General Procedures

This chapter provides verification procedures, debugging procedures, maintenance and remedial procedures and other general information that may be used in other chapters of this guide.

This chapter is organized as follows:

Obtaining Third Party Tools

The following publicly available troubleshooting tools (or equivalent) are required for some of the instructions in this chapter:

- WinSCP—Utility for navigating and transferring files to/from *nix servers through SFTP, SCP, or FTP.

  Freeware available at www.winscp.net
- puTTY—SSH client, used to invoke CLI on *nix servers.

  Available at: http://www.putty.org/
- Firebug—Firefox plug-in that allows real-time debugging of web pages.

  Obtain at: http://getfirefox.com

Running Linux Commands on Nodes

When troubleshooting or following steps from other sections of this document, you may need to log in to various Cisco WebEx Social nodes and run Linux commands. The procedure is as follows:

Step 1 You first need to obtain and install an SSH client such as puTTY (see Obtaining Third Party Tools).

Step 2 Then you need to obtain the hostname or IP address of the node that you want to connect to. You can check this information on the System > Topology page on the Director.

Step 3 Having this information at hand, start your SSH client and point it to the hostname or IP address of the node.

Step 4 You see a login prompt. Enter user **admin** and your unified access password as password.

Step 5 You see a menu. Select **Drop to shell** and press **Enter**.

Step 6 Enter the command line you want to run at the prompt.

Modifying Advanced Portal Properties

You may want to change various Advanced Portal Properties when following the troubleshooting instructions in this document. To avoid clutter, in many cases only the Advanced Portal Property name and its target value are mentioned; detailed instructions as to how to access and modify an Advanced Portal Property are provided to the *Cisco WebEx Social Administration Guide.*

Setting Log Trace Levels

You can set log trace levels (log verbosity) by feature in Cisco WebEx Social. Log trace levels can be set independently for each App Server or Worker node or at once for all nodes of these types. Take the following steps to set a log trace level:

Step 1 Point your web browser to the IP or hostname of any App Server node.

Step 2 Sign in as administrator.

Step 3 Open your profile menu and click **Account Setttings**.

Step 4 On the page that opens go to **Server > Server Administration > Log Properties**.

Step 5 From the **Select a Node** drop-down box, select a node for which to set log trace levels.

Step 6 Find the feature (Group) whose log trace level you want to modify.

Step 7 Select the new log trace level from the drop-down box under Level.

Step 8 Click:

- **Apply** to apply the changes to the selected node only.
- **Apply All** to apply the changes to all App Server and Worker nodes.

You can also reset all log trace levels to their default values. Take these steps:

Step 1 On the same Account Settings page, select a node for which to reset log trace levels from the **Select a Node** drop-down box,

Step 2 Click:

- **Reset** to reset all log trace levels on the selected node only.
- **Reset All** to reset all log trace levels on all App Server and Worker nodes.

Checking Where solr Indexes Reside

On Search Store Nodes

These instructions apply to both master and slave nodes.

Log in to the machine, open /opt/cisco/search/conf/solrconfig.xml for viewing and find the <dataDir> entry.

If the value is "${solr.data.dir:./solr/data}", then /opt/cisco/search/data contains the indexes.

Otherwise the full path to the data directory is specified (for example /quaddata/search/solr/data).

On Index Store Nodes

Log in to the machine, open /opt/cisco/search/conf/solrconfig.xml for viewing and find the <dataDir> entry.

- For posts, check the <dataDir> entry in solrconfig.xml under /opt/cisco/searchcache/multicore/post/conf. If no entry is present, /opt/cisco/searchcache/multicore/post/data is the folder. Otherwise the full path to the data directory is specified.
- For social activity, check the <dataDir> entry in solrconfig.xml under /opt/cisco/searchcache/multicore/social/conf. If no entry is present, /opt/cisco/searchcache/multicore/social/data is the folder. Otherwise the full path to the data directory is specified.
- For video, check the <dataDir> entry in solrconfig.xml under /opt/cisco/searchcache/multicore/video/conf. If no entry is present, /opt/cisco/searchcache/multicore/video/data is the folder. Otherwise the full path to the data directory is specified.
- For followers, check the <dataDir> entry in solrconfig.xml under /opt/cisco/searchcache/multicore/follower/conf. If no entry is present, /opt/cisco/searchcache/multicore/follower/data is the folder. Otherwise the full path to the data directory is specified.

How To Verify a WebEx Social Upgrade File Using MD5

Upgrades for WebEx Social are typically performed using .img file downloads. Because of these files' significant size, they may become corrupted in the download process. Checking the integrity of the .img files is highly recommended.

You first need to obtain the MD5 checksum for the file. Check Obtaining the MD5 from CCO, page 2-4. Once you have this, you can check the file integrity on these operating systems:

- Linux, page 2-5
- Mac OS, page 2-6
- Windows, page 2-6

Obtaining the MD5 from CCO

Each .img file uploaded to www.cisco.com (CCO) for download by customers has an MD5 checksum calculated to help ensure the integrity of the downloaded copy. Here are the steps to get the MD5 for a given .img:

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

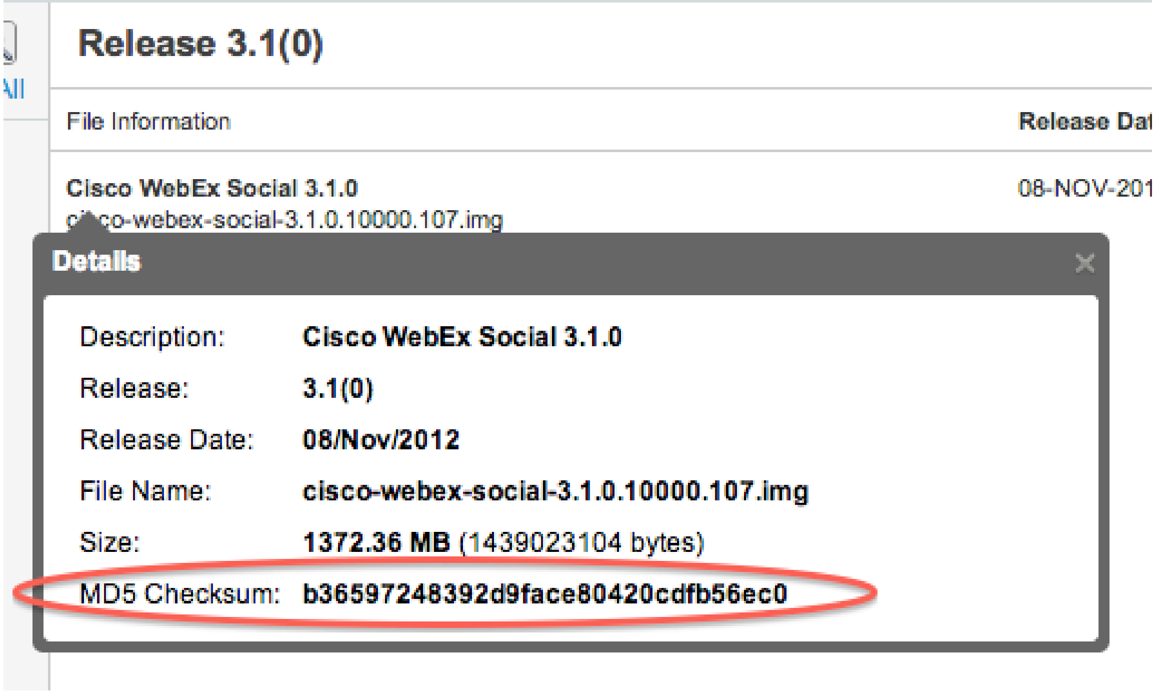
Step 2 Click **Support**, then click the **Downloads** tab.

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

Step 4 Click the Cisco WebEx Social link that appears.

Step 5 Navigate to the release and service release (SR) that you downloaded.

Step 6 Hover your mouse over the filename and you see a window like this one that has the MD5 (circled in red for clarity):



Cisco WebEx Social 3.1.0 08-NOV-201
cisco-webex-social-3.1.0.10000.107.img

Description: Cisco WebEx Social 3.1.0

Release: 3.1(0)

Release Date: 08/Nov/2012

File Name: cisco-webex-social-3.1.0.10000.107.img

Size: 1372.36 MB (1439023104 bytes)

MD5 Checksum: b36597248392d9face80420cdfb56ec0

Step 7 Take note of the checksum.

Linux

Follow these steps to check the integrity of an .img file on Linux:

Step 1 Using SSH, log in to the server where the .img file resides.

Step 2 Go to the directory where the .img file resides.

Step 3 Run this command:

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

where cisco-webex-social-X.Y.Z.AAAAA.BBB.img is the filename of the .img file you downloaded from CCO.

The output of this command will be the MD5 checksum and the file name, like so:

```
88a5dba53661da5dcd37f81011201933  cisco-webex-social-3.0.1.10305.39.img
```

Step 4 Compare the MD5 generated in the previous step with the MD5 that was obtained in the Obtaining the MD5 from CCO section.

Step 5 If they are not an identical match then your file download is corrupt and you should redownload the file before attempting to upgrade.

Mac OS

Follow these steps to check the integrity of an .img file on Mac:

Step 1 Open a terminal window on the Mac where the .img file resides.

Step 2 Go to the directory where the .img file resides.

Step 3 Run this command:

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

where cisco-webex-social-X.Y.Z.AAAAA.BBB.img is the filename of the .img file you downloaded from CCO.

The output of this command will be the MD5 checksum and the file name, like so:

```
88a5dba53661da5dcd37f81011201933  cisco-webex-social-3.0.1.10305.39.img
```

Step 4 Compare the MD5 generated in the previous step with the MD5 that was obtained in the Obtaining the MD5 from CCO section.

If they are not an identical match then your file download is corrupt and you should redownload the file before attempting to upgrade.

Windows

Windows users need to download the “FCIV” utility to check the integrity of an .img file. This Microsoft Knowledge Base article details where to get the required utility and how to use it:

http://support.microsoft.com/kb/889768

After you download and install the utility, follow these steps to check the integrity of an .img file on Windows:

Step 1 Open a Command Prompt window by clicking Start > Run and then typing cmd followed by the Enter key.

Step 2 In the command prompt that opens, go to the directory where the .img file resides.

Step 3 Run this command:

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

where cisco-webex-social-X.Y.Z.AAAAA.BBB.img is the filename of the .img file you downloaded from CCO.

The output of this command will be the MD5 checksum and the file name, like so:

```
//
// File Checksum Integrity Verifier version 2.05.
//
88a5dba53661da5dcd37f81011201933  cisco-webex-social-3.0.1.10305.39.img
```

Step 4 Compare the MD5 generated in the previous step with the MD5 that was obtained in the Obtaining the MD5 from CCO section.

If they are not an identical match then your file download is corrupt and you should redownload the file before attempting to upgrade.

Manually Running Synthetic Monitor

If you need to run the synthetic monitoring script for troubleshooting purposes you can do so by taking these steps:

Step 1 Log in to an App Server node using the admin user.

Step 2 Select **Drop to Shell** from the menu.

Step 3 Run this command:

```
sudo -u quad /opt/cisco/quad_synthetic/MonitorTest.py --log=INFO
```

Also see the list of supported command-line options in the table.

Table 2-1 MonitorTest.py Command-Line Options

Option	Description

`-h`
or
`--help`
	Display usage information

`-s QUADSERVER`
or
`--quadserver=QUADSERVER`
	Specify a Cisco Webex Social App Server node to perform monitoring on. The localhost is used if this option parameter is not specified.
	This option takes either a hostname or an IP address.

`-u QUADUSER`
or
`--quaduser=QUADUSER`
	Specify a local user to use when running the script. Access to Cisco WebEx Social is only allowed on port 9001.

`-t SEARCH_MAX_DELAY`
or
`--searchmaxdelay=SEARCH_MAX_DELAY`
	Specify the Search API maximum delay in seconds. The default value is 600 but you may need to increase it in large deployment where the search index can take a long time to build.
	Lower limit is 600. There is no upper limit.

`-p XAUTHSERVER`
or
`--xauthserver=XAUTHSERVER`
	Specify a Cisco Webex Social XAuth server.

Table 2-1 MonitorTest.py Command-Line Options

Option	Description

`-c CONFIG`
or
`--config=CONFIG`
	Specify a non-default configuration file.

`-l LOG`
or
`--log=LOG`
	Specify a log level. Possible values are (from most verbose to less verbose): DEBUG, ERROR, INFO

Accessing the Notifier Administration Console

This procedure is applicable after either a fresh installation or if there is a problem with Notifier and lets you access the Notifier web UI.

To provision Cisco WebEx Social to Communicate with the Notifier Server, follow these steps:

Procedure

Step 1 Sign in to Cisco WebEx Social as an administrator.

Step 2 Take these actions to access the Common Configurations window:

a. Click the down-arrow ▼ to the right of your name in the Global Navigation bar.

b. Select **Account Settings from** the drop-down menu.

c. Click the right-arrow ▶ next to **Server**

d. Click **Common Configurations** in the Server drawer.

Step 3 Select the **Notification Service** tab.

Step 4 Verify that at least one Message Queue node is running. If it is not, enable the Message Queue nodes, verify they are running, then restart the quad service on all App Server nodes.

Step 5 In the **Notification Service** tab, click **Start Synchronization**.

The system displays a message that informs you when the synchronization process completes.

Step 6 If the Cisco WebEx Social node that is running the synchronization operation is restarted in the middle of this operation, click **Reset Sync Flag**, then click **Start Synchronization** again.

Step 7 If you received a synchronization-error notification, you can resume the synchronization where it was stopped by clicking the **Resume Synchronization** button, or you can start the synchronization from the beginning by clicking the **Start Synchronization** button.

Step 8 To receive XMPP updates:

a. Sign out of Cisco WebEx Social.

b. Sign in to Cisco WebEx Social as a regular user.

Additional Steps

To access the Notifier administration user console, follow these steps:

Procedure

Step 1 Enable ports 9095 and 9096 in the firewall by performing the following substeps:

Note For security reasons, ports 9095 (for http) and 9096 (for https), which are used by the Notifier administration console, are blocked by the firewall by default.

a. Use an SSH client to access the Notifier server and log in as the admin user.

b. Enter these commands:

```
sudo iptables -A INPUT -p tcp --dport 9095 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 9096 -j ACCEPT
```

Step 2 Sign in to the console as follows, where *Notifier_server_host* is the fully qualified domain name or IP address of the Notifier node:

http://*Notifier_server_host*:9095\

Use the username **admin** and use the Unified Access password that you set when you performed the Cisco WebEx Social installation or upgrade procedure.

Step 3 To close the ports, enter the following command:

```
sudo /sbin/service firewall restart
```

For more information about the Notification Service, see *Cisco WebEx Social Administration Guide*.

Accessing the Search Store Administration Console

When troubleshooting Search Store problems you can access the Solr administration console by taking these steps:

Procedure

Step 1 Point your browser to the following URL:

http://*search_store*:8983/solr/admin/

Where *search_store* is the hostname or IP address of the Search Store master or slave node.

Step 2 When prompted, log in using user admin and your unified access password.

Accessing the Index Store Administration Console

When troubleshooting Index Store problems you can access the Solr administration console by taking these steps:

Procedure

Step 1 Point your browser to the following URL:

http://*index_store*:7973/solr/admin/

Where *index_store* is the hostname or IP address of the Index Store node.

Step 2 When prompted, log in using user admin and your unified access password.

Step 3 Select a category on the page that appears.

Accessing the Message Queue Administration Console

When troubleshooting message queue problems you can access the RabbitMQ administration console by taking these steps:

Procedure

Step 1 Run the following command on the Message Queue node to open port 15672 on that node.

```
sudo iptables -A INPUT -p tcp --dport 15672 -j ACCEPT
```

Step 2 Point your web browser at http://*MQ_node*:15672, where *MQ_node* is the hostname or IP address of your Message Queue node.

Step 3 Log in as user admin and your unified access password.

Step 4 Use the administration console.

Step 5 After you finsh using the console, run this command on the Message Queue node to reset the firewall configuration effectively closing port 15672 back up:

```
sudo /etc/init.d/iptables restart
```