESXi 7.0
- Xen Hypervisor in Amazon Web Services (AWS)

NOTE
Use only `aws.bcsi` images to install or upgrade Management Center on AWS.

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

Supported Downgrades

- Downgrades from Management Center 3.3.x to 3.2.x and earlier are not supported.

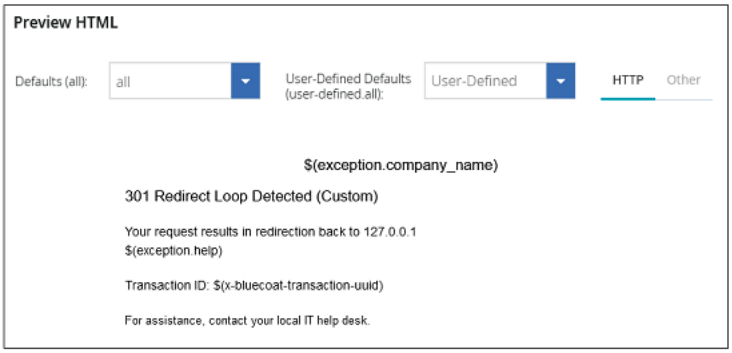
The database structure in Management Center 3.3.x has been updated, and cannot be reconstructed with earlier versions of Management Center.

New Features in Management Center 3.3.1.1

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 MC. Version control and simplified and efficient deployment ensure the continuity of an exception page standard across multiple devices.

Exception pages can be created in MC, 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 sees 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.

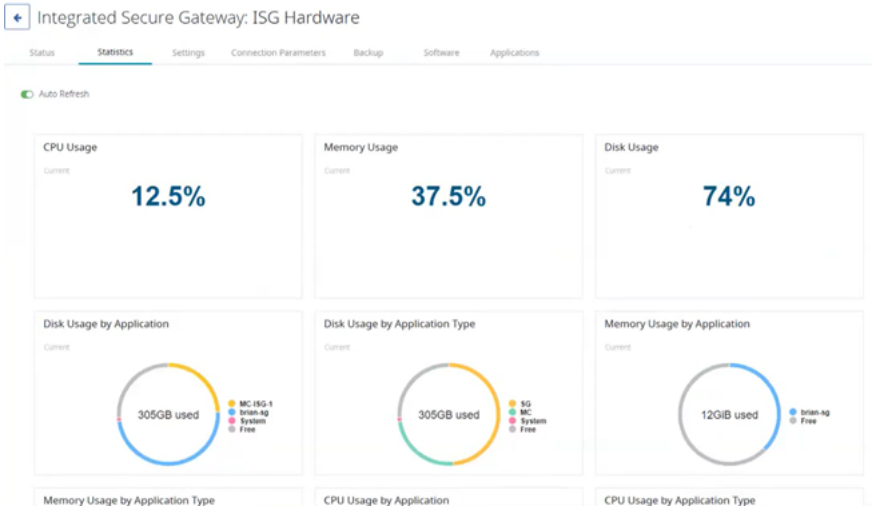
Management Center Supported As An ISG Virtual Instance

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

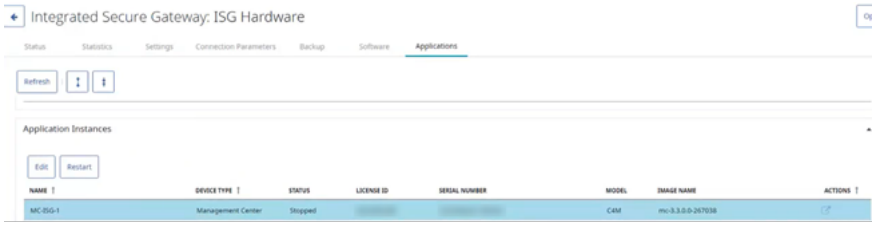
Integrated Secure Gateway (ISG) Enhancements

MC 3.3 includes the following ISG enhancements:

- **ISG Dashboard**: MC 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**: MC 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 the 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 models defined on that ISG. When you select a model, the system displays the details for each model, for example, CPUs, and RAM. 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.

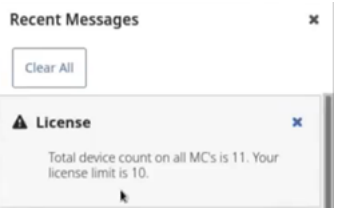
  To restart or edit an ISG application, go to **Network** > ***Device*** > **Applications** > **Application Instances**. Choose the instance and click **Restart** or **Edit**.
- **System Installation**: Installing a system image on a Edge SWG (ProxySG) that is installed as an ISG application is now supported, with the following caveats:
  - The ISG device hosting that Edge SWG (ProxySG) instance must also be managed by Management Center.
  - The system cannot mark the Edge SWG (ProxySG) image as default and does not reboot the Edge SWG (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 Edge SWG (ProxySG) appliances running 7.3.6.1 or later installed as an Integrated Secure Gateway (ISG) application. However, the ISG device hosting the Edge SWG (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 depends on your license. If you exceed the number of devices that are specified by your Enterprise license, Management Center displays a warning.



For example, consider that you have an Enterprise license with 100 devices and two appliances: with 40 devices on one appliance, and 60 devices on the other. 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 only see it again if you later add more devices. If you delete the offending devices, the system removes the message.

Ability to Filter ProxySG/ASG Policy Trace

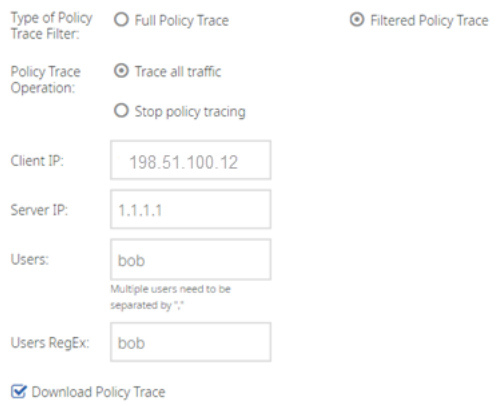
3.3 includes a new feature that allows you to filter a ProxySG/ASG policy trace for specific data. When creating a policy trace using the device operations or by creating a Policy Trace Device job, you can apply one or more filters to the policy trace action. When you select **Filtered Policy Trace**,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

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 that are 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, MC generates the following snippet of policy and installs it at the end of the forward policy for the device.

```
; START OF MC POLICY TRACE, DO NOT MODIFY <proxy>client.address=198.51.100.12 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
MC 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

MC 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 or IP address.
- **Include Network**: Settings that apply to machines on this network, such as proxy, DNS, or NTP.
- **Include ca-policy**: This setting includes information about how a CA system operates when processing a file or object that is 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, the CA backup sections are ignored. The system only processes those sections when 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

MC 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, MC 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

MC 3.3 introduces the following Appstat collector improvements that improve system performance:

- Upgraded to a 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 to reduce the impact of statistics collection on overall performance.

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 Management Center as a virtual instance on an ISG appliance. Refer to the Virtual Machine Sizing Guidelines and the ISG documentation for more information.

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. The release 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 the Web VPM has already been used in that release, proxy administrators must verify their existing policy. Then the administrators must 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.

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 Warning.
- **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 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 that 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.

Fixed Issues in Management Center 3.3.1.1

Management Center 3.3.1.1 includes the following fixes:

Issue	Description
MC-2958	The backup job timestamp did not match the system time.
MC-2900	Unable to install the certificate to the ISG appliance.
MC-2874	Disk space on the primary partner in failover mode was consumed by the unused replication slot.
MC-2826	The jobs API did not allow users to filter by time.
MC-2798	Interface issues after upgrade to 3.1.x.
MC-2792	Unexpected reboot and downgrade.
MC-2470	The PCAP filter did not work for UDP traffic.
MC-2338	Management Center UI disconnects while failover shows waiting for successful subscription status.
MC-2332	SYMSA17650 Tomcat Vulnerabilities.
MC-2318	SYMSA17570 OpenSSL Vulnerabilities (CVE-2021-23840 and CVE-2021-23841).
MC-2242	SYMSA17570 OpenSSL Vulnerabilities (CVE-2020-1968 and CVE-2020-1971).

Known Issues in Management Center 4.x

Symantec is aware of the following issues in Management Center 4.x:

Issue	Description
SWGMGT-10506	Management Center 4.1.1.1 does not support Microsoft Hyper-V hypervisor.
MC-2963	Certain illegal characters on URL strings are incorrectly allowed.
MC-808	Dashboard widgets can show connection failures in certain cases involving long-running queries.
MC-807	**Export Backup** jobs fail if the job name has more than 64 characters. Long job names can occur if the job name is a duplicate of an existing job name with auto-appended characters.
MC-806	An error message is encountered when there is a version-mismatch that is incorrect.
MC-803	Diagnostics Heartbeat data does not include failure details; only **OK** and **Failed** messages are currently displayed.
MC-802	The following CLI `show` commands do not return results: • `show security` • `show health-monitoring` • `show notification`
MC-784	You cannot download a license file when the URL contains an IPv6 address. **Workaround**: Use the license installation in the Management Center user interface.
MC-699	Management Center alert notifications still report license issue after the issue is resolved.

Limitations

Limitations are issues that Symantec is aware of. However, the issues 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 before 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 Edge SWG (ProxySG) to an SGOS version where this issue is addressed. Depending on the branch of SGOS running on your Edge SWG (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 earlier than 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.

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, or ESXi 7.0, 8.0
- Dual-core processor
- 8 GB of virtual memory
- 100-GB hard disk space

Important VMware Requirements and Notes

- 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 uses 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 #unique_26 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 systems:

- 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.

Support up to 10 Devices

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.

Support up to 250 Devices

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

Support up to 500 Devices

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

Support up to 1000 Devices

To support from 501 through 1000 devices, configure the MC 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 #unique_27, 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.

Support and Technical Documentation

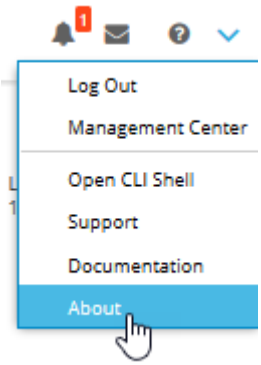
Broadcom Support Resources

- Broadcom Support
- Broadcom Knowledge Base
- Broadcom Community

Product Downloads

To download software images, licenses, release notes, and MIBs:

- Log in to the Broadcom Support portal with your username, password, and appliance serial number.
- To locate the appliance 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 Symantec Getting Started guide.

Management Center Technical Documentation

Document	URL
Management Center Documentation	https://techdocs.broadcom.com/mc
Management Center Admin and Deployment Guide	https://techdocs.broadcom.com/mc-cli-reference
Management Center CLI Reference Guide	https://techdocs.broadcom.com/mc-cli-reference
Management Center Help	On-box help
Symantec Web and Network Security Documentation	https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security.html

NOTE
Send feedback on Symantec technical documentation to: documentation.inbox@broadcom.com

Management Center MIB Files

A description of the various MIBS used by Symantec 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.

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.

For instructions on configuring SNMP, see *Device Management* in the Management Center documentation.

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.

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 © 2005–2024 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.

Symantec™
by Broadcom Software