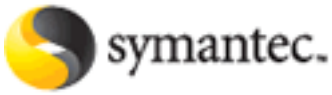

Symantec Control Compliance Suite Vulnerability Manager Software Installation Guide

Document version 2.3

Contents

Revision history

The current document version is 2.3

Revision Date	Version	Description
November 11, 2009	2.0	Verified, tested, and updated installation procedures. Updated document template.
November 25, 2009	2.1	Updated lists of required packages for Linux and instructions for using md5sum.
December 3, 2009	2.2	Updated system requirements.
March 8, 2009	2.3	Added note recommending 64-bit configuration.

About this guide

Use this guide to help you to perform three tasks:

- installing the Windows or Linux version of Symantec Control Compliance Suite Vulnerability Manager software
- starting Symantec Control Compliance Suite Vulnerability Manager
- logging on to the Symantec Control Compliance Suite Vulnerability Manager Console Web interface, with which you can perform all Symantec Control Compliance Suite Vulnerability Manager functions

Document conventions

Words in bold typeface are names of hypertext links and controls.

Words in italics are document titles, chapter titles, and names of Web and GUI interface pages.

Procedural steps appear in a blue sans serif typeface.

```
Command examples appear in the Courier typeface in shaded boxes.
```

Generalized file names in command examples appear between box brackets. Example: `[installer_file_name]`

Multiple options in commands appear between arrow brackets: Example: `$ /etc/init.d/[daemon_name] <start|stop|restart>`

NOTES appear in shaded boxes.

Using the Help site and other documents

After you start Symantec Control Compliance Suite Vulnerability Manager and log on to the Symantec Control Compliance Suite Vulnerability Manager Console Web interface, use the Help site by clicking the **Help** link that appears on any page of the interface. The site provides information on how to perform all Symantec Control Compliance Suite Vulnerability Manager functions:

- learning important Symantec Control Compliance Suite Vulnerability Manager concepts and terms
- setting up sites and scans
- running scans
- creating and running reports
- viewing vulnerabilities and excluding specific vulnerabilities from reports
- creating tickets
- creating and modifying scan templates
- creating user accounts
- creating asset groups

- configuring various Symantec Control Compliance Suite Vulnerability Manager settings
- maintaining and troubleshooting Symantec Control Compliance Suite Vulnerability Manager
- backing up and restoring the Symantec Control Compliance Suite Vulnerability Manager database

You will also find useful the document *Best Practices for Planning and Executing a Symantec Control Compliance Suite Vulnerability Manager Deployment*. You can download it from the *Support* page in Symantec Control Compliance Suite Vulnerability Manager Help.

About Symantec Control Compliance Suite Vulnerability Manager

Reading this section will help you to understand the components that you are about to install.

Understanding what Symantec Control Compliance Suite Vulnerability Manager does

Symantec Control Compliance Suite Vulnerability Manager is a unified vulnerability solution that scans networks to identify the devices running on them and to probe these devices for vulnerabilities. It analyzes the scan data and processes it for reports. You can use these reports to help you assess your network security at various levels of detail and remediate any vulnerabilities quickly.

The vulnerability checks in Symantec Control Compliance Suite Vulnerability Manager identify security weaknesses in all layers of a network computing environment, including operating systems, databases, applications, and files. Symantec Control Compliance Suite Vulnerability Manager can detect malicious programs and worms, identify areas in your infrastructure that may be at risk for an attack, and verify patch updates and security compliance measures.

Understanding Symantec Control Compliance Suite Vulnerability Manager components

Symantec Control Compliance Suite Vulnerability Manager consists of two main components:

- **Symantec Control Compliance Suite Vulnerability Manager Scan Engines** perform asset discovery and vulnerability detection operations. You can deploy scan engines outside your firewall, within your secure network perimeter, or inside your DMZ to scan any network *asset*.

DEFINITION: An asset is a device on your network that is identified by an IP address, such as a computer, router, or printer. Assets are what Symantec Control Compliance Suite Vulnerability Manager scans. In the Symantec Control Compliance Suite Vulnerability Manager Console Web interface, the words "asset" and "device" are used interchangeably. In some of Symantec Control Compliance Suite Vulnerability Manager's report templates, assets are referred to as "nodes".

- The **Symantec Control Compliance Suite Vulnerability Manager Console** communicates with Symantec Control Compliance Suite Vulnerability Manager Scan Engines to start scans and retrieve scan information. All exchanges between the console and scan engines occur via encrypted SSL sessions over a dedicated TCP port that you can select. For better security and performance, scan engines do not communicate with each other; they only communicate with the console.

  When Symantec Control Compliance Suite Vulnerability Manager scans an asset for the first time, the console creates a repository of information about that asset in its database. With each ensuing scan that includes that asset, the console updates the repository.

  The console includes a Web-based interface for configuring and operating Symantec Control Compliance Suite Vulnerability Manager. An authorized user can log on to this interface securely, using HTTPS, to perform any Symantec Control Compliance Suite Vulnerability Manager-related task that his or her role permits. See the section titled *Understanding user roles and permissions* in the *Symantec Control Compliance Suite Vulnerability Manager Manual* or Help. The authentication database is stored in an encrypted format on the console server, and passwords are never stored or transmitted in plain text.

  Other console functions include generating user-configured reports and regularly downloading patches and other critical updates from the Symantec central update system.

Symantec Control Compliance Suite Vulnerability Manager requirements

Make sure that your host hardware and network support Symantec Control Compliance Suite Vulnerability Manager operations.

Hardware requirements

A computer hosting Symantec Control Compliance Suite Vulnerability Manager components should have the following configuration:

Symantec Control Compliance Suite Vulnerability Manager	
server	dedicated server with no IPS, IDS, or virus protection
processor	2 GHz
RAM	2 GB (32-bit), 8 GB (64-bit)
disk space	80 GB + for a console/scan engine combination; 10 GB + for a scan engine only
network interface card (NIC)	100 Mbps

NOTE: The 64-bit configuration is recommended for enterprise-scale deployments. For smaller deployments, the 32-bit configuration may be sufficient.

Network activities and requirements

The Symantec Control Compliance Suite Vulnerability Manager Console communicates over the network to perform four major activities:

Activity	**Type of communication**
manage scan activity on Symantec Control Compliance Suite Vulnerability Manager Scan Engines and pull scan data from them	outbound; scan engines listen on 40814
download vulnerability checks and feature updates from a server at updates.rapid7.com	outbound; server listens on port 80
upload PGP-encrypted diagnostic information to a server at symantec.com	outbound; server listens on port 443
provide Web interface access to Symantec Control Compliance Suite Vulnerability Manager users	inbound; console accepts HTTPS requests over port 3780

Symantec Control Compliance Suite Vulnerability Manager Scan Engines contact target assets using TCP, UDP, and ICMP to perform scans. Scan engines do not not initiate outbound communication with the Symantec Control Compliance Suite Vulnerability Manager Console.

Ideally there should be no firewalls or similar devices between a scan engine and its target assets. These devices interfere with the scanning process and can limit the accuracy of results. Scanning may also require some flexibility in security policies. For more information, see the guide *Best Practices for Planning and Executing a Symantec Control Compliance Suite Vulnerability Manager Deployment*.

Officially supported platforms

Symantec Control Compliance Suite Vulnerability Manager has been tested on the following platforms:

Windows

- MS Windows Server 2003 SP2 / Server 2003 R2 (64-bit)

NOTE: Symantec does not support installation on Windows XP because of an issue related to this operating system sending packets over raw sockets.

Linux

- Red Hat Enterprise Linux 5.4

Unofficially supported platforms

Symantec Control Compliance Suite Vulnerability Manager is also known to run on other platforms, but Symantec does not officially support these.

Windows

- MS Windows Server 2003 SP1

Linux

- SUSE Enterprise Linux 9
- Red Hat Enterprise Linux 4
- Fedora 9 or later
- Debian 4.0 or later
- CentOS 4 or later
- Ubuntu 7.10 or later

NOTE: For HTML reporting on Linux, you must have an X Windows server installed or the X Virtual Frame Buffer (Xvfb) must be running.

Making sure you have necessary installation items

Make sure you have the following items, which are necessary for installation:

- Symantec Control Compliance Suite Vulnerability Manager installers for all supported environments in 32-bit and 64-bit versions (.bin files for Linux and .exe files for Windows)
- the md5sum, which helps to ensure that installers are not corrupted during download
- documentation, including this guide
- a product key, which you will use to activate your Symantec Control Compliance Suite Vulnerability Manager license during installation

If you do not have any of these items, contact your Symantec account representative.

Installing Symantec Control Compliance Suite Vulnerability Manager in Windows environments

You must have local administrator rights in order to install Symantec Control Compliance Suite Vulnerability Manager on a Windows host. The computer cannot be part of a domain and cannot have a local firewall running. Installation on a Windows domain controller is not supported.

1. Double-click the icon for the Symantec Control Compliance Suite Vulnerability Manager installer.
2. The installer displays the Symantec Control Compliance Suite Vulnerability Manager InstallShield Wizard. Click **Next** on the *Welcome* page.
3. The installer displays the end-user license agreement. Read it, and select the option for accepting the terms.
4. The installer displays the default installation directory, which is C:\Program Files\Symantec\CCSVM. Click **Next** to accept the default.

   OR

   If you want to use a different directory, delete the default directory, and type the preferred path in the text box. Then, click **Next**.

   OR

   Click **Browse** to open an explorer and locate a preferred directory. When you find that directory, click **Open** in the explorer. The path appears in the **Directory Name** text box of the installer wizard. Note the directory you selected. Click **Next**.
5. The installer displays two options for an installation type. If you want to install a Symantec Control Compliance Suite Vulnerability Manager Console that includes a Symantec Control Compliance Suite Vulnerability Manager Scan Engine, select the **Typical** option. If you want to install the Symantec Control Compliance Suite Vulnerability Manager Scan Engine only, select the second option. For information about these options, see *Understanding Symantec Control Compliance Suite Vulnerability Manager components* (on page 5).
6. The installer displays a request for a product key, which you received from Symantec. See *Making sure you have necessary installation items* (on page 9). Enter the product key. You will not be able to complete the installation without a product key. If you do not have one, contact your Symantec account representative. After you enter the product key, click **NEXT**.
7. The installer displays a request for your name and company name. Symantec Control Compliance Suite Vulnerability Manager includes this information when sending logs to Symantec Technical Support for troubleshooting. Enter the names, and click **NEXT**.
8. The installer displays a summary of installation details. If you want to change any details, click **Back** to go to the desired wizard page, make the change, and then return to the summary. When you approve of the installation details, click **Install**.

   The installer displays a status bar and names of files that it is installing.

9. The installer displays a request for a user name and password. These will be the credentials for the Symantec Control Compliance Suite Vulnerability Manager global administrator account. If you wish to change the user name from the default "vmadmin", type a new name.
10. Type a password, and retype it for confirmation.

    Symantec Control Compliance Suite Vulnerability Manager does not support recovery of credentials. If you forget your user name or password, you will have to reinstall Symantec Control Compliance Suite Vulnerability Manager. Credentials are case-sensitive.

NOTE: You can change these credentials later in Symantec Control Compliance Suite Vulnerability Manager. See Symantec Control Compliance Suite Vulnerability Manager Help or the *Symantec Control Compliance Suite Vulnerability Manager Manual* for more information.

11. Click **Finish**.
12. The installer displays a success message. Click **Finish**.

Starting Symantec Control Compliance Suite Vulnerability Manager in Windows

1. To start the console in Windows, double-click the Symantec Control Compliance Suite Vulnerability Manager Console server icon on the desktop:

   

   If the icon isn't available, you can double-click the `nsc.bat` file to start the console. The file is located in the installation directory.

   The startup process may take a few minutes the first time you start the console because Symantec Control Compliance Suite Vulnerability Manager is initializing its database of vulnerabilities. You may log on to the Symantec Control Compliance Suite Vulnerability Manager Console Web interface immediately after Symantec Control Compliance Suite Vulnerability Manager has completed the startup process.

Making Symantec Control Compliance Suite Vulnerability Manager start automatically when Windows starts

You can make Symantec Control Compliance Suite Vulnerability Manager start automatically as a service when Windows starts. This eliminates the need for you start it manually.

1. Click the Windows **Start** button, and select **Run...**
2. In the *Run* dialog box, type `services.msc`, and click **OK**.
3. In the *Services* pane, double-click the icon for the Symantec Control Compliance Suite Vulnerability Manager Console service.
4. From the drop-down list for **Startup type:** select "Automatic", and click **OK**.
5. Close *Services*.
6. Restart your computer. Symantec Control Compliance Suite Vulnerability Manager starts automatically as a service.

Removing Symantec Control Compliance Suite Vulnerability Manager from Windows

Each instance of Symantec Control Compliance Suite Vulnerability Manager must be installed from scratch. If you need to reinstall Symantec Control Compliance Suite Vulnerability Manager, you must first remove it. Multiple copies of the same instance of Symantec Control Compliance Suite Vulnerability Manager on the same server will not function correctly and are not supported.

1. Stop the Symantec Control Compliance Suite Vulnerability Manager server: Go to the Symantec Control Compliance Suite Vulnerability Manager command prompt, type `quit`, and press **ENTER.**
2. Make sure that the Symantec Control Compliance Suite Vulnerability Manager PostgreSQL server is no longer running: Open the Windows Command Prompt, and type `net stop nxpgsql`. If the service is still running, this command will stop it. Otherwise, the system will display a message that the service is no longer running.
3. Click the Windows **Start** button, and select **Run...**
4. In the *Run* dialog box, type `regedit`, and click **OK**.
5. In the Registry Editor, open the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ folder.
6. Delete the NeXposeConsole and nxpgsql folders.
7. Restart the computer.
8. Delete the Symantec Control Compliance Suite Vulnerability Manager installation folder.

Installing Symantec Control Compliance Suite Vulnerability Manager in Linux environments

You must have root privileges to install Symantec Control Compliance Suite Vulnerability Manager. You can log on as root, begin each command with `sudo`, or run `sudo -i`.

Ensuring that the Symantec Control Compliance Suite Vulnerability Manager Linux installer file is not corrupted

Symantec recommends this step to prevent installation problems. You will need the md5sum file as described in *Making sure you have necessary installation items* (on page 9).

1. Go to the directory that contains the Symantec Control Compliance Suite Vulnerability Manager installer and the md5sum file.
2. Run the md5sum program with the -c option to check the MD5 checksum:

```
$ md5sum -c [installer_file_name].md5sum
```

3. If this command returns an "OK" message, the file is valid. If it returns a "FAILED" message, obtain the installer and md5sum file from Symantec again, and repeat this procedure.

Installing Symantec Control Compliance Suite Vulnerability Manager in a Red Hat environment

These steps apply to Red Hat 5.4. There may be some variation on other versions of Red Hat.

Make sure you have downloaded all items necessary for installation. See *Making sure you have necessary installation items* (on page 9).

You need a Red Hat Enterprise Linux license in order to install Symantec Control Compliance Suite Vulnerability Manager.

Manually installing necessary packages in Red Hat

You need yum and RPM to install packages on Red Hat.

To verify that you have yum, run:

```
$ yum --version
```

To verify that you have RPM, run:

```
$ rpm -v
```

To determine if you have a required package and install it as necessary, run:

```
$ yum install [package_name]
```

The following packages must be installed:

- compat-libstdc++-33.i386 (32-bit only)
- screen

Ensuring that SELinux is disabled

SELinux is a security-related feature that must be disabled before you can install Symantec Control Compliance Suite Vulnerability Manager.

1. Open the SELinux configuration file in your preferred text editor, for example:

```
$ vi /etc/selinux/config
```

2. Go the line that begins with `SELINUX=`
3. If the setting is `enabled`, change it to `disabled`:

```
SELINUX=disabled
```

4. Save and close the file.
5. Restart the server for the change to take effect:

```
$ shutdown -r now
```

Running the Symantec Control Compliance Suite Vulnerability Manager installer in Red Hat

After making sure that the required Linux packages are installed, take the following steps.

1. Go to the directory containing the Symantec Control Compliance Suite Vulnerability Manager installer.
2. Change the pemisrsions for the installation file to make it executable:

```
$ chmod +x [installation_file_name]
```

3. Start the Symantec Control Compliance Suite Vulnerability Manager installer:

```
$ ./[installation_file_name] –console
```

NOTE: If you are using a desktop interface such as KDE or Gnome, omit the –console flag. For the rest of the installation, follow the directions that appear in the interface display.

4. The installer displays a message that it will install Symantec Control Compliance Suite Vulnerability Manager. Press **1** and then **ENTER** to continue.
5. The installer displays the end-user license agreement. Read each displayed section and press **ENTER** to continue.
6. At the end of the agreement, press **1** to accept the terms. Then press **0** to continue.
7. Press **1**, and then press **ENTER** to proceed to the next step.
8. The installer displays the default installation directory. Press **ENTER** to accept the default, or type a different directory, and then press **ENTER**.

NOTE: Make sure to note the installation directory.

9. Press **1**, and then press **ENTER** to proceed to the next step.

10. The installer displays two options for an installation type. If you want to install a Symantec Control Compliance Suite Vulnerability Manager Console that includes an Symantec Control Compliance Suite Vulnerability Manager Scan Engine, press **1** for the "Typical" option. If you want to install the Symantec Control Compliance Suite Vulnerability Manager Scan Engine only, press **2**. For information about these options, see *Understanding Symantec Control Compliance Suite Vulnerability Manager components* (on page 5).
11. Press **1**, and then press **ENTER** to proceed to the next step.
12. The installer displays a request for a product key, which you received from Symantec. See *Making sure you have necessary installation items* (on page 9). Type the product key. You will not be able to complete the installation without a product key. If you do not have one, contact your Symantec account representative. After you type the product key, press **ENTER**.

NOTE: You must enter the key with hyphens. The key is not case-sensitive.

13. Press **1**, and then press **ENTER** to proceed to the next step.
14. The installer displays a request for your name. Type it, and press **ENTER**.
15. The installer displays a request for your company name. Type it, and press **ENTER**.
16. Press **1**, and then press **ENTER** to proceed to the next step.
17. The installer displays details about the installation. Review them, and press **1** to continue. The installer displays the percent of the installation that has been completed.
18. After the installation is complete, the installer displays a request for a user name for the Symantec Control Compliance Suite Vulnerability Manager global administrator account. Press **ENTER** to accept the default name "vmadmin", or type a different name, and then press **ENTER**.
19. The installer displays a request for a password. Type a password, and then press **ENTER**. Type the password again to confirm it, and press **ENTER**.

    Symantec Control Compliance Suite Vulnerability Manager does not support recovery of credentials. If you forget your user name or password, you will have to reinstall Symantec Control Compliance Suite Vulnerability Manager. Credentials are case-sensitive.

NOTE: You can change these credentials later in Symantec Control Compliance Suite Vulnerability Manager. See Symantec Control Compliance Suite Vulnerability Manager Help or the *Symantec Control Compliance Suite Vulnerability Manager Manual* for more information.

20. The installer displays a message that the installation is complete. Press **3**.
21. The installer displays a message that it is executing the DBInitializer. After this process finishes, press **3** to complete the installation and exit the installer.

Starting Symantec Control Compliance Suite Vulnerability Manager in Red Hat

1. Make sure that you are in the Symantec Control Compliance Suite Vulnerability Manager installation directory, which you selected during installation. See *Running the Symantec Control Compliance Suite Vulnerability Manager installer in Red Hat* (on page 14).
2. Go to the directory containing the script that starts Symantec Control Compliance Suite Vulnerability Manager:

```
$ cd [installation_directory]/nsc
```

3. Type the command to run the script:

```
$ ./nsc.sh
```

The startup process may take a few minutes, especially the first time you start the console, since Symantec Control Compliance Suite Vulnerability Manager is initializing its database of vulnerabilities. You may log on to the Symantec Control Compliance Suite Vulnerability Manager Console interface immediately after Symantec Control Compliance Suite Vulnerability Manager has completed the startup process.

Installing Symantec Control Compliance Suite Vulnerability Manager as a daemon in Red Hat

Installing Symantec Control Compliance Suite Vulnerability Manager as a daemon has two benefits: Symantec Control Compliance Suite Vulnerability Manager can automatically start when the server starts, and it will continue running even if the current user logs off.

1. Go to the directory that contains the nexposeconsole.rc file:

```
$ cd [installation_directory]/nsc
```

2. Open the nexposeconsole.rc file in your preferred text editing program.
3. Look for two consecutive lines that read:

```
#defines
NXP_ROOT=/opt/Symantec/CCSVM
```

   The directory in the second line is the default installation directory.

4. If you did not use the default directory for installation, change the directory path to the one you chose:

```
#defines
NXP_ROOT=[installation_directory]
```

5. Save and close the nexposeconsole.rc file.
6. Copy the nexposeconsole.rc file to the /etc/init.d directory, and give it the desired daemon name:

```
$ cp [installation_directory]/nexposeconsole.rc /etc/init.d/[daemon_name]
```

7. Ensure that the daemon can run:

```
$ chmod +x /etc/init.d/[daemon-name]
```

8. Make the daemon start when the operating systems starts:

```
$ chkconfig --add [daemon_name]
```

Manually starting, stopping, or restarting Symantec Control Compliance Suite Vulnerability Manager as a daemon in Red Hat

To manually start, stop, or restart Symantec Control Compliance Suite Vulnerability Manager as a daemon:

```
$ /etc/init.d/[daemon_name] <start|stop|restart>
```

Preventing the daemon from automatically starting with the host system in Red Hat

To prevent the Symantec Control Compliance Suite Vulnerability Manager daemon from automatically starting when the host system starts:

```
$ chkconfig -del [daemon_name]
```

Removing Symantec Control Compliance Suite Vulnerability Manager in Red Hat

Each instance of Symantec Control Compliance Suite Vulnerability Manager must be installed from scratch. If you need to reinstall Symantec Control Compliance Suite Vulnerability Manager, you must first remove it. Multiple copies of the same instance of Symantec Control Compliance Suite Vulnerability Manager on the same server will not function correctly and are not supported.

To remove Symantec Control Compliance Suite Vulnerability Manager:

```
$ rm -fr [installation_directory]
```

NOTE: Be careful to enter this command exactly as it appears.

Logging on to Symantec Control Compliance Suite Vulnerability Manager

1. Start a Web browser. The Symantec Control Compliance Suite Vulnerability Manager Console Web interface supports Microsoft Internet Explorer 7.x and Firefox 3.5 browsers. Other browsers may operate successfully with the interface.
2. If you are running the browser on the same computer as the console, go to the IP address 127.0.0.1, and specify port 3780. Make sure to indicate HTTPS protocol when entering the URL.

   Example: `https://127.0.0.1:3780`

NOTE: If there is a usage conflict for port 3780, you may specify another available port in the XML file [installation_directory]nsc\conf\httpd.xml. You also can switch the port after you log on. See *Managing Symantec Control Compliance Suite Vulnerability Manager Console settings* in the *Symantec Control Compliance Suite Vulnerability Manager Manual* or Help.

If you are running the browser on a separate computer, substitute `127.0.0.1` with the correct host name IP address.

NOTE: Browsers do not include non-English, UTF-8 character sets, such as those for Chinese languages, in their default installations. To use your browser with one of these languages, you must install the appropriate language pack. In the Windows version of Internet Explorer 7.0, you can add a language by selecting **Internet Options** from the *Tools* menu, and then clicking the **Languages** button in the *Internet Options* dialog box. In the Windows version of Firefox 2.0, select **Options** from the *Tools* menu and then clicked the **Advanced** icon in the *Options* dialog box. In the Languages pane, click **Choose...** to select a language to add.

3. When your browser displays the *Log in* box, enter your user name and and password that you specified during installation. Click the **Login** button. User names and passwords are case-sensitive and non-recoverable.

NOTE: If the logon box indicates that the Symantec Control Compliance Suite Vulnerability Manager Console is in maintenance mode, then either an error has stopped the system from starting properly, or a scheduled task has initiated maintenance mode. See the topic *Running Symantec Control Compliance Suite Vulnerability Manager in maintenance mode* in the Symantec Control Compliance Suite Vulnerability Manager Manual or Help.

If the console displays a warning about authentication services being unavailable, and your network uses an external authentication source such as LDAP or Kerberos, your Symantec Control Compliance Suite Vulnerability Manager global administrator must check the configuration for that source. See *Using external sources for user authentication* in Help. The problem may also indicate that the authentication server is down.

The first time you log on to the console, you will see the *News* page, which lists all updates and improvements in the installed Symantec Control Compliance Suite Vulnerability Manager system, including new vulnerability checks. If you do not wish to see this page every time you log on to Symantec Control Compliance Suite Vulnerability Manager after an update, clear the check box for automatically displaying this page after every login. You can always view the *News* page by clicking the **News** link that appears in a row near the top right corner of every page of the console interface.

4. Click the **Home** link to view the Symantec Control Compliance Suite Vulnerability Manager Console *Home* page.
5. Click the **Help** link on any page of the Web interface for information on how to use Symantec Control Compliance Suite Vulnerability Manager.