CHAPTER 5

# Additional Installation-Related Information

This section contains the following topics:



## Enabling or Disabling Cisco WebEx Social Nodes

You use the Topology window in the Director to enable and disable App Server, Cache, and Worker nodes in your Cisco WebEx Social cluster.

Some requirements exist regarding the order in which you must enable or disable nodes:

- When enabling nodes, App Server roles must be enabled after all other roles are enabled. The order of other roles does not matter.
- When disabling nodes, all App Server roles must be disabled first. After that, the order does not matter.

To enable or disable nodes in your Cisco WebEx Social cluster, follow these steps:

**Procedure**

**Step 1** Sign in to the Director with your administrator user ID and password.

**Step 2** Click **System** in the Menu bar, then click **Topology** in the left panel.

**Step 3** In the Server List area, use the **Enable** and **Disable** options in the Action drop-down menu to start or stop a node (role).

You also can click the **Enable All** button in the Server List area to enable all disabled Cache, Worker, and App Server nodes, in that order. You can click the **Disable All** button in this area to disable all enabled App Server, Worker, and Cache nodes, in that order

# Using Refresh Buttons

The Server List area in the System > Topology window in the Director contains **Refresh All** button, and the Action drop-down menu next to each node includes the **Refresh** option. Use the **Refresh All** button or the **Refresh** option to fetch version information and to display current operational status of nodes. States that the Status column shows are:

- Running
- Stopped
- Not Installed
- Unreachable Host
- Connection Failed

# Verifying the Integrity of a Cisco WebEx Social .img File

The Cisco WebEx Social .img file that you use for an upgrade is a large file, which can occasionally become corrupted when you download it from Cisco.com. Cisco recommends that you verify the integrity of a .img file before you use it. To do so, you obtain an MD5 checksum value that Cisco calculates for the file, then compare that value with an MD5 checksum value that you calculate for the file. An MD5 checksum is a unique 128-bit value that you can use to ensure that various versions of a file are identical.

Verifying the integrity of a .img file is a two-step process, which the following sections describe:

- Obtaining an MD5 Checksum Value from Cisco, page 5-2
- Performing an MD5 Checksum Comparison, page 5-3

## Obtaining an MD5 Checksum Value from Cisco

The first general step to verify the integrity of a Cisco WebEx Social .img file is to obtain an MD5 checksum value for the file from Cisco. To obtain this value, follow these steps:

**Procedure**

**Step 1** Go to http://www.cisco.com.

**Step 2** Click **Support**, then click the **Downloads** tab.

**Step 3** Type **webex social** in the Find field, then click the **Find** button.

**Step 4** Click the **Cisco WebEx** Social link that appears in the search results.

**Step 5** In the panel on the left of the Download Software window that appears, navigate to the Cisco WebEx Social version that you are installing.

**Step 6** Hover your mouse over the .img file name that appears to display the Details window.

**Step 7** Make a note of the MD5 Checksum value that appears in the Details window.

# Performing an MD5 Checksum Comparison

After you download the .img file, perform a checksum comparison by generating an MD5 checksum value for the file and comparing this value with the checksum value that you obtained from Cisco. To do so, follow the steps in the section that is appropriate for the system to which you downloaded the .img file:


- Performing an MD5 Checksum Comparison on a Microsoft Windows System, page 5-3
- Performing an MD5 Checksum Comparison on a Mac System, page 5-4
- Performing an MD5 Checksum Comparison on a Linux System, page 5-4


## Performing an MD5 Checksum Comparison on a Microsoft Windows System

After you download a .img file and obtain its MD5 checksum value from Cisco (see the "Obtaining an MD5 Checksum Value from Cisco" section on page 5-2), follow these steps to perform an MD5 checksum comparison on a system that is running the Microsoft Windows operating system.

### Before You Begin

- Identify the name of the .img file that you downloaded from Cisco.com and the directory in which you saved the file on the local system.
- Install the Microsoft File Checksum Integrity Verifier (FCIV) utility that is required to perform an MD5 checksum, if this utility is not installed on your system. To do so, follow the instructions in the Microsoft knowledge base article *How to Compute the MD5 or SHA-1 Cryptographic Hash Values for a file*, which is available from the Microsoft website (article ID 889768).

### Procedure

**Step 1** Click the Windows **Start** button, choose **Run**, type **cmd** in the Run window, and press **Enter**.

**Step 2** In the Command window, use the **cd** command to make the directory in which you saved the .img file the current directory.

**Step 3** Enter the following command, replacing the sample file name shown with the name of the .img file that you downloaded:

**FCIV -md5 cisco-webex-social-*X.Y.Z.AAAAA.BBB*.img**

This command displays output that includes an MD5 checksum value, similar to the following example. In this example, the checksum value is shown in bold type for your reference:

```
1. C:\>fciv -md5 md5sum cisco-webex-social-3.0.1.10305.39.img
//
// File Checksum Integrity Verifier version 2.05.
//
88a5dba53661da5dcd37f81011201933  cisco-webex-social-3.0.1.10305.39.img
```

**Step 4** Compare the MD5 checksum value that you generated for the file with the MD5 checksum value that you obtained from Cisco as described in the "Obtaining an MD5 Checksum Value from Cisco" section on page 5-2.

If the checksum values are identical, the .img file that you downloaded is OK to use for an installation or upgrade of Cisco WebEx Social.

If the checksum values are not identical, .img file that you downloaded is corrupt. In this case, download the file from Cisco.com again and rerun the procedure in this section.

## Performing an MD5 Checksum Comparison on a Mac System

After you download a .img file and obtain its MD5 checksum value from Cisco (see the "Obtaining an MD5 Checksum Value from Cisco" section on page 5-2), follow these steps to perform an MD5 checksum comparison on a system that is running an Apple Mac operating system.

### Before You Begin

- Identify the name of the .img file that you downloaded from Cisco.com and the directory in which you saved the file on the local system.

### Procedure

**Step 1** Open a terminal window on the Mac system.

**Step 2** In the Terminal window, use the **cd** command to make the directory in which you saved the .img file the current directory.

**Step 3** Enter the following command, replacing the sample file name shown with the name of the .img file that you downloaded:

**md5 cisco-webex-social-*X.Y.Z.AAAAA.BBB*.img**

This command displays output that includes an MD5 checksum value, similar to the following example. In this example, the checksum value is shown in bold type for your reference:

```
1. C:\>fciv -md5 md5sum cisco-webex-social-3.0.1.10305.39.img
//
// File Checksum Integrity Verifier version 2.05.
//
88a5dba53661da5dcd37f81011201933  cisco-webex-social-3.0.1.10305.39.img
```

**Step 4** Compare the MD5 checksum value that you generated for the file with the MD5 checksum value that you obtained from Cisco as described in the "Obtaining an MD5 Checksum Value from Cisco" section on page 5-2.

If the checksum values are identical, the .img file that you downloaded is OK to use for an installation or upgrade of Cisco WebEx Social.

If the checksum values are not identical, .img file that you downloaded is corrupt. In this case, download the file from Cisco.com again and rerun the procedure in this section.

## Performing an MD5 Checksum Comparison on a Linux System

After you download a .img file and obtain its MD5 checksum value from Cisco (see the "Obtaining an MD5 Checksum Value from Cisco" section on page 5-2), follow these steps to perform an MD5 checksum comparison on a system that is running the Linux operating system.

### Before You Begin

- Identify the name of the .img file that you downloaded from Cisco.com and the directory in which you saved the file on the local system.

### Procedure

**Step 1** Use an SSH client to access the system and log in as the admin user.

**Step 2** Use the **cd** command to make the directory in which you saved the .img file the current directory.

**Step 3** Enter the following command, replacing the sample file name shown with the name of the .img file that you downloaded:

**md5sum cisco-webex-social-*X.Y.Z.AAAAA.BBB*.img**

This command displays output that includes an MD5 checksum value, similar to the following example. In this example, the checksum value is shown in bold type for your reference:

```
[admin@director-d deployer]$ md5sum cisco-webex-social-3.0.1.10305.39.img
88a5dba53661da5dcd37f81011201933  cisco-webex-social-3.0.1.10305.39.img
```

**Step 4** Compare the MD5 checksum value that you generated for the file with the MD5 checksum value that you obtained from Cisco as described in the "Obtaining an MD5 Checksum Value from Cisco" section on page 5-2.

If the checksum values are identical, the .img file that you downloaded is OK to use for an installation or upgrade of Cisco WebEx Social.

If the checksum values are not identical, .img file that you downloaded is corrupt. In this case, download the file from Cisco.com again and rerun the procedure in this section.

# Using the Software Page

You can use the Software page in the Director for upgrades provided that you have received a patch in the form of an .img file. To upgrade to the latest version of Cisco WebEx Social using the provided .img file, perform the following steps.

### Before You Begin

Verify the integrity of the installation image file as described in the "Verifying the Integrity of a Cisco WebEx Social .img File" section on page 5-2.

### Procedure

**Step 1** Sign in to the Director with your administrator user ID and password.

**Step 2** Click **System** in the menu bar, then select **Software** from the list on the left of your screen.

**Step 3** Take either of these actions:

- If you want to use SCP to obtain the .img file:
  - **a.** Click the **SCP** button to display options for using SCP.
  - **b.** In the Host Name field, enter the fully qualified domain name or the IP address of the node where you placed the patch .img file.

c. In the File Name field, enter the complete path and file name of the .img file.

d. In the Linux/Unix User Name field, enter the user ID of the node on which the patch .img file has been placed.

e. In the Password field, enter the password for the User ID that you entered.

- If you want to enter a URL where the .img file is stored:
  a. Click the **URL** button to display options for entering a URL.
  b. In the Upgrade File URL field, enter the URL.

**Step 4** Click **Fetch Image**.

The .img file is copied to the Director node and the software version that you uploaded appears in the Available Upgrade Version field in the Upgrade area of the page.

**Step 5** Click **Upgrade**.

The upgrade process begins.

**Note** You can monitor the upgrade process by checking the opt/logs/*date*/*node-hostname*_messages logs.

**Step 6** Allow up to 15 minutes for the Director web service to automatically restart.

**Step 7** Sign in to the Director with administrator credentials.

**Step 8** Click **System** in the menu bar, then select **Topology** from the list on the left of your screen

**Step 9** Verify that all the nodes have been upgraded to the desired version by checking the "Version Info" column next to each node.

If "Error" appears for any node, use an SSH client to connect to the node showing the symptom, log in as the admin user, and run the following command to identify the error:

**sudo service puppet debug**

**Step 10** Because the Cache, App Server, and Worker nodes will be in the Disabled state after a successful upgrade, take these actions in the Director System > Topology page:

a. Enable Cache nodes by choosing **Enable** from the Action drop-down menu next to each Cache node.

b. Enable Worker nodes by choosing **Enable** from the Action drop-down menu next to each Worker node.

c. Enable App Server nodes by choosing **Enable** from the Action drop-down menu next to each App Server node.

**Step 11** Allow up to 15 minutes for the App Server nodes to become enabled.

Monitor the /opt/cisco/quad/deploy folder on App Server nodes for all .war files to be consumed. When these files are consumed, Cisco WebEx Social should be ready for use.

# Using the Director

The Director is used for setting values of specific properties to complete configuration for some Cisco WebEx Social features. See *Cisco WebEx Social Administration Guide* for information about when to set properties.

# Checking Installation-Related Log Files

You can check the progress of the upgrade process for a node by opening the following log files on the Director:

/opt/logs/*date*/*hostname*_messages

/opt/logs/*date*/*hostname*_puppet.log