

Symantec Management Center Initial Configuration

For Virtual Appliances

Management Center v1.9.1.1
Guide Revision: 3/27/2017



Legal Notice

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

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

www.symantec.com

3/27/2017

Management Center Initial Configuration	7
Prerequisite Tasks	8
Verify VMware Requirements	9
Virtual Machine Sizing Guidelines	9
Support up to 100 Devices	9
Support Between 101 and 250 Devices	10
Support Between 251 and 500 Devices	10
(Optional) Configure ESX Server if Management Center is Already Deployed	10
(Optional) Migrate a Management Center Appliance	10
Required Ports, Protocols, and Services	11
Inbound Connections to Management Center	11
Outbound Connections from Management Center	11
Required URLs	12
Prepare for Initial Configuration	14
Proceed to the first step	14
Retrieve the Serial Number	15
Perform the Initial Configuration	16
Download and Extract the OVF File	17
Create the Virtual Appliance	18
Power On the VA	18
Proceed to the next step	18
Enter the Serial Number	19
Configure the Virtual Appliance	20
Proceed to the next step	20
(Optional) Configure Explicit Proxy	21
Verify Web Console Access	22
Update the Management Center License	23
Verify License Components from the Web Console	24

Prevent Licensing Issues on a Virtual Appliance	25
Duplicate Serial Numbers	25
Expiring Licenses	25
Retrieve and Install the License from the CLI	26
<i>(Optional) Update an existing license</i>	26
Access the Management Center CLI	27
Stop or Restart Services	28
Stop Management Center Services	28
Restart Services	28
Troubleshoot and Resolve Issues	29
Reset or Restore Admin Account Passwords	30
Upgrade/Downgrade System Images	31
Encrypt Sensitive System Data	34
Potential Data Loss	34
Back Up the Management Center Configuration	36
Backup Requirements	36
Back Up Management Center	36
Back Up Management Center Using the CLI	36
Restore a Management Center Backup Configuration	38
Restore Management Center Backup	38

Management Center Initial Configuration

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 ProxySG, SSL Visibility Appliance, Content Analysis System, Malware Analysis Appliance, and PacketShaper products.

This documents provides the Management Center initial configuration tasks.

Prerequisite Tasks


Complete the following tasks before beginning the Management Center installation.


- "Verify VMware Requirements" on page 9
- "Required Ports, Protocols, and Services" on page 11
- "Prepare for Initial Configuration" on page 14
- "Retrieve the Serial Number" on page 15


Verify VMware Requirements

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

- VMware® ESX Server 5.5
- Dual-core processor
- 8 GB of virtual memory
- 100 GB hard disk space

 Your VMware license must be Enterprise or Enterprise Plus if you want to use remote serial connections. For more information, please refer to VMware documentation.

 Running Management Center as a virtual appliance can be demanding towards ESX server disk subsystems. Symantec recommends using enterprise grade hardware RAID controllers with 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). As an example, if your VMWare vSphere environment utilizes Pure Storage®, Disk.DiskMaxIOSize must be set to 4 MB or the image will fail to boot. For more information, refer to the VMware and storage vendor documentation.

Virtual Machine Sizing Guidelines

Symantec recommends reserving memory and a CPU core for your Management Center VA. If resource allocation is not accurate to support the number of devices that your license allows, the virtual appliance might not perform optimally. For example, if the ESX Server does not have the available resources to satisfy the VA resource reservations, the Management Center VA might not power on.

The following recommendations do not take into account tenant policies that can be configured on ProxySG 6.6.x appliances. If Management Center is collecting statistics from ProxySG appliances configured with tenant policy, you will need to significantly increase the space requirements on Management Center. 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 configured (bringing the total number of tenants to 20480), the space requirement on Disk 2 is increased by an additional 400 GB.

Support up to 100 Devices

Default configuration of Management Center VA can support up to 100 devices. Symantec delivers the following default VA configuration:

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



For additional device support on a Management Center VA, an administrator will need to increase the requirements as listed below:

Support Between 101 and 250 Devices

To support between 101 and 250 devices, configure the Management Center VA with the following:

- CPU: 4 Cores
- RAM: 16 GB
- Disk 1: 2 GB
- Disk 2: 300 GB

Support Between 251 and 500 Devices

To support between 251 and 500 devices, configure the Management Center VA with the following:

- CPU: 8 Cores
- RAM: 32 GB
- Disk 1: 2 GB
- Disk 2: 500 GB



If you are installing Management Center VA for the first time and you need to adjust your virtual machine settings to match the guidelines outlined in the previous sections, "Create the Virtual Appliance" on page 18, without powering on the VA (step 12).

(Optional) Configure ESX Server if Management Center is Already Deployed

1. Back up Management Center.
2. Export the backup to another appliance.
3. Access the Management Center CLI and shutdown the Management Center VA using the # `shutdown` privileged mode command.
4. Adjust your hardware requirements to better match your Virtual Machine configuration.
5. Power on Virtual Appliance.
6. Restore factory defaults, using the # `restore-defaults` privileged mode command.
7. Wait for the Management Center VA to start up and begin the initial configuration wizard.
8. Import and restore the desired Management Center backup.

(Optional) Migrate a Management Center Appliance

Management Center supports VMware vSphere versions 5.5 and above. You can use the vMotion Migration wizard to migrate a powered-on virtual machine from one host to another without powering the Virtual Appliance off.



If necessary, a virtual appliance failover can be configured with vMotion but is not recommended.

For more information on using the web client in vSphere 5.5, see [Migrating Virtual Machines \(5.5\)](#).

For more information on using the web client in vSphere 6.0, see [Migrating Virtual Machines \(6.0\)](#).

Required Ports, Protocols, and Services

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

Inbound Connections to Management Center

Service	Port	Protocol	Configurable?	Source	Description
SSL	8080 8082	TCP	No	User's client	Management Center web console
SSH	22	TCP	No	User's client	Management Center CLI
SSL	8082	TCP	No	User's client	Management Center API

Outbound Connections from Management Center

Service	Port	Protocol	Configurable?	Destination	Description
LDAP LDAPS	10389 389 636	TCP	Yes	LDAP server	Authentication
Active Directory	10389 389 636	TCP	Yes	Active Directory server	Authentication
RADIUS	1812	UDP/TCP	Yes	RADIUS server	Authentication
RADIUS	1813	UDP/TCP	Yes	RADIUS server	Accounting
SMTP	25	TCP	Yes	SMTP server	SMTP alerts
SNMP Trap	162	UDP	Yes	Trap receiver	SNMP traps
HTTP Proxy	8080	TCP	Yes	HTTP Proxy	Updates
NTP	123	UDP/TCP	No	NTP server list	Time sync to customer-configured NTP time server
HTTPS	443	TCP	No	Symantec	bto.bluecoat.com License activation, Web Application Protection (WAP) subscription, the latest release information and documentation
DNS	53	UDP/TCP	No	DNS server	FQDN lookups
MA	443	TCP	No	Malware Analysis	Health monitoring and backup

Service	Port	Protocol	Configurable?	Destination	Description
PacketShaper	80/443	TCP	No	PacketShaper	Health Monitoring (unencrypted/encrypted)
Reporter	8080/8082	TCP	No	Reporter	Reporter API (unencrypted/encrypted)
ProxySG	22	TCP	No	ProxySG appliance	ProxySG appliance monitoring and management
Management Center	22	TCP	No	Management Center	Management Center communication with fail-over partner
VPM	8082	TCP	No	ProxySG appliance	Visual Policy Manager
CAS	8080/8082	TCP	No	Content Analysis	Health Monitoring (unencrypted/encrypted)
ProxySG	9009	TCP	No	ProxySG appliance	ProxySG appliance Performance Statistics. Starting with Management Center 1.7, Port 9009 is disabled unless HTTP is enabled via the <code>security http enable</code> command.
ProxySG	9010	TCP	No	ProxySG appliance	ProxySG appliance Performance Statistics over HTTPS
SSL Visibility	443	TCP	No	SSL Visibility	Health monitoring and configuration synch

Required URLs

Ensure connectivity from Management Center to the following URLs.

URL	Protocol	Port	Description
validation.es.bluecoat.com/phs.cgi	HTTPS TCP	443	Validates the license every 5 minutes. After successful validation, validation occurs every hour.
bto-services.es.bluecoat.com	HTTPS TCP	443	Validates the license.
device-services.es.bluecoat.com	HTTPS TCP	443	License related.
services.es.bluecoat.com	HTTPS TCP 443	443	License related.

Management Center Initial Configuration

URL	Protocol	Port	Description
abrca.bluecoat.com	HTTPS TCP	443	Symantec CA.
appliance.bluecoat.com	HTTPS TCP	443	Trust package downloads.
subscription.es.bluecoat.com	HTTPS TCP	443	Subscription services.
upload.bluecoat.com	HTTPS TCP	443	Upload diagnostic reports to Symantec support.
sgapi.es.bluecoat.com	HTTPS TCP	443	Universal VPM policy.

Prepare for Initial Configuration

The initial configuration wizard prompts you to configure basic network settings. Obtain and record the information specific to your deployment in this table, and then use your notes for reference when you go through the installation process.



Print this chapter for reference

Requirement	Description	My values
Appliance serial number	The serial number from the Symantec Licensing Portal (BCLP). See "Retrieve the Serial Number" on the next page.	
Interface configuration	IP address.	
	Subnet mask.	
Default gateway	IP address for the default gateway.	
DNS servers	IP address for the primary DNS server.	
	(Optional) IP address for the secondary DNS server.	

Proceed to the first step

Before you begin, make sure that you have all ports and protocols readily available, then go to "Retrieve the Serial Number" on the next page.

Retrieve the Serial Number

You must use the correct serial number to ensure that your license is valid.

To retrieve appliance serial numbers:

1. Make sure you have a BTO username and password. In addition to retrieving appliance serial numbers, these credentials are required for obtaining your license and downloading software upgrades.
If you do not have a BTO account, contact customercare@bluecoat.com.
For additional contact information, go to <https://bto.bluecoat.com>.
2. Locate the e-mail you received from Symantec. This e-mail contains the software activation codes as well as a link to the BCLP.
3. Log in to BCLP:
 - a. Click the link embedded in the e-mail (https://services.bluecoat.com/eservice_enu/licensing/register.cgi).
The web browser displays the BCLP page.
 - b. On the BCLP login screen, enter your BTO username and password, and then click **Login**.
The BCLP displays the Home page.
4. In the Enter Activation Code field, enter the activation code from your e-mail.
5. Click **Next**.
The BCLP displays the License Agreement page.
6. Read and accept the License Agreement, and then click **Next**.
A BCLP displays the serial numbers page.
7. Record the appliance serial number. You will need this number to complete this initial configuration wizard.



Each serial number is unique. When performing initial configuration, ensure that you use a dedicated serial number. Reusing a serial number from another VA could cause the license to be suspended.

Perform the Initial Configuration

Complete the following tasks to install and perform initial Management Center configuration.

- "Download and Extract the OVF File" on the next page
- "Create the Virtual Appliance" on page 18
- "Configure the Virtual Appliance" on page 20
- "(Optional) Configure Explicit Proxy" on page 21
- "Verify Web Console Access" on page 22
- "Enter the Serial Number" on page 19
- "Update the Management Center License" on page 23
- "Prevent Licensing Issues on a Virtual Appliance" on page 25
- "Retrieve and Install the License from the CLI" on page 26
- "Access the Management Center CLI" on page 27
- "Stop or Restart Services" on page 28

Download and Extract the OVF File

Log in to BTO and download the Management Center VAP file. The VAP file is a .zip file that contains:

- An Open Virtualized Format (OVF) file
 - Two Virtual Machine Disk Format (VMDK) files:
 - MC-V10-disk1.vmdk (for the boot disk).
 - MC-V10-disk2.vmdk (for the virtual disk).
 - This guide in PDF format.
1. Log in to BTO (<https://bto.bluecoat.com/download>) and select **Downloads**.
 2. Browse to the Management Center page.
 3. In the Management Center section, click the link for the VAP file and follow the instructions to save the file.
 4. Extract the contents of the VAP file to a location that you can access from the system where you are running the VMware client.



The OVF file includes a pointer to the .vmdk files; thus, you must extract and store the contents of the .zip file within the same folder. Do not rename the files.

Create the Virtual Appliance

After you extract the OVF file, create the Management Center VA.

1. Log into VMware client.
2. Select **File > Deploy OVF Template**. The VMware client displays a wizard.
3. In the Source dialog, click **Browse** and browse to where you extracted the OVF file; click **Next**.
4. Verify the details for OVF template and click **Next**.
5. Specify a name for the VA and the inventory location; click **Next**.
6. Select where to put the VA (host or cluster); click **Next**.
7. Select where to store the virtual machine's files; click **Next**.

8. Specify thick or thin provisioning for the disk format and click **Next**.

If you select thin provisioning, VMware allocates only the required amount of virtual disk space for the VA. Thick provisioning could result in slightly better performance, but it is not required. Refer to VMware documentation if you require more information on virtual disk provisioning.

9. Select a network to map to and click **Next**.
10. On the Ready to Complete dialog, review your settings.
11. (Optional) At the bottom of the dialog, select **Power on after deployment** to power on the VA after deployment. If you do not select it, you can power on the VA later.



Do not power on the virtual appliance if you need to adjust the resource allocation for the virtual machine. See "Virtual Machine Sizing Guidelines " on page 9.

12. Click **Finish**. The VMware client displays a `Deploying name` message with a progress bar. When deployment is complete, close the message. The inventory on the left displays the VA.

Power On the VA

If you did not power on the VA in step 12 of the previous procedure, power it on now.

1. Locate the VA in the inventory, select it, and right-click. Select **Power > Power On**.
2. Verify that the VA is powered on. If it is powered on, its icon should look similar to the following:



You can also select the VA and right-click. If the VA is already powered on, the **Power > Power On** option should be unavailable.

Proceed to the next step

"Enter the Serial Number" on the next page.

Enter the Serial Number

To activate your Virtual Appliance , enter the serial number that was provided in the eFulfillment e-mail from Symantec. After your serial number is validated, you can enter the Management Center CLI console.

1. In the VMware client, in the inventory on the left, right-click the VA.
2. Select **Open Console**. The VMware client displays the console. The console prompts you to enter the serial number.
3. Type in your serial number and press Enter.
4. If the serial number is not valid, check the number and try again. If the serial number is not accepted, do not proceed to the next steps; contact Symantec Support.

See the BlueTouch Support Options web page for information:

<http://www.bluecoat.com/support/technical-support/bluetouch-support-options>

If the serial number is valid, the console prompts you to press Enter three times.

5. Press Enter three times. The console displays the initial configuration wizard.

Configure the Virtual Appliance

After your serial number was validated, the initial configuration wizard displayed. Follow the prompts to complete initial configuration of Management Center and refer to your notes in "Prepare for Initial Configuration" on page 14.

You can change these settings at any time after initial configuration. When you change the IP address, note the following:



The web console can take a while to load; if the browser displays an error after you change the IP address, try connecting to the web console again in a few moments.

The SSL certificate is regenerated; you do not have to do it manually. If a new certificate is required after is already configured, use the CLI command `#security generate-ssl-certificate` to regenerate it.

1. In the initial configuration wizard, enter the following details, pressing Enter after each entry:
 - IP address (you will use this IP address for the web console)
 - Subnet mask
 - IP address for the default gateway
 - IP address for the primary DNS server
 - (optional) IP address for the secondary DNS server
 - The `admin` account password; the wizard prompts you to enter the password again for confirmation

Make sure that the password is not easily guessed; if the password is not valid (for example, it is too short or is a dictionary word), the wizard prompts you to enter another password. Use an alphanumeric password that is at least 8 characters long.

When setup is complete, the CLI displays the welcome banner:

```
Copyright (c) 2015, Symantec Corporation
Welcome to the Symantec Management Center CLI
Version: 1.4.1.1 Release id: 154515
-----MENU-----
1) Command Line Interface
2) Setup
-----
Enter option:
```

2. Perform one of the following to close the console:
 - Press Ctrl+Alt to release the cursor from the Console.
 - Click an area outside of the Console tab.



You can only reset the `admin` account with the following conditions:

- Serial console access.
- The CLI command `#security enable-password`: Resets the password used to access the CLI for the `admin` account.

Proceed to the next step

Before proceeding to the next step, verify that Management Center has been configured correctly. Go to "Verify Web Console Access" on page 22 then go to "Update the Management Center License" on page 23.

(Optional) Configure Explicit Proxy



Perform these steps only if you have an explicit proxy deployment.

Because Management Center is deployed behind the ProxySG appliance, you must configure proxy settings in an explicit deployment. If the proxy configuration is missing or incorrect, Management Center will be unable to connect to BTO for license downloads.

1. Log on to the CLI. See "Access the Management Center CLI" on page 27 for instructions.
2. To enable use of the proxy server, issue the following command:
`#http-proxy enable`
3. To configure the explicit proxy, issue the following command and specify the settings:
`# http-proxy configure HTTP Proxy host: <proxy_IP_address_or_hostname>`
`HTTP Proxy port: <proxy_port_number>`
`Username: <proxy_username>`
`Password: <proxy_password>`
4. (Recommended) Issue the `#show setupinfo` command to display and verify the proxy settings you entered. The proxy settings display in the `HTTP Proxy Settings` section of the command output.

For more information on configuring proxy settings in the web console, refer to the [Management Center Configuration Guide](#) on BTO. To configure proxy settings using the CLI, refer to the [ProxySG CLI Reference Guide](#).

Verify Web Console Access

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



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

1. Open a web browser.
2. In the address bar, enter the URL.

`https://ip_address:8082`



You cannot change the port number.

The web browser displays the login screen.

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

Update the Management Center License



The Management Center license contains all of the features for which you have purchased a subscription. The documentation covers all features, including ones that you may not have purchased.

You can update your existing license from BTO, download the license from a web server or workstation, or install it manually.

1. To view license status or to update or install a license, select **Administration > License**.
2. To view detailed license component information, select the **License Components** tab.



Use the passphrase field when you are installing a license you generated with a passphrase; the passphrase is required for VA Offline licensing.

3. To determine how you will install the license, select the **Install New License** tab. See the following sections for instructions.
4. (Optional) To troubleshoot the license installation, do the following:
 - To check the status of a license, run the CLI command `#license view`.
 - To verify network settings, run the CLI command `#show interface`.
 - To verify site accessibility, run the CLI command `>ping` with the following sites:
 - `ping bto-services.es.bluecoat.com`
 - `ping validation.es.bluecoat.com`
 - To update the license, run the CLI command `#license get-from-bluecoat`.
 - Try to update the license again, after running the CLI command `#restart reboot`.
5. (Optional) From a web browser, log into Management Center. If the web console loads, the license was installed successfully.
If the web console does not load, run the CLI command `# license view` to determine if the license was installed and is valid.

Install the license from BTO



You must install the license from BTO using the `#license get-from-bluecoat` CLI command at least once before you can install it from BTO using the web console.

1. Select **Install from BTO**.
2. Enter your BTO User ID and BTO Password.
3. Click **Install License**.
4. Click **Refresh** to display the updated license information in the License Components table.

Install from URL

Before you can install your license you must first get the license file (*.bcl or *.bin) and save it to a location on a web server or workstation that the VA can access.

1. Select **Install from URL**. The web console displays a text field.
2. Enter the location (a valid URL) of the license file into the field.
3. Click **Install License**.
4. Click **Refresh** to display the updated license information in the License Components table.

Paste license text from a text editor

Before you can install your license you must first get the license file (*.bcl or *.bin) and save it to a local directory. Open the license file in a text editor (such as Notepad) and make sure you save the file.

1. Select **Paste license text**. The web console displays a text box.
2. Copy and paste the license from the text editor to the box.
3. Click **Install License**.
4. Click **Refresh** to display the updated license information in the License Components table.

Verify License Components from the Web Console

Management Center has a flexible license model. Components can be licensed, and are exposed dependent upon the license type and component name. You can view the validity of licensed components, add more devices to your license, and view the serial number and appliance model of the hardware appliance. Install or update your licenses directly from BTO while logged into the web console.

1. To verify the license components, type and status, log in to the web console.
2. Select **Administration > License**. From the **License Component** tab you verify the following **General Information** about the license:
 - Manufacturer (Symantec Corporation)
 - Number of Maximum Devices allowed
 - Serial Number
 - Appliance Model
 - Status
 - Component Name
 - Activation date
 - Expiration date
 - License Type

Prevent Licensing Issues on a Virtual Appliance

To prevent licensing issues, ensure that the VA is allowed network access to the license validation server at <https://validation.es.bluecoat.com>. See "Verify Web Console Access" on page 22.

If communication with the server fails, the license may be suspended. Unless you have purchased a VA offline license, constant Internet connection is required for Management Center to communicate regularly with the license validation server to confirm that the serial number is valid.

Duplicate Serial Numbers

If the license validation server detects duplicate serial numbers, your license is invalidated and the license health status goes to a critical state. Verify your license in [BCLP](#) and contact Symantec Support if you continue to have problems.

Expiring Licenses

Management Center health goes into a Warning state when the license is 15 days from expiring. For example, if the license will expire on January 30th, the Messages option in the web console banner displays Warning-level alerts, such as the following, starting on January 15th.



The web console banner displays an alert for each licensed component.

Once the license expires, Management Center goes into an Error state and remains in that state for another 15 days or until the license is updated (whichever occurs first). For example, starting on January 30th, the Messages option in the web console banner displays Warning-level alerts for each licensed component until the license is renewed.

If you do not renew the license within 15 days after the expiration date, you will be unable to load the web console. You must renew the license through the CLI using `# license get-from-bluecoat` or `# license get-from-url`.

Retrieve and Install the License from the CLI

The Management Center license contains data that is used to uniquely identify the VA as a Symantec appliance.



Make sure that you are connected to the internet while performing this procedure.

1. Log on to the CLI. See "Access the Management Center CLI" on the next page for instructions.
2. Enter privileged mode from standard mode by using the `enable` command. The prompt changes from a `>` to a `#`, indicating that you are in privileged mode.
3. At the `#` command prompt, type the following command and press Enter.

```
#license get-from-bluecoat
```



For more information, refer to `#license` in the *Management Center Configuration Guide*.

4. Restart the Management Center services. See "Stop or Restart Services" on page 28.
5. Go to the Management Center web console in a web browser. See "Verify Web Console Access" on page 22.



If a license is not installed and the VA is powered on, users will be unable to load the Management Center web console. Additionally, once installed, connectivity to the license validation server must be maintained unless you have purchased a VA Offline license. The VA Offline license requires the use of a passphrase. When you use the offline license installation process, enter the same passphrase used to generate the Offline VA license. See "Update the Management Center License" on page 23 for more information.

(Optional) Update an existing license

To update an existing license, you can run the `#license get-from-bluecoat` CLI command. In addition, unless you have purchased a VA offline license, the VA must be allowed access to the following server:

<https://bto-services.es.bluecoat.com>

Access the Management Center CLI

Log on to the CLI through an SSH connection or through the Management Center VMware console.



For hardware appliances, access the CLI through the serial console.

Log on using SSH

1. Install an SSH client. This procedure uses PuTTY as an example; your steps might be slightly different.
2. Open PuTTY and specify the following information:
 - **Host Name (or IP address)**—The IP address that you specified for
 - **Port**—22
3. (Optional) Specify a name for the connection and click **Save** to save the settings.
4. Click **Open**. The SSH window opens, with a login prompt.
5. At the `login as:` prompt, type **admin** and press Enter.
6. At the `admin@IP_address's password:` prompt, type your password and press Enter. The console displays the CLI banner.

Log on through the VMware console



Use the VMware console or SSH if you are logging into a Virtual Appliance.

1. In the VMware client, browse to the VM in the inventory.
2. Select the VM, right-click, and select **Open Console**.
The console displays the CLI console and prompts you to press Enter three times.
3. Press Enter three times. The console displays the CLI banner.

Stop or Restart Services

To troubleshoot some issues, you might need to stop or restart Management Center services. You will need to restart the services after you install or update a Management Center license.

Stop Management Center Services

You can start or stop the Management Center, report generator, or statistics monitoring services.

1. "Access the Management Center CLI" on the previous page.
2. Enter privileged mode by typing **enable** at the command prompt.
3. Enter your enable password and press Enter.
4. At the # prompt, type the following command and press Enter:

```
#service stop-service [ management-center | report-generator | statistics-monitoring ]
```

The CLI displays the command prompt.

Restart Services

1. "Access the Management Center CLI" on the previous page.
2. Enter privileged mode by typing **enable** at the command prompt.
3. Enter your enable password and press Enter.
4. At the # prompt, type **restart services** and press Enter.
The CLI displays the command prompt.



You cannot access the web console while the services are restarting; however, you can try accessing the web console a few minutes after issuing the command.

Troubleshoot and Resolve Issues

This section discusses troubleshooting steps and advanced procedures for Management Center.

The following topics provide information for resolving common issues:

- "Reset or Restore Admin Account Passwords" on the next page
- "Upgrade/Downgrade System Images" on page 31
- "Encrypt Sensitive System Data" on page 34
- "Back Up the Management Center Configuration" on page 36
- "Restore a Management Center Backup Configuration" on page 38

Reset or Restore Admin Account Passwords

You can reset the password for the CLI (serial console). You can also restore the default password for the admin UI (web console). The admin account to access the CLI versus the admin account to access the web console are different accounts (and thus the passwords are not the same).



To reset the CLI admin account password, use `# security reset-password`. This command is only available through the serial console for hardware appliances and Management Center VMware console for virtual appliances.

1. "Access the Management Center CLI" on page 27.
2. Enter privileged mode by typing `enable` at the command prompt. See Privileged Mode Commands.
3. Enter your enable password and press Enter.
4. At the `#` prompt, type `restore-defaults reset-admin` and press Enter.

The CLI prompt displays the following:

```
This operation will restore admin password on UI to default. Management Center ser-
vice will be unavailable during this operation.
```

```
Are you sure you want to restore UI admin password? [y/N]
```

Resets the UI admin password to admin/admin.

Upgrade/Downgrade System Images

When new features and improvements are made to Management Center, you can download a system image from Symantec and *upgrade* the appliance. If you ever experience issues with a new image, you can activate an older image to *downgrade* the appliance.

Manage System Images

Management Center stores up to six images on the system. For Management Center virtual appliances, this number also depends on the image size and boot partition (limited to 2 GB by default). The image that is marked as the default image will be loaded the next time that the appliance is rebooted.

If the maximum number of images are stored on your system and you download another image, Management Center deletes the oldest unlocked image to make room for the new image. To prevent an image from being deleted or replaced, you can lock the image.

You perform image management using Management Center CLI commands. See # installed-systems for a description of the commands for adding, deleting, locking, unlocking, and viewing images.

Install a New System Image

To install a new system image, you first download the image from Symantec, place the file on a web server the Management Center appliance can access, then use a CLI command to add the file. The final step is to reboot to activate the image.

1. (Optional, but recommended) "Back Up the Management Center Configuration" on page 36.
2. Log into Blue Touch Online (BTO): <https://bto.bluecoat.com/>
3. Download the desired image from BTO.
 - a. Transfer the image directly to Management Center. Select **Configuration > Files** and transfer the image using the [Transfer File](#) button.
 - b. Download the image to a local drive, select **Configuration > Files**, and [upload the image](#) to Management Center.



Alternatively, you can store the image file on a web server that the Management Center appliance can access. The add image process works with any HTTP server, and HTTPS servers configured with trusted certificates. If your HTTPS server does not have a trusted certificate, place the file on an internal HTTP server.

4. Add the system image using the `#installed-systems add <URL>` command.

where `<URL>` is the location of the image on a web server, in the following format:

`http://host/path, for example http://webserver.mycompany.com/images/542386.bcsi`

If the image was uploaded to Management Center, do the following:

- a. Copy the file URL. In the **Configuration > Files** page, select the image and click **Copy URL**. The file will have a format similar to the following:

`https://10.131.38.36:8082/fs/download/6c80d3a2cc124347aedb2a688da3859e`

- b. Change the protocol to HTTP and the port to 8080. The URL should now look like this:

`http://10.131.38.36:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e`

If HTTP access to Management Center is disabled, you should change the URL to the following:

`http://localhost:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e`

- c. Execute the `installed-systems add` command.

5. Make sure the new image is the default image. (Rebooting will install whichever image is marked as the default.)

```
# installed-systems view
```

A plus (+) sign indicates the default system image. If the new image is not the default, make note of the index value next to the image you want as the default.

6. If necessary, make the new image the default system image:

```
# installed-systems default <index_number>
```

Replace `<index_number>` with the image's index ID value.

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

```
# restart reboot
```

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



View the progress of downloads in progress or the status of the last download using the `# installed-systems view-downloads` command. If you need to cancel an image download, use the `# installed-systems cancel-downloads` command.

Downgrade to an Earlier Management Center Version

If you are running an upgraded version of Management Center, you can downgrade (revert) to a previous version. Downgrading has the following special guidelines you must follow:

- Downgrades can be performed down two dot releases (e.g., from 1.6 to 1.4).
- All maintenance/patch releases of a version will be treated as equivalent. For example, 1.6.2.1 would be the same as any other 1.6.x release.
- Upon downgrade, newer data (data from the upgraded image that is not handled in the older version) is lost.
- Upon downgrade, newer configuration settings (settings from the upgraded image that are not handled in the older version) are lost.
- Data and configuration settings that are common to the upgraded image and downgraded image are seamlessly maintained, regardless of schema differences between versions.
- Administrator access and permissions are needed to downgrade Management Center.

To downgrade:

1. "Back Up the Management Center Configuration" on page 36.
2. Decide which installed image to revert to. (Make sure to follow the guidelines listed above regarding release

numbers.)

```
# installed-systems view
```

Make note of the index value next to the image you want to revert to.

3. Make an older image the default image. (Make sure to follow the guidelines listed above regarding release numbers.)

```
# installed-systems default <index_number>
```

Replace *<index_number>* with the image's index ID value.

4. Reboot the hardware appliance to activate the default image:

```
# restart reboot
```

5. Before trying to use the older version, restore the Management Center backup immediately. See "Restore a Management Center Backup Configuration" on page 38.

Encrypt Sensitive System Data

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

Potential Data Loss

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

New Management Center Appliance Recommendations

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

1. Select **Administration > Data Protection**.
2. Click **Generate Key**.

A new encryption key is created and a recovery key is displayed.

3. Record the recovery key and secure it in a safe location.
4. Click **Restart System**.
5. Configure the appliance.
6. Run a Management Center backup. See "Back Up the Management Center Configuration" on page 36.

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

Upgrade Recommendations

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

1. Select **Administration > Data Protection**.
2. Click **Generate Key**.

A new encryption key is created and a recovery key is displayed.

3. Record the recovery key and secure it in a safe location.

4. Click **Restart System**.
5. Run a Management Center backup. See "Back Up the Management Center Configuration" on the next page.

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

Back Up the Management Center Configuration

Symantec recommends that you back up the Management Center configuration often. The backup contains Management Center database, settings, and, optionally, device reporting statistics. To save disk space on the appliance, you can export the backup to an external server as part of the backup job. Exporting backups to an external server is required before upgrading or downgrading the software image. See "Upgrade/Downgrade System Images" on page 31.

Backup Requirements

Backing up the Management Center configuration requires specific permissions. See Reference: Understanding Job Permissions. Additionally, sensitive data in the backup will be encrypted with an encryption key. You must have the recovery key to restore the encrypted data in the backup. See "Encrypt Sensitive System Data" on page 34 for more information.

Back Up Management Center

To back up the Management Center configuration, you must create a job for it. You can either schedule the job to run on a regular basis, run immediately, or on demand at a time that you want to create a backup.

1. From **Jobs > Scheduled Jobs**, select **New Job**. The web console displays the New Job wizard. An asterisk denotes fields that are mandatory.
2. Enter a unique **Name**.
3. Enter a **Description** (perhaps the reason why a backup of Management Center is needed). Click **Next**.
4. From the **Operation** drop-down list, select **Backup Management Center**.
5. (Optional) Select the **Exclude Statistics Monitoring Trend Data** check box to exclude device reporting statistics. By excluding these statistics, the backup will be substantially smaller (perhaps by hundreds of gigabytes). Keep in mind, however, that the restored backup will not have any statistics data.
6. If you want the backup file to be exported to an external HTTP, FTP, or SCP server, select the **Export to Server** check box and fill in the server details:
 - **Server URL**: Enter the protocol (SCP, FTP, FTPS, HTTP, HTTPS) and server name and path. For example: *ftp://mycompany.com/backups*
 - **Encryption Phrase**: This is required for exporting the archive.
 - **Username**
 - **Password**
7. In the Targets screen, click **Next**. (No targets are required for this operation.)
8. In the Schedule screen, define a schedule for the job. See Job Scheduling Options for explanations of each option. Click **Finish**.



Management Center retains only five backups. When the sixth backup occurs (such as in a recurring job), the oldest backup is deleted. This is a rolling five backup retention and cannot be configured. To retain additional backup configurations, you can export the backup to an external server as part of the backup job, or you can export backups later using the `backup export` CLI command.

Back Up Management Center Using the CLI

1. Log in to the CLI. See "Access the Management Center CLI" on page 27
2. Enter privileged mode. See Privileged Mode Commands.

3. At the command prompt, type the following command and press Enter:
backup create

The CLI indicates that the backup is being created. You should see a response similar to the following:

```
Creating backup ...  
Backing up runtime configuration and plugins ...  
Backing up database ..  
Completed backup, Wed Jun 3 11:01:33 CMT 2015.
```

Restore a Management Center Backup Configuration

You can restore a configuration backup after reinstalling, upgrading, or downgrading Management Center or if you want to revert to a previous configuration. You perform this operation using the command-line interface.



Restoring a backup requires shutting down services; you should perform the restore during off-hours.

Restore Management Center Backup

Before you restore a backup, you should view the backup files currently stored on the system to make sure that you restore the correct version. If the backup you want to restore was exported to an external server, you should import the backup file before the restore process.

1. "Access the Management Center CLI" on page 27.
2. Enter privileged mode. See Privileged Mode Commands.
3. At the command prompt, type the following command and press Enter:
backup view

The CLI displays a list of all the backups that were created for this instance of Management Center. You should see a response similar to the following:

Available Backups:

	Timestamp	Version
1	2015-May-29 03:33:00 UTC	1.4.1.1 (555156)
2	2015-Apr-15 09:02:00 UTC	1.3.3.1 (555000)

The backups are listed in descending chronological order; for example, the backup with index number 1 is more recent than index 2. Each backup indicates the date and time when the backup was created, the build version, and in parentheses, the build number.

4. Once you identify the backup you want, make note of the index number.
5. (Optional) If the backup you want to restore was exported to a server and is not on the list of backups stored on the appliance, you can import it to Management Center.

#**backup import <URL>**

<URL> is the URL of the server and path to the backup file. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP.

6. At the command prompt, type the appropriate command.
 - To restore the latest version (the backup with the most recent timestamp):
backup restore latest
 - To restore a specific version:
backup restore <index_number>
where <index_number> is the index number of the backup.

7. Press Enter. The CLI indicates that you are about to restore a backup and asks you to confirm the action:

Warning, restoring a backup replaces all Management Center configuration.
Do you wish to proceed with restoring the backup taken on 2015-May-29 03:33:00

UTC? [Y/N]

8. Type **Y** to proceed. The CLI displays the progress of the restore:

```
Restoring backup ...
Decompressing ...
Verifying backup contents ...
Shutting down services ...
Restoring database ...
Restoring configuration ...
Restarting services ...
Completed restoring backup.
```