



Using the Transport Gateway

Revised: November 22, 2013 Version 3.5

This chapter covers the following areas:

[Transport Gateway Requirements](#)

[Security Considerations while using a Transport Gateway](#)

[Installation Process Overview for the Transport Gateway](#)

[Download and Install the Transport Gateway Software](#)

[Configuration and Registration of the Transport Gateway](#)

[Transport Gateway Processing of Call Home Messages](#)

Transport Gateway Requirements

The Transport gateway is operational on the following 64-bit operating systems:

- Redhat Linux v5 and v6
- Windows 7
- Windows Server 2008 R2 platforms



Note

Transport Gateway is supported on hosts with above Operating Systems on VMware vSphere ESXi 5.x

The Transport Gateway uses the ports and protocols listed in the Table 4-1

Table 4-1 *Ports and Protocols used with Transport Gateway*

Source	Destination	Protocol	Port	Purpose
Cisco Device	Customer Email Server	SMTP	25	Cisco device to send mail to the Transport Gateway
Cisco Device	Transport Gateway	HTTP/HTTPS	110/143 respectively and can be changed by the customer	Cisco device to send messages to the Transport Gateway.

Source	Destination	Protocol	Port	Purpose
Transport Gateway	Customer Email Server	POP3/IMAP	110/143 respectively and can be changed by the customer	Transport Gateway to pick up the mail from the Cisco device
Transport Gateway	Cisco backend server	HTTPS	443	Transport Gateway to send Smart Call Home messages to the backend server without a proxy server - Option 1
Transport Gateway	Customer proxy server en route to Cisco backend server	HTTPS	Customer Supplied	Transport Gateway to send Smart Call Home messages to the backend server using a proxy server - Option 2
Transport Gateway	tools.cisco.com	HTTP/HTTPS	80/443	Provides access to tools.cisco.com
Transport Gateway	upload.cisco.com	HTTPS	443	Provides access to upload.cisco.com

System Requirements for Redhat Linux

If installing the Transport Gateway software on a Redhat Linux platform, system requirements are:

- Operating System - Red Hat Enterprise Linux AS release 3 (Taroon Update 7) or higher is recommended, 64 bit
- Mozilla 1.x or later
- Gedit or nedit application for viewing log files from the Transport Gateway UI
- PC or laptop with 512 MB of RAM (1 GB recommended)
- Hard disk: 70 MB + (Approx. 1MB for every Call Home message. Message size varies from 15KB - 1MB)

System Requirements for Windows

If installing the Transport Gateway software on a Windows platform, system requirements are:

- 64 bit Operating Systems:
 - Windows Server 2008 R2
 - Windows 7
- 512 MB (1 GB recommended)
- Hard disk: 100 MB + (Approx. 1MB for every Call Home message. Message size varies from 15KB - 1MB)

Security Considerations while using a Transport Gateway

Consider the following security information when using the Transport Gateway:

- The SMTP protocol is not encrypted, so the path between the Cisco device and the Transport Gateway through the SMTP server should be located in a secure zone.
- Sensitive information in the device configuration, such as passwords and SNMP Community strings, are masked before leaving the device to mitigate exposure within the LAN or over the Internet.
- It is recommended that the Transport Gateway is installed on the secure internal network, rather than off another segment on the firewall. In a typical configuration, this setup provides access to the proxy server, the email server, and the Internet. This does not require changes to the firewall configuration, as all communication is initiated by the Transport Gateway from the internal network on the highest security zone to other segments in lower security zones.
- Any return communication passes through the firewall as the traffic is part of an existing session.
- As part of Transport Gateway registration, the Transport Gateway sends a registration request to the Cisco backend. The Cisco backend generates a unique Transport Gateway ID and a password and sends these back to the Transport Gateway in the response. This ID and Password are sent in any request to the Cisco backend after the initial registration.
- This communication is through HTTPS and using port 443; see Table 4-1 for a list of the protocols and ports used between the source and destination devices in this mode of communication.
- For customers who need to proxy any traffic between their network and the outside world, the Transport Gateway can communicate with a HTTPS proxy server.

Installation Process Overview for the Transport Gateway

Figure 4-1 is an overview of the Transport Gateway installation and registration process:



Figure 4-1 **Transport Gateway Steps**



Note

Configuring Proxy Settings is optional step.

Download and Install the Transport Gateway Software

Browse to the [Transport Gateway software](#) on Cisco.com. This page is available to registered Cisco.com users with a Cisco service contract. Choose the desired version and click **Download**.

To install the Transport Gateway software on a Linux system:

- Step 1** Initiate a terminal session and navigate to the directory where the installation files were saved. Two files, install.sh and SCH-TG.tar.gz, are present in the unzipped folder.
- Step 2** Run the command `chmod +x install.sh`
- Step 3** Run the install.sh file
- Step 4** Go to `/opt/CSCOSchtg/tg/bin` and run `start.script` to start the Transport Gateway service.
- Step 5** Browse to `http://<ip address of Linux machine>/Transportgateway` to access the Transport Gateway application.

```
[root@CentOS-6-3-138-231 SCH-TG]# ls
install.sh  SCH-TG.tar.gz
[root@CentOS-6-3-138-231 SCH-TG]# chmod +x install.sh
[root@CentOS-6-3-138-231 SCH-TG]# ./install.sh
Do you wish to proceed with Transport Gateway installation?y
Creating installation directory
Installing Transport Gateway
Setting JAVA_HOME to /opt/CSCOSchtg/_jvm
Editing Wrapper Configuration to use /opt/CSCOSchtg/_jvm/bin/java
setownership
Registering as daemon
```

Figure 4-2 Linux installation commands

To install the Transport Gateway software on a Windows system, browse to the location of the downloaded files for the Transport Gateway. Double-click on the Transport Gateway executable (TransportGatewayWin64_v3_5.exe) and follow the installation wizard.

Once installed, follow the instructions for configuration and registration contained in [Configuration and Registration of the Transport Gateway section](#)

Uninstall the Transport Gateway for Linux

To uninstall the Transport Gateway application, go to the location of the installed files (`/opt/CSCOSchtg`) and run the `uninstall.sh` script in the `tg/bin` folder

```
[root@CentOS-6-3-138-231 opt]# ./CSCOSchtg/tg/bin/uninstall.sh
Stopping service
Stopping Cisco Transport Gateway ...
Stopped Cisco Transport Gateway .
Unregistering TG daemon
Deleting current installation
```

Figure 4-3 Uninstall sh script

Uninstall the Transport Gateway for Windows

To uninstall the Transport Gateway application, go to the folder containing the installation files. Double-click on the uninstall icon to start the uninstallation. Follow the wizard until uninstallation is complete.

Configuration and Registration of the Transport Gateway

Once the software is installed, configure the Transport Gateway. To do this:

Step 1 Browse to <http://<ip-address>/Transportgateway> or <http://<ip-address>/Transportgateway/home.jsp> to access the Transport Gateway application.

Step 2 Log in with the default username and password of **admin/admin**. The Set Proxy Settings window appears. This allows you to specify an HTTPS proxy for communication with the Smart Call Home servers at Cisco.com.



Note

Configuring proxy settings is optional. If the network has HTTPS proxy, then these settings can be configured.

Step 3 Enter the IP address or Hostname, Port Number, Proxy User Name, and Proxy Password. Click **Save**.

Figure 4-4 Set Proxy Settings

Step 4 After the proxy server is configured, click **Test Connection** to test the connection to Cisco.com.

Step 5 Click **Registration** to register the Transport Gateway with the Smart Call Home servers. The Register Transport Gateway screen appears.

Step 6 Enter the Cisco.com ID, password, a name and description for the Transport Gateway (user defined), and an email address (optional) for registration failure notification.

Step 7 Click **Register with SCH**. Upon successful registration, the Registration Status will change to Registered.

- Step 8** Once registration is successful, the email address for failure notification can be changed by entering an email address in the Notify Email Address field and clicking **Update**.

Figure 4-5 Register Transport Gateway

Configure mailbox

If using email to send Call Home messages from the device to the Transport Gateway, configure the mailbox as follows:

- Step 1** From the Mail Server Type drop-down menu, choose the appropriate mail server protocol. The Mail Server Port Number automatically populates with the corresponding port number.
- Step 2** Enter the name of the Mail Server Folder that will receive the Call Home messages.
- Step 3** Enter the Account Name and Password that has access to the mail server.
- Step 4** Check the Send Call Home Messages checkbox to upload Call Home messages to Cisco.com. If this option is unchecked, the Call Home messages are stored locally. This option must be checked in order to realize the full benefits of Smart Call Home.
- Step 5** Enter the desired Mail Store Size. This defines the capacity of the local mail store. Note that if this limit is exceeded, Call Home messages are not processed.
- Step 6** Enter the email address of the person to notify in the event the mail store approaches capacity.
- Step 7** Click **Save**.



Note

The Transport Gateway must be restarted to effect changes in the mailbox configuration. Once restarted, Call Home messages are received by the Transport Gateway, stored locally, and uploaded to Cisco.com.

Configure HTTP settings

If using HTTP to send Call Home messages from the device to the Transport Gateway, configure the HTTP Settings as follows:

- Step 1** Click **Configuration** and then click the HTTP Settings tab (Figure 4-5).
- Step 2** Check the Send Call Home Messages checkbox to upload Call Home messages to Cisco.com. If this option is unchecked, the Call Home messages are stored locally. This option must be checked in order to realize the full benefits of Smart Call Home.
- Step 3** Enter the desired Mail Store Size. This defines the capacity of the local mail store (Httpmsgstore). Note that if this limit is exceeded, Call Home messages are not processed.



Note All other fields are automatically populated.

- Step 4** Click **Save**.



Note The Transport Gateway must be restarted to effect changes in the HTTP settings. Once restarted, Call Home messages are received by the Transport Gateway, stored locally, and uploaded to Cisco.com.

The screenshot displays the Cisco Transport Gateway web interface. On the left is a sidebar with buttons for 'Proxy Settings', 'Registration', 'Configuration', 'Reset Password', 'Message Box', 'Log Status', 'Test Connection', 'Restart Service', and 'Change Password'. The main area has two tabs: 'Mailbox Configuration' and 'Http Settings'. The 'Http Settings' tab is selected, showing a 'Configure for Http Server' section. This section includes a 'Http Server Setting' box with the following fields: 'Send Call Home Messages' (checked), 'Http Store Size (in MB)' (20), 'Http Server Port Number' (80), 'Https Server Port Number' (443), and 'IP Address' (10.77.21.131). Below this box are 'Save' and 'Reset' buttons. At the bottom of the main area is an 'HTTP Service URLs' section with three entries: 'NMS Service URL' (http://10.77.21.131:80/Transportgateway/services/NMSRequestHandler), 'Device Service URL' (http://10.77.21.131:80/Transportgateway/services/DeviceRequestHandler), and 'Https Device Service URL' (https://10.77.21.131:443/Transportgateway/services/DeviceRequestHandler). The top right corner shows 'TG Version: 3.5' and links for 'About', 'Help', and 'Logout'.

Figure 4-6 HTTP Settings

Reset Password

Allows the user to reset the password that transport gateway uses to communicate with Cisco backend.

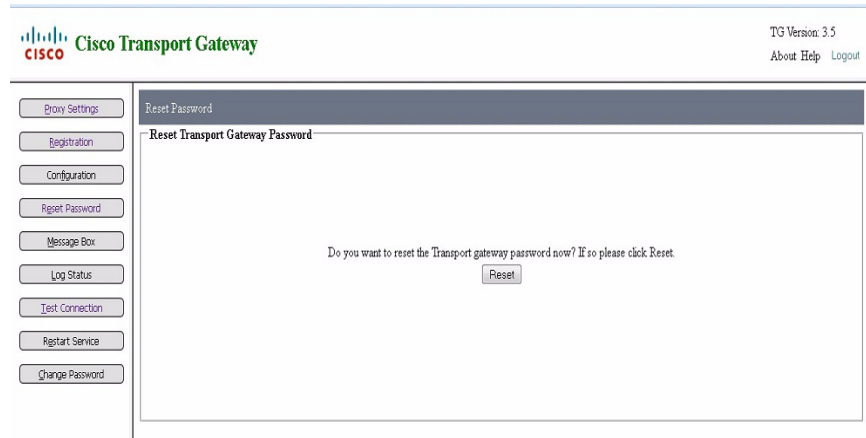


Figure 4-7 **Reset Password Snapshot**

Message Box

The Transport Gateway allows you to view the Call Home messages that are available to be sent to Cisco. This list contains Call Home messages that have been received in the mailbox more than three hours previous, but less than two days previous, and have not been successfully sent to Cisco. If the message is not sent to Cisco within three hours, it is stored and viewable in the message box. If the message is not sent to Cisco within two days, it is automatically deleted.

In the Transport Gateway application, click **Message Box**. In the **Email Messages** tab, you can view a list of mails from devices configured to send mails to Cisco via the Transport Gateway (Figure 4-1). You may send email messages to Cisco or delete selected messages. If using HTTP, click the **HTTP Messages** tab to view the HTTP mailbox.

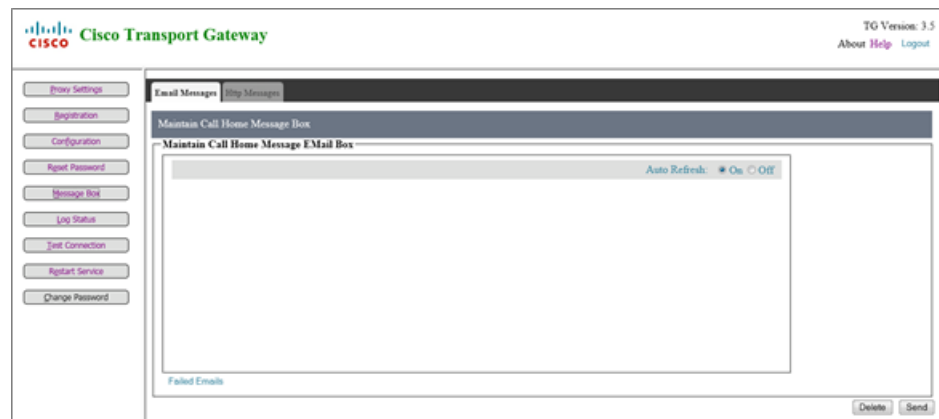


Figure 4-8 **Message Box**

Subject	Received
System Notification From rbml-test-router 4 TestMohan_1	Sep 26 2012 01:29:37 PDT
System Notification From rbml-test-router 1 TestMohan_1	Sep 26 2012 01:29:41 PDT
System Notification From rbml-test-router 2 TestMohan_1	Sep 26 2012 01:29:25 PDT
System Notification From rbml-test-router 3 TestMohan_1	Sep 26 2012 01:29:29 PDT
System Notification From rbml-test-router 0 TestMohan_1	Oct 08 2012 03:06:29 PDT

Figure 4-9 Sample Email Messages

Log Status

In the Transport Gateway application, click **Log Status**. From here you can:

- View the list of Warning or Informational logs by choosing the appropriate Log Mode from the drop-down menu.
- Change the log mode.
- View log files by checking the box next to the desired log file and click **View**.
- Send log files to Cisco support by checking the box next to the desired log files and click **Zip**. Save the .zip file to a local machine. Enter an email address in the Support Email ID field and click **Upload to Support**.

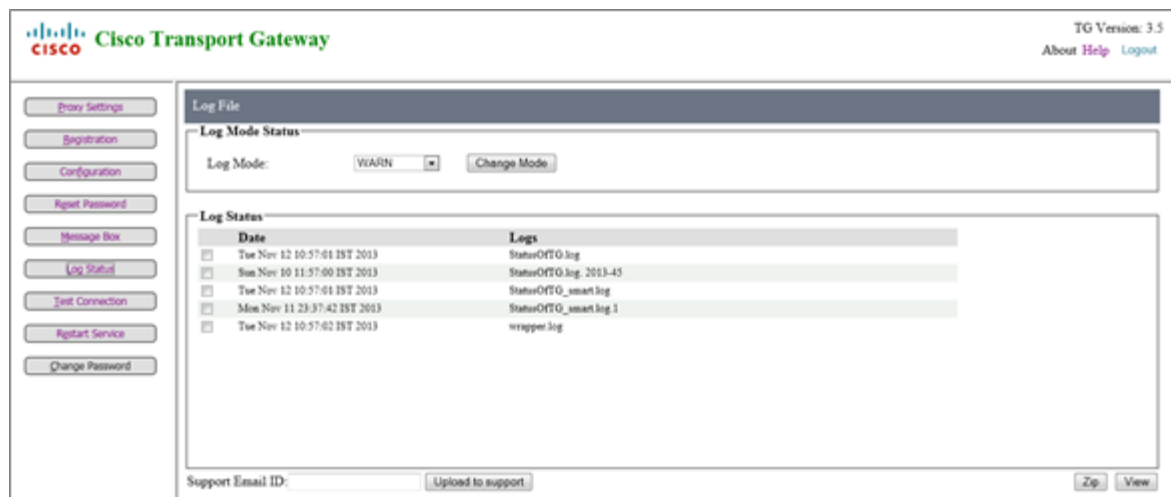


Figure 4-10 Log Status

To view, change the log mode, or zip the log status file perform the following steps:

- Step 1** On the Transport Gateway Application click Log Status; the **Log Status** area appears.

- Step 2** Select the desired status log by clicking the Log Mode drop-down menu and selecting the Warn or Info log mode.
- Step 3** Click **Change Mode**. An informational message appears indicating:
- What the Log Mode was changed to.
 - You must restart the Transport Gateway to effect the change in log mode.
- Step 4** Once the log mode has been specified, and activated if changed, then:
- Click **View** to view the status log file; the Status Of TG file opens with the status information displayed.
 - Click **Zip**; a Save window appears with a filename for the log status zip file.
- Step 5** Click **Save**.
- Step 6** In the Support Email ID field, enter an email address to send the zip file. Click **Upload to support** to select the zip file and send it to the support email address.

Test Connection

The Test Connection option tests the connection between the Transport Gateway and Cisco. Click **Begin Test** to test the connection. A success or failure message is returned.

Restart Service

This option restarts the Transport Gateway service. Restarting the service effects any changes to the Transport Gateway configuration.

Change Password

This option enables you to change the password for the Transport Gateway. The default user name and password is admin/admin.

Transport Gateway Processing of Call Home Messages

Devices use one of two methods to deliver Call Home messages to a Transport Gateway:

- HTTP
- EMAIL

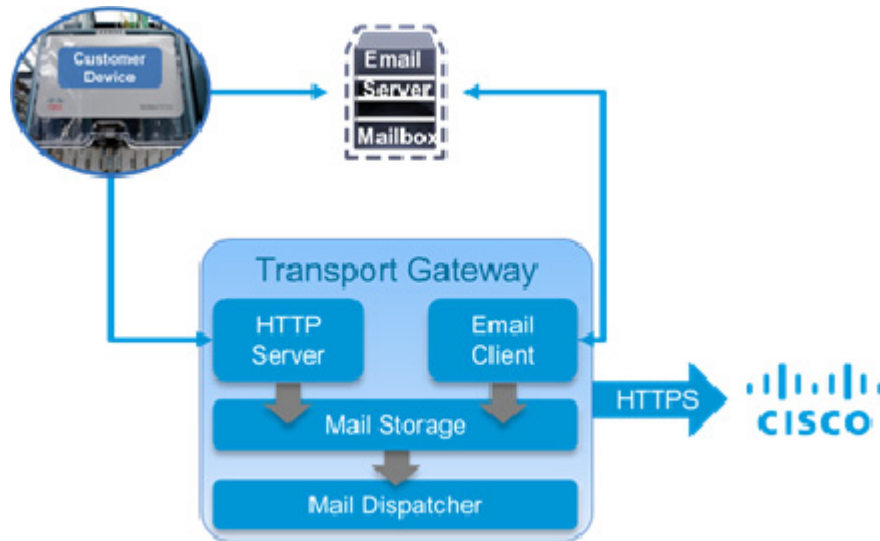


Figure 4-11 Call Home message path through the Transport Gateway

Using an HTTP Server to Process Call Home Messages

In the first method, Call Home devices make an HTTP connection on a specified port and deliver messages directly to the Transport Gateway.

The steps in processing Call Home messages using an HTTP server are:

-
- Step 1** Device(s) send generated Call Home messages to the Transport Gateway.
 - Step 2** The Transport Gateway passes the Call Home messages to the embedded HTTP server.
 - Step 3** The embedded HTTP server sends the Call Home messages to the Cisco Backend.

Using a Mail Server to Process Call Home Messages

Alternatively, the Transport Gateway's email client can retrieve messages from an email inbox. This section explains how the Transport Gateway processes the Call Home messages sent to a client server/mailbox and retrieved to the Transport Gateway Call Home mailbox.

The Transport Gateway automatically retrieves Call Home messages from the client mailbox, and those messages are forwarded automatically to Cisco.

The following describes the process the Transport Gateway uses to retrieve Call Home messages from the client mailbox, then sends to Cisco:

- Device(s) send generated Call Home messages to the client mailbox.
- The Transport Gateway connects to the client mailbox to retrieve the CallHome messages.
- The Transport Gateway checks at regular intervals to see if any Call Home messages have arrived in the client mailbox.

**Note**

When the Transport Gateway cannot connect to the client mailbox, an error is logged indicating the date/time, event and reason of the error. The Transport Gateway will try to connect to the client mailbox every 60 seconds until the connection is restored.

- When new Call Home messages arrive in the client mailbox, they are retrieved by the Transport Gateway, then deleted from the client mailbox.
- The Transport Gateway automatically sends the Call Home messages to Cisco.

Temporarily disable automatic message forwarding.

By default, the Transport Gateway automatically forwards messages to Cisco as they arrive. This behavior is controlled by the "Send Call Home Messages" option in the HTTP and SMTP configuration. Automated message forwarding can be temporarily disabled by unchecking this option for one or both transports. When automatic forwarding is disabled, the Transport Gateway stores messages until they are sent manually using the configuration GUI.

**Note**

HTTP and SMTP messages are stored in separate inbox. If both are disabled, it will be necessary to check both inbox for queued messages.

Manually Forwarding messages:

In order for the Transport Gateway to forward Call Home messages to Cisco, the following tasks must be completed:

- Transport Gateway is registered with Cisco
- Transport Gateway has been successfully configured
- The user checks the **Send Call Home Messages** check box in the configuration window
- Transport Gateway has a connection to Cisco

The Transport Gateway forwards Call Home messages to Cisco without user interaction if the above tasks are complete.

If for some reason the Transport Gateway is not able to send messages to Cisco, the Transport Gateway continues attempting to send them for three hours. If messages cannot be sent to Cisco after three hours, the messages become available in the Transport Gateway mail store, which is accessible by clicking the **Message Box** option. The user can manually send the messages to Cisco or delete them from the mail store without sending. Messages older than 2 days that are not sent to Cisco are deleted automatically.

Notifying the Customer When Mail Store Reaches the Size Limit

During configuration the customer has the option to specify a mail store size for each inbox to indicate when they want to be notified when a Transport Gateway mail store is becoming full.

The configuration also has a corresponding option to specify a notification email address that the system uses to send an email notification when the mail store is reaching its size limit. When the mail store is reaching its size limit, an email notification is sent to the email address specified in the Notify Email Address field.