Security Event Manager

Version 6.7.1
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
# Table of Contents

**Prepare to upgrade SEM** .......................................................................................................................... 4  

**Determine your upgrade path to the latest version of SEM** ................................................................. 5  

**Best practices for SEM upgrades** ............................................................................................................. 6  

- Resize the SEM virtual appliance .................................................................................................................. 6  
- Additional considerations for VMware vSphere ............................................................................................ 7  

**Upgrade SEM: complete steps** .................................................................................................................. 8  

- SEM upgrade options - Debian upgrade ..................................................................................................... 8  
- Upgrade the virtual appliances ..................................................................................................................... 8  
- Troubleshoot errors during the appliance upgrade ....................................................................................... 9  
- Prepare and share information with Customer Support .............................................................................. 9  
  - Pull debugging information from your SEM virtual appliance .................................................................... 9  
- Upgrade to SEM 6.4 or later using an ISO .................................................................................................... 10  
  - Mount the ISO image on Microsoft Hyper-V or VMware ........................................................................ 11  
- Upgrade to SEM 6.4 or later across a network share .................................................................................. 12  
- Upgrade the connectors ............................................................................................................................... 13  
  - Upgrade connectors using the SEM console .............................................................................................. 13  
  - Upgrade connectors using the CMC interface ............................................................................................ 13  
- Upgrade the web console ............................................................................................................................ 14  
- Upgrade the reports console ....................................................................................................................... 15  
- Upgrade the agents ....................................................................................................................................... 15  
  - Upgrade agents from the virtual appliance using the SEM console ......................................................... 15  
  - Upgrade SEM agents for Windows using the SEM console ..................................................................... 16  
  - Upgrade SEM agents for Windows using an installer ............................................................................... 16  
- Adjust your Global Automatic Updates setting ......................................................................................... 16
Prepare to upgrade SEM

The Security Event Manager (formerly Log & Event Manager), upgrade process consists of upgrading the SEM appliance and related components: console, agents, and reports.

The SEM 6.7.1 appliance upgrade package upgrades all components of SEM appliances running SEM versions 6.4 through 6.7.1. All previous versions must upgrade to 6.4 before upgrading to 6.7.1.

To upgrade from a pre-6.4 version of SEM (LEM), see Upgrading from prior versions.
Determine your upgrade path to the latest version of SEM

The SEM 6.7.1 appliance upgrade package upgrades SEM appliances running version 6.4 and later. If you need an upgrade package for an earlier version of SEM or TriGeo SIM (no longer supported), open a Customer Support ticket.

The following table lists the full upgrade paths from all prior SEM versions to the latest version.

<table>
<thead>
<tr>
<th>SEM VERSION</th>
<th>UPGRADE PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6*</td>
<td>6.0.1 &gt; 6.2.1 &gt; 6.3.1 &gt; 6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>5.7*</td>
<td>6.0.1 &gt; 6.2.x &gt; 6.3.1 &gt; 6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>6.0*</td>
<td>6.0.1 &gt; 6.2.1 &gt; 6.3.1 &gt; 6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>6.0.1*</td>
<td>6.2.x &gt; 6.3.1 &gt; 6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>6.1**</td>
<td>6.2.x &gt; 6.3.1 &gt; 6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>6.2.x (6.2 or 6.2.1)**</td>
<td>6.3.1 &gt; 6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>6.3.0***</td>
<td>6.3.1 &gt; 6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>6.3.1***</td>
<td>6.4 &gt; 6.7.1</td>
</tr>
<tr>
<td>6.4***</td>
<td>6.7.1</td>
</tr>
<tr>
<td>6.5***</td>
<td>6.7.1</td>
</tr>
<tr>
<td>6.6***</td>
<td>6.7.1</td>
</tr>
<tr>
<td>6.7***</td>
<td>6.7.1</td>
</tr>
</tbody>
</table>

* Reached end of life
** Reached end of engineering
*** Supported version

- Download the latest upgrade media from the SolarWinds Customer Portal under Additional Components in the left pane.
- If you need upgrade media for previous versions, contact SolarWinds Support.
Best practices for SEM upgrades

Most standard SEM deployments upgrade a single virtual appliance. If you have multiple SEM virtual appliances, SolarWinds recommends upgrading these appliances in the following order:

1. Alert database appliances
2. RAW nDepth appliances
3. Manager appliances

If you have a High Availability (HA) system, upgrade the primary appliance first, followed by the secondary appliance. You can upgrade logging servers and network sensors at any time.

The upgrade will overwrite the system partition and cannot be interrupted or undone. SolarWinds recommends exporting (Hyper-V) or taking a snapshot of (vSphere) your SEM virtual appliance before running the upgrade. You can delete the snapshot upon confirmation of a successful upgrade.

Resize the SEM virtual appliance

You can increase the SEM virtual appliance capacity by increasing the SEM virtual appliance size in your hypervisor. This process adds up to 15 minutes to the boot-up process to adjust the file systems.

During the boot-up process, do not turn off or reboot the appliance until the startup is completed. Subsequent bootups and reboots do not require an additional amount of time.

To retain your log data for an extended amount of time, you may need to increase the SEM virtual appliance size. You can increase your SEM virtual appliance capacity by increasing the hard disk size in your VMWare vSphere® or Microsoft® Hyper-V client.

Always shut down the SEM virtual appliance before you reconfigure the vSphere or Hyper-V client disk.

When you increase the size of your virtual appliance, use the following guidelines:

- You can exceed the 2 TB limit with a fresh SEM deployment (for versions 6.4 and later only). If your upgrade path included 6.3.1 and older, please contact Customer Support for assistance.
- The maximum virtualization platform disk size for Hyper-V:
  - VHD - 2TB, for very old Hyper-V only.
  - VHDX (recommended) - 2TB or more is supported.
- After you increase the virtual disk size, you cannot decrease its size using the same methods.
- If you have VM snapshots, you cannot increase the size of your virtual appliance.
Additional considerations for VMware vSphere

If you are running VMware and do not have snapshots, you can edit the VM settings and change the size of the disk. During startup, the virtual appliance recognizes the change in disk size and partitions and adjusts the file systems appropriately. If snapshots are available, the disk size field is disabled.

If you need to increase the size of your virtual appliance, delete all VM snapshots or increase the existing VM by cloning it onto a larger disk. See your vSphere documentation for more information about performing these tasks.
Upgrade SEM: complete steps

When you upgrade your SEM appliances and components, upgrade the SEM appliances first.

Upgrade your SEM appliances and components in the following order:

- Virtual appliances
- Connectors
- Consoles
- Reports console
- Agents

When you perform a SEM upgrade, always reboot the SEM appliances.

SEM upgrade options - Debian upgrade

Upgrade 6.4 and later versions via network SMB share.

Custom changes made on any SEM appliance (by root) will not be preserved after the upgrade. Specifically, any unexpected configuration formats created outside of CMC. For example:

- Iptables custom rules
- Modified scripts
- Added scripts
- Modified chron scheduler

Upgrade the virtual appliances

During this process, the upgrade script disconnects the SEM virtual appliance from all SEM agents and consoles.

1. Prepare the upgrade media.
   a. Download the Upgrade Package for SEM Virtual ZIP file from the SolarWinds Customer Portal.
   b. Unzip the file.
   c. Open the SolarWinds Security Event Manager 6.7.1 Upgrade folder.
   d. Copy the Upgrade folder to a shared network folder (this applies to any SMB share functionality in CMC).

2. Connect to the SEM virtual appliance using the virtual console (vSphere or Hyper-V Manager) or an SSH client (such as PuTTY).
   If you are using an SSH client, use port 22 or 32022, and then log in with your CMC user credentials.

3. Access the CMC prompt.
In vSphere, arrow down to Advanced Configuration, and then press Enter.
In PuTTY, log in using your CMC credentials.

4. At the `cmc>` prompt, enter `upgrade`.
5. Follow the on-screen instructions to complete the SEM appliance upgrade.

During the upgrade, SEM may require a reboot.

Troubleshoot errors during the appliance upgrade
If you encounter errors during the appliance upgrade, review the error message information below before you contact Customer Support.

<table>
<thead>
<tr>
<th>ERROR MESSAGE</th>
<th>RESOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>An error occurred during the upgrade.</td>
<td>Attempt to upgrade again. If the second attempt fails, pull debugging information and open a Customer Support ticket.</td>
</tr>
<tr>
<td>You must upgrade to 6.4 before upgrading to 6.7.1.</td>
<td>See <a href="#">Upgrading from prior versions</a> for the appropriate upgrade procedure.</td>
</tr>
</tbody>
</table>

Prepare and share information with Customer Support
Use the `debug` command on your SEM virtual appliance to pull log files from the appliance to share with Customer Support. These files contain debugging information used by Customer Support to troubleshoot your issue.

Pull debugging information from your SEM virtual appliance

1. Connect to your SEM virtual appliance using the vSphere console view or an SSH client (such as PuTTY).
   If you are using an SSH client, log in to your SEM virtual appliance using your CMC credentials.
2. At the `cmc>` prompt, enter `manager`, and then press Enter.
3. At the `cmc::manager` prompt, enter `debug`, and then press Enter.
4. Follow the prompts on your screen to generate the files.
5. Verify that the script generated the `.tgz` file.
6. Use Samba to share the `.tgz` file with Customer Support.

This file does not contain alert data or other data from your SEM database.
7. Enter `exit` to return to the `cmc>` prompt.
8. Enter `exit` to log out of your SEM virtual appliance.
Upgrade to SEM 6.4 or later using an ISO

From SEM 6.3.1 Hotfix 5 or later, you can upgrade to SEM 6.4 or later to the latest version using an ISO.

During this process, the upgrade script disconnects the SEM virtual appliance from all SEM agents and consoles.

1. Prepare the upgrade media.
   a. Download the Upgrade Package for the SEM ISO image from the SolarWinds Customer Portal.
   b. Mount the ISO image on your hypervisor.
      - Find instructions for mounting the ISO image on Microsoft Hyper-V here.
      - Find instructions for mounting the ISO image on VMware vSphere here.

2. Connect to the SEM virtual appliance using either the virtual console (vSphere or Hyper-V Manager) or an SSH client (such as PuTTY).

   Use port 22 when using an SSH client.

3. Log in with your CMC user credentials.
4. Access the CMC prompt.
5. In vSphere, arrow down to Advanced Configuration, and then press Enter.
6. In PuTTY, log in using your CMC credentials.
7. At the CMC > prompt, enter: upgrade

   ![Command Prompt](image.png)

   Type (i) to install the update from an ISO image mounted in vSphere or Hyper-V, or type (n) to install the update from a network share.

   Is the LEM Manager update located on an ISO image, or is it available on the network? <i/n> i

8. Enter i for ISO, and then follow the prompts.

   After you perform a SEM upgrade, always reboot the SEM appliance.
Mount the ISO image on Microsoft Hyper-V or VMware

Refer to your vendor-provided documentation for additional assistance.

**Microsoft Hyper-V**

1. Right-click the virtual machine and select Settings.
2. In the left pane, select the DVD drive.
3. In the Media pane, click Browse, and then select the ISO image.
4. Click Apply, and then OK.

**VMware vSphere**

1. Start the VMware vSphere Client and log in with administrator privileges.
2. In the left navigation pane, right-click the VM, and then select Edit Settings.
3. In the Virtual Machine Properties window, click CD/DVD Drive 1, and then select your ISO file.
4. In the Device Type section, select Client Device, and then click OK to save the changes.
5. Before you can mount the ISO, the VM needs to be started. To start the VM, right-click the VM, and then select Power > Power On.
6. In the top menu, click the CD-ROM icon, and then select CD/DVD Drive 1 > Connect to ISO image on local disk.
Upgrade to SEM 6.4 or later across a network share

During the upgrade process, the upgrade script disconnects the SEM virtual appliance from all SEM agents and consoles.

1. Prepare the upgrade media.
   a. Download the Upgrade Package for SEM Virtual Appliance ZIP file from the SolarWinds Customer Portal.
   b. Place the upgrade folder on the network share drive.

   The upgrade network path should look similar to: \\server-IP\\SEM.

2. Connect to the SEM virtual appliance using either the virtual console (vSphere or Hyper-V Manager) or an SSH client (such as PuTTY).

   Use port 22 when using an SSH client.

3. Log in with your CMC user credentials.
4. Access the CMC prompt.
5. In vSphere, arrow down to Advanced Configuration, and then press Enter.
6. In PuTTY, log in using your CMC credentials.
7. At the CMC > prompt, enter: upgrade

![10.199.129.30 - PuTTY]

   [ appliance ] Network, System
   [ manager ] Upgrade, Debug
   [ service ] Restrictions, SSH, Snort
   [ ndepth ] nDepth Configuration/Maintenance
   [ upgrade ] Upgrade this Appliance
   [ admin ] Run Admin UI (for better usability browse https://10.199.129.30/mvc/configuration)
   [ import ] Import a file that can be used from the Admin UI
   [ help ] display this help
   [ exit ] Exit

   SolarWinds SEM Upgrade
   Checking disk space before upgrading...

   /usr/local 43% (1.2G/3.0G) 160000 KB 1679620 KB
   /var 13% (20G/234G) 100000 KB 203505760 KB
   /tmp 5% (231M/5.9G) 100000 KB 5587260 KB

   done.

   Type (i) to install the update from an ISO image mounted in vSphere or Hyper-V, or type (n) to install the update from a network share.

   Is the IEM Manager update located on an ISO image, or is it available on the network? <i/n> [n]

8. Enter n for network, and then follow the prompts.

   After you perform a SEM upgrade, always reboot the SEM appliance.
Upgrade the connectors

Beginning in SEM 6.2.0, you can upgrade your connectors using the SEM console. For versions prior to 6.2.0, update your connectors using the CMC command interface.

Upgrade connectors using the SEM console

1. In the SEM console toolbar, navigate to Manage > Appliances.
2. In the upper right side of the Appliances view, click the Connector Updates drop-down list and select Update now.
   A confirmation message appears indicating the update was applied successfully.

Upgrade connectors using the CMC interface

1. Download the current Connector Update package from the SEM Additional Components page located on the SolarWinds Customer Portal.
   The download requires approximately 3.6 MB of disk space.
2. Prepare the update package.
   a. Unzip the Connector Update Package file.
      The directory structure uses approximately 100 MB of disk space.
   b. Open the SolarWinds-SEM-Connectors folder.
   c. Copy the SEM folder to the root of a network share.
      For example: \\<server-IP>\<share-name>
      The connector locates the SEM directory under the root of the share.
3. Connect to the SEM virtual appliance using a virtual console or SSH client.
4. Access the cmc> prompt.
   If you are using a virtual console, scroll down to Advanced Configuration, and then press Enter.
   If you are using an SSH Client, log in using your CMC credentials.
5. Update the connectors.

- At the **cmc>** prompt, enter `manager`.
- At the **cmc::manager** prompt, enter `sensortoolupgrade`.
- Press Enter to begin the upgrade process.
- Enter your Windows destination share. For example: `\server\share:\share\folder\`
- When prompted (see below), enter your user name and password.
  - Please enter the username, including any domain information (e.g. `DOMAIN\user`):
  - Please enter the password:

6. Verify that the configured connectors restart after the update by monitoring the SEM console and searching for `InternalToolOnline` events in the default SolarWinds events filter.

7. When the update is completed, enter `exit` twice to exit the CMC interface.

### Upgrade the web console

Upgrading the SEM appliance automatically updates the SEM web console. During the upgrade, you may be reconnected automatically. To ensure you are running the latest web console version, you can:

- Refresh the console in your browser
- Close the console, reopen your browser, and reconnect
Upgrade the reports console

After you upgrade the SEM virtual appliance, upgrade the SEM reports application so it is compatible with the web or desktop console. Previously-scheduled reports will not run until you upgrade the reports application to the latest version. This is especially important when using Windows 8 and later operating systems.

SEM Reports version 6.4 is the latest version and also works with SEM 6.5 through 6.7.1.

1. Open the Reports folder from your unzipped upgrade download.
2. Copy setup.exe to the local drive on your Reports computer.

   The security settings in some Windows operating systems require the installer to be on the local hard drive prior to the launch.

3. Log in to the Reports computer.
4. Right-click setup.exe and select Launch to run as administrator.
5. Complete the installation wizard.

   If you are installing the update on systems running Microsoft Windows 8.1, Windows 10, or Windows 2012 R2, include Windows 7 compatibility for the installation.

Upgrade the agents

To take advantage of new enhancements such as Java Runtime Environment (JRE) and infrastructure updates, be sure to upgrade the SEM agents.

If you selected the Enable Global Automatic Updates check box when you adjusted your Global Automatic Update setting, your SEM agents will update automatically. If you did not enable global automatic updates, you can manually upgrade the SEM agents by accessing the installer through the SEM console or using an installer downloaded directly from the SolarWinds Customer Portal.

Upgrade agents from the virtual appliance using the SEM console

Manually pushing agent upgrades from the virtual appliance is the fastest, easiest way to manually upgrade agents.

1. On the SEM console toolbar, click Manage, and then select Nodes.
2. In the Nodes pane, select the SEM agent to upgrade.

   Press and hold <Ctrl> to select more than one agent.

3. From the Remote Updates drop-down list, select Update.

   An Update Status icon for your selected agent opens, indicating the update procedure.
When the update is complete, the Update Status icon changes back to the green Updated icon and displays the new agent version.

A SEM agent upgrade does not require you to reboot the host computer.

Upgrade SEM agents for Windows using the SEM console

If your console is connected to the Internet, you can update your SEM agents through the SEM console.

1. On the SEM console toolbar, click Manage, and then select Nodes.
2. Click Add Node, and then select Agent node.
3. Select the appropriate installation type.
   - Select Remote Installation to push SEM agents to Microsoft Windows hosts across your network.
   - Select Local Installation to log in to the device and install the SEM agent.
4. Copy the setup.exe file to the local hard drive on the computer.

   The security settings in some Windows operating systems require the installer to be on the local hard drive prior to the launch.

5. Right-click the installer, select Run as Administrator, and then complete the installation wizard.

Upgrade SEM agents for Windows using an installer

If your console is not connected to the Internet, you can update your SEM agents by downloading the agent installer from another computer with an Internet connection. Install your new SEM agents in the same folder as your existing SEM agents. This process allows the installer to update the SEM agent software while maintaining all other configuration settings.

1. Download the agent installer from the Additional Components page on the SolarWinds Customer Portal.
2. Extract the ZIP file contents to your desktop or another location.
3. Copy the SolarWinds-SEM-6.7.1-Agent-WindowsInstaller.exe file to the local hard drive on the computer.

   The security settings in some Windows operating systems require the installer to be on the local hard drive prior to the launch.

4. Right-click setup.exe, select Run as Administrator, and then complete the installation wizard.

Adjust your Global Automatic Updates setting

Before you upgrade your SEM appliance, ensure that the Global Automatic Updates setting for your SEM agents is configured correctly. When enabled, agent upgrades occur automatically when available. Disable this option if change management or other testing is required for agent upgrades.
1. Open the SEM console and authenticate to the SEM manager.
2. Click Manage and select Appliances.
3. Click the Settings tab in the Properties pane.
4. Select or clear the Enable Global Automatic Updates check box according to your preferences.
5. Click Save.
   
   The Remote Updates setting is updated.