



Using the Transport Gateway

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](#)

[Troubleshooting Cisco Transport Gateway Errors Transport](#)

[Gateway and SNTC Collectors](#)

[Frequently Asked Questions](#)

Transport Gateway Requirements

The Transport gateway is operational on the following 64-bit operating systems with Java 8 installed:

- Redhat Linux v5 and v6
- CentOS v8 supported in TG 4.1.9 version
- Windows 7
- Windows Server 2008 R2 platforms
- Windows Server 2012 R2 platforms



Note

Transport Gateway is supported on hosts with above Operating Systems on VMware virtualization platform.

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
Transport Gateway	Customer Email Server	POP3/IMAP /Secure POP3/Secure IMAP	110/143/995/993 respectively	Transport Gateway to pick up the email from the Customer Email Server.
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	HTTPS	443	Provides access to tools.cisco.com

System Requirements for Redhat Linux

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

- Operating System - Red Hat Linux v5 or v6 recommended, 64 bit
- PC or laptop or VM (created using VMware virtualization platform) with 2 GB of RAM
- Hard disk: 10 GB + (Approx. 1MB for every Call Home message. Message size varies from 15KB - 1MB)
- Java 8 to be installed before starting TG installation

System Requirements for Windows

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

- 64 bit Operating Systems:
 - Windows Server 2008 R2
 - Windows 7
 - Windows Server 2012 R2
- 2 GB RAM
- Hard disk: 10 GB + (Approx. 1MB for every Call Home message. Message size varies from 15KB - 1MB)
- Java 8 to be installed before starting TG installation

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**.

Linux

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



Note

If TG needs to be installed as a non-root user, follow the below steps:

- Create a Linux user *tguser*
- Copy the installation file to */home/tguser* and proceed with installation under *tguser*

-
- Step 4** Browse to <http://<ip address of Linux machine>/Transportgateway> to access the Transport Gateway application.
- Once installed, follow the instructions for configuration and registration contained in [Configuration and Registration of the Transport Gateway](#) section

Windows



Note

To install TG on Windows VM, ensure you download the correct executable ending with “_VM.exe”.

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_<x>.exe*) and follow the installation wizard. Here <x> stands for the TG release version.

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

OVA Image

To install the Transport Gateway software on Open Virtualization Appliance Image Format

Prerequisites:

1. Download and install vSphere Client version 5.5.
2. Create an ESXi server.

Perform the following steps:

-
- Step 1** OVA image file can be locally stored or remote location, that is accessible
- Step 2** Enter **Installation Name** for the OVA image installation then click **Next**.
- Step 3** Select *Thin Provision* option under **Disk Format** and click **Next**.
- Step 4** Verify the information displayed and click **Next**.
- Step 5** Check the *Power on after deployment* checkbox and click **Finish** to install the image.

After installation, OVA Installation image will be created, that is visible on the left pane. It displays the name of the installation entered in step 4.

**Note**

Incase the VM is not ON, then right-click on the OVA installation name and select **Power ON**. You must use *sudo* prefix for some of the commands that cannot be executed from tguser.

- Step 6** Go to CONSOLE tab on the right panel, double click on the console screen to activate the console mode.
- Step 7** Login with **username:** *tguser* and **password:** *tguser*. [Change the password after first time login]
- Step 8** TG installation directory will be available at */home/tguser/CSCOSchtg*.
- Step 9** Run the command: *sh/home/tguser/CSCOSchtg/tg/bin/sh.script status* to verify the TG Service.
- Step 10** Run the command *ifconfig* to locate the IP address.

If **IP address is not assigned** or IP address need to be changed, then perform the following steps: If you are using TG OVA version 4.1.8 or below

1. Edit the file */etc/sysconfig/network-scripts/ifcfg-eth0* by using sudo access privilege and update the following information and save it.

Eg. *sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0*

DEVICE=eth0

TYPE=Ethernet

ONBOOT=yes

BOOTPROTO=static

IPADDR=x.x.x.x [available IP from the network IP pool can be used]

NETMASK=255.255.255.0

GATEWAY=x.x.x.1

2. Restart the service by running command with sudo access privilege

\$sudo service network restart

3. Run *ifconfig* to verify newly assigned IP Address.

4. Restart TG Service and access TG UI with new IP Address assigned

To restart TG, go to */home/tguser/CSCOSchtg/tg/bin/*

Run *./sh.script restart*



If IP address is not assigned or IP address need to be changed, then perform the following steps: If you are using TG OVA version 4.1.9

5. Edit the file */etc/sysconfig/network-scripts/ifcfg-ens160* by using sudo access privilege and update the following information and save it.

Eg. *sudo vi /etc/sysconfig/network-scripts/ifcfg-ens160*

DEVICE=ens160

TYPE=Ethernet

ONBOOT=yes

BOOTPROTO=static

IPADDR=x.x.x.x [available IP from the network IP pool can be used]

NETMASK=255.255.255.0

GATEWAY=x.x.x.1

6. Restart the service by running command with sudo access privilege

\$sudo systemctl restart NetworkManager.service

7. Run *ifconfig* to verify newly assigned IP Address.
8. Restart TG Service and access TG UI with new IP Address assigned
To restart TG, go to */home/tguser/CSCOSchtg/tg/bin/*
Run *./sh.script restart*

Note Using the IP address, access the TG UI with URL <http://<IP Address>:8080/Transportgateway>

If **Test Connection** fails, then perform the following steps:

- Check if you can reach to *tools.cisco.com* e.g:ping tools.cisco.com.
 - If this fails then it could be due to the fact that domain name resolution might have failed. One of the reason for this is that ESXi host where this OVA is getting deployed is not DHCP enabled.

In such cases please follow the below steps:-

- Check */etc/resolv.conf* file and ensure that it has the entries corresponding to your name servers. If not, then overwrite the entries with your name server details.



Note To know your name server you can issue a command *nslookup www.cisco.com* from a system which is connected to Internet to list the name servers.

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

Applying Security Patch for Linux Vulnerabilities

Applicable TG OVA Images: 4.1.3, 4.1.4, 4.1.5.

Follow the below steps to apply the security patch for linux vulnerabilities:

-
- Step 1** Download the patch [linux-vulnerability-patch.zip](#).
- Step 2** Login to system where the TG OVA image is installed.
- Step 3** Execute the following commands:
- ```
unzip linux-vulnerability-patch.zip
sudo ./install.sh
```
- VM gets restarted and new patch will be applied.

## Applying Security Patch for glibc Vulnerabilities

**Affected TG OVA Images:** 4.0, 4.1, 4.1.1, 4.1.2, 4.1.2.1, 4.1.3



---

**Note** Applying glibc vulnerability patch is not required, if **linux vulnerability** patch is already applied.

---

Follow the below steps to apply the security patch for glibc vulnerability (CVE-2015-7547):

- 
- Step 1** Download the patch [glibc-vulnerability-patch.zip](#).
- Step 2** Login to system where the TG OVA image is installed.
- Step 3** Execute the following commands:
- ```
unzip glibc-vulnerability-patch.zip
cd glibc-vulnerability-patch
sudo ./install.sh
sudo reboot
```
- VM gets restarted and new patch will be applied.

Applying Security Patch for bash shell vulnerability

Affected TG Image: Cisco Transport Gateway 4.0 Linux Build - OVA Image



Note Applying bash shell vulnerability patch is not required, if **linux vulnerability** patch is already applied.

Follow the below steps to apply the security patch for bash shell vulnerability:

-
- Step 1** Download the patch (bash-security-patch.zip) from : <http://software.cisco.com>
- Step 2** Login to system where the TG OVA image is installed as root

- Step 3** Unzip the patch obtained in [Step 1](#)
- Step 4** cd to directory "bash-patch"
- Step 5** Execute `./install.sh`
- Step 6** Machine will get auto rebooted after patch is installed.

Uninstall the Transport Gateway for Linux

To uninstall the Transport Gateway application, go to the installation directory and run the `uninstall.sh` script in the `tg/bin` folder.

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:

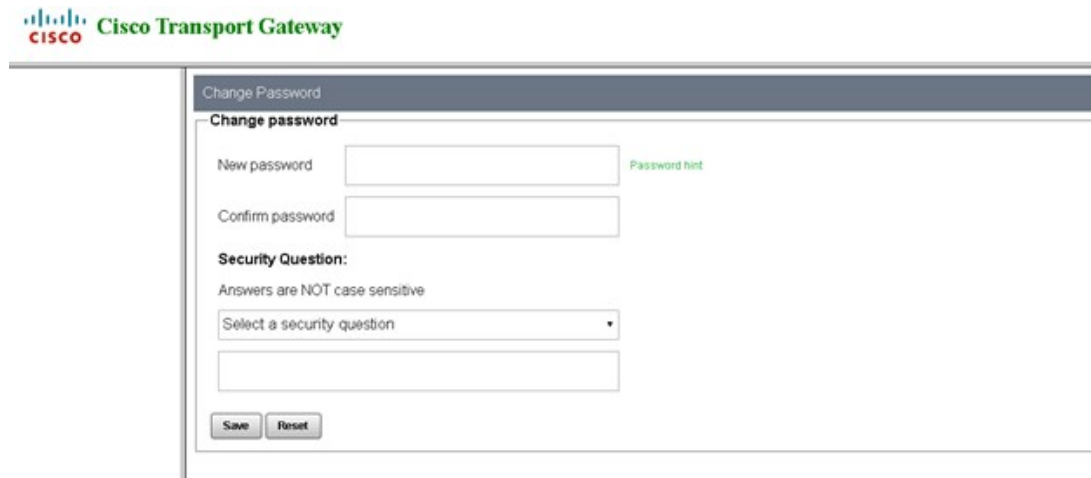
- Step 1** Browse to <http://<ip-address>/Transportgateway> or <http://<ip-address>/Transportgateway/home.jsp> to access the Transport Gateway application.
- Step 2** At first time login, enter the default username and password of **admin/admin**.



The image shows the Cisco Transport Gateway login interface. At the top, there is a Cisco logo and the text "Cisco Transport Gateway". Below this, the title "Login to Transport Gateway" is displayed. Under the title, there are two input fields: "User Name" and "Password". Below the "Password" field, there are two buttons: "Login" and "Reset".

Figure 4-2 *Transport gateway Login screen*

The system prompts the user to enter new password, select a security question and provide an answer to that question that can be used for future prospects.



The image shows the 'Change Password' form in the Cisco Transport Gateway interface. The form is titled 'Change Password' and 'Change password'. It contains two text input fields for 'New password' and 'Confirm password', with a 'Password hint' link next to the first field. Below these is a 'Security Question' section with the instruction 'Answers are NOT case sensitive'. It features a dropdown menu labeled 'Select a security question' and a corresponding text input field for the answer. At the bottom are 'Save' and 'Reset' buttons.

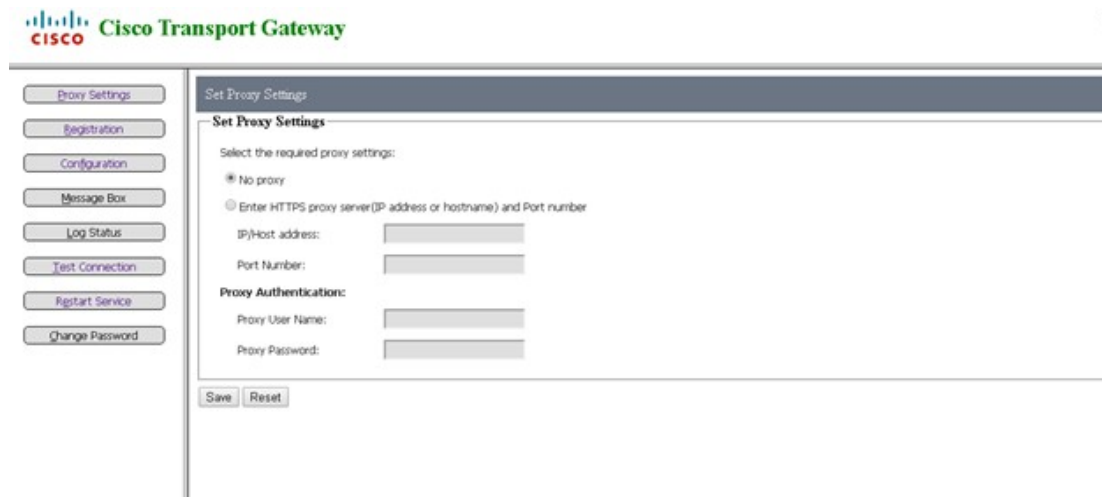
Figure 4-3 *Change Password*

Step 3 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.



The image shows the 'Set Proxy Settings' form in the Cisco Transport Gateway interface. The form is titled 'Set Proxy Settings' and 'Set Proxy Settings'. It contains a section 'Select the required proxy settings:' with two radio buttons: 'No proxy' (selected) and 'Enter HTTPS proxy server(IP address or hostname) and Port number'. Below this are input fields for 'IP/Host address:', 'Port Number:', 'Proxy User Name:', and 'Proxy Password:'. At the bottom are 'Save' and 'Reset' buttons. A sidebar on the left contains links to 'Proxy Settings', 'Registration', 'Configuration', 'Message Box', 'Log Status', 'Test Connection', 'Restart Service', and 'Change Password'.

Figure 4-4 *Set Proxy Settings*

Step 4 Enter the IP address or Hostname, Port Number, Proxy User Name, and Proxy Password. Click **Save**.

- Step 5** After the proxy server is configured, click **Test Connection** to test the connection to Cisco.com.
- Step 6** Click **Registration** to register the Transport Gateway with the Smart Call Home servers. The Register Transport Gateway screen appears.
- Step 7** 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 8** Click **Register with SCH**. Upon successful registration, the Registration Status will be changed to Registered and **TG SSL Certificate & Reset Password** buttons will be shown in Left navigation pane. To know more details on TG SSL Certificate, please refer the corresponding section.
- Step 9** 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

- Step 10** **Re-register Transport Gateway** option is provided to the user to register with an alternate Cisco.com Id. User can check this option and enable the screen to register TG once again.



Note For TG Registration only CCO with access level L2 and L4 are supported.

If you are using the CSSM Satellite OVA image, the feature **TG SSL Certificate** will not be shown even after successful registration.

Forgot Password

To get the password, use the Forgot password link on the login screen that is visible on subsequent logins. Perform the following steps to get the forgotten password:

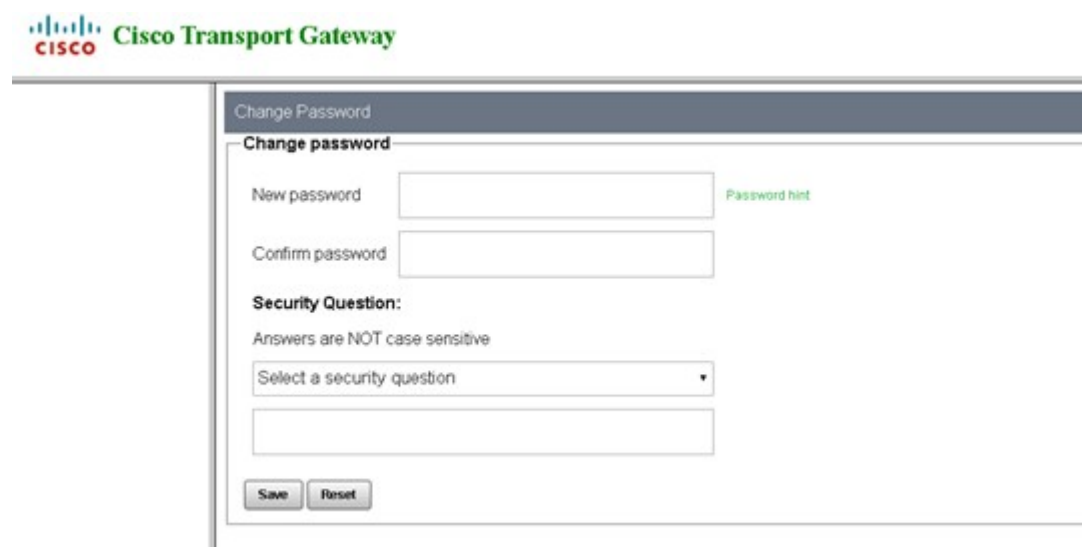
- Step 1** On the login screen, click **Forgot password?** link.



The image shows the Cisco Transport Gateway login interface. At the top is the Cisco logo and the text "Cisco Transport Gateway". Below this is a box titled "Login to Transport Gateway". Inside the box, there are two input fields: "User Name" and "Password". Below the "Password" field are two buttons: "Login" and "Reset". At the bottom of the box is a link that says "Forgot your password?".

Figure 4-6 Login screen with Forgot Password link

The application directs to a new screen to enter new password and answer the security question as entered while creating password.



The image shows the Cisco Transport Gateway "Change Password" screen. At the top is the Cisco logo and the text "Cisco Transport Gateway". Below this is a box titled "Change Password". Inside the box, there are two input fields: "New password" and "Confirm password". To the right of the "New password" field is a link that says "Password hint". Below these fields is a section titled "Security Question:". Under this section, it says "Answers are NOT case sensitive". There is a dropdown menu labeled "Select a security question" and an input field below it. At the bottom of the box are two buttons: "Save" and "Reset".

Figure 4-7 Set New Password

- Step 2** Enter the answer to the security question, new password and also reenter the password to confirm.
- Step 3** Click **Save**.



Note

Security answer should match with the answer entered while configuration else the password change fails. If you have forgotten the answer to the security question, please contact the support team to reset the password and security question.

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,

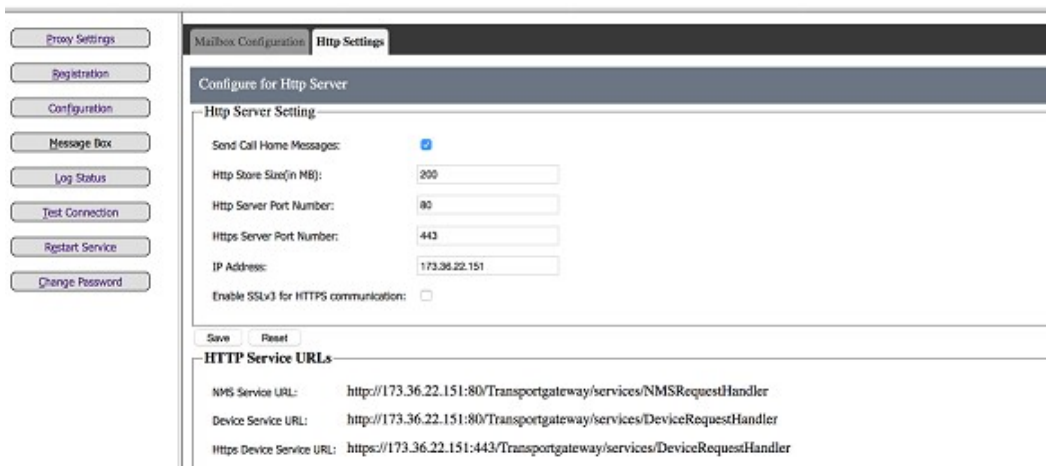
The screenshot shows the Cisco Transport Gateway web interface. On the left is a navigation menu with buttons: Proxy Settings, Registration, Configuration, Message Box, Log Status, Test Connection, Restart Service, and Change Password. The main area is titled 'Mailbox Configuration' and 'Http Settings'. Below this is a section 'Configure Transport Gateway for Call Home Mailbox' and 'Transport Gateway Configuration for Call Home Mailbox'. The configuration fields are: Mail Server Type (Secure IMAP), Mail Server Folder (FG-Messages), Mail Server IP/Host Address (mail.cisco.com), Account Name (demo-acc), Password (masked with asterisks), Mail Server Port Number (993), Send Call Home Messages (checked), Mail Store Size (in MB) (200), and Notify Email Address (testuser@cisco.com). There is also a text input for 'Enter Email address if you would like to be notified when the mail store is becoming full'.

Call Home messages are received by the Transport Gateway, stored locally, and uploaded to Cisco.com.

Configure HTTP settings

If you are 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
- Step 2** Port numbers and IP address are editable.




Note

If you want to change the default port numbers:

1. Ensure, you input the available free port number
2. Restart Service, when the TG restart is in progress, access the UI by giving the new port number in the URL

Step 3

Enter the desired Http 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.



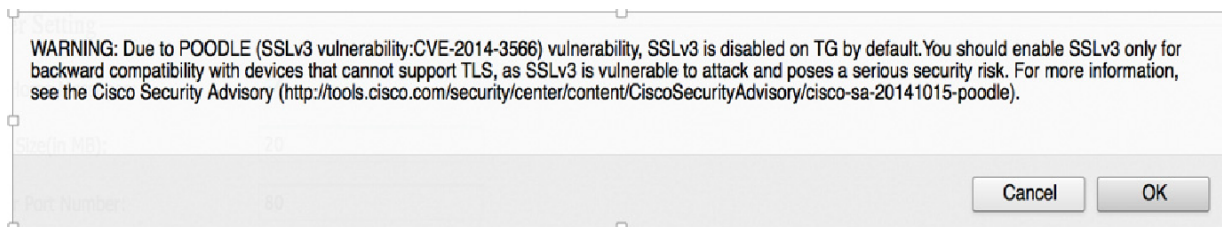
Note

All other fields are automatically populated.

Step 4

Enable SSLv3 for HTTPS communication: By default, SSLv3 is disabled on TG due to security vulnerabilities associated with SSLv3. However if there are some devices in your network which still use SSLv3 for SSL handshake, and you are not in a position to upgrade the OS image on those devices, then you can use this option to enable SSLv3 on TG. Enabling SSLv3 on TG poses serious security risks and it is strongly discouraged to turn it ON. Instead try to upgrade the device OS to get the TLS capability for SSL handshake. By default, it is unchecked.

To enable SSLv3 on TG, check **Enable SSLv3 for HTTPS communication**, below warning message appears:



Step 5

Click **Save**.

Step 6

Restart TG to reflect the **Http Settings** configuration changes.

**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.

Step 7 If you are using HTTP for communication from device to TG, copy the URL under "*Device Service URL*:" If you are using HTTPS for communication from device to TG, copy the URL under "*Https Device Service URL*:"

and use it in call home profile on device, as below:

```
Router# configure terminal
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@domain-name
Router(cfg-call-home)# profile CiscoTAC-1
Router(cfg-call-home-profile)# no active
Router(cfg-call-home-profile)# #profile {Your_profile_name}
Router(cfg-call-home-profile)# active
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# no destination transport-method email
Router(cfg-call-home-profile)# destination address http {Device Service URL from TG to be pasted here}
Router(cfg-call-home-profile)# end
Router# copy running-config startup-config
```

Reset Password

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

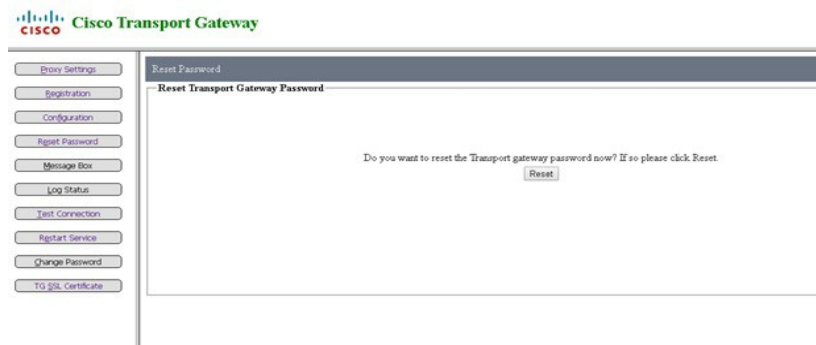


Figure 4-8 **Reset Password Snapshot**

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 four 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 four 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.

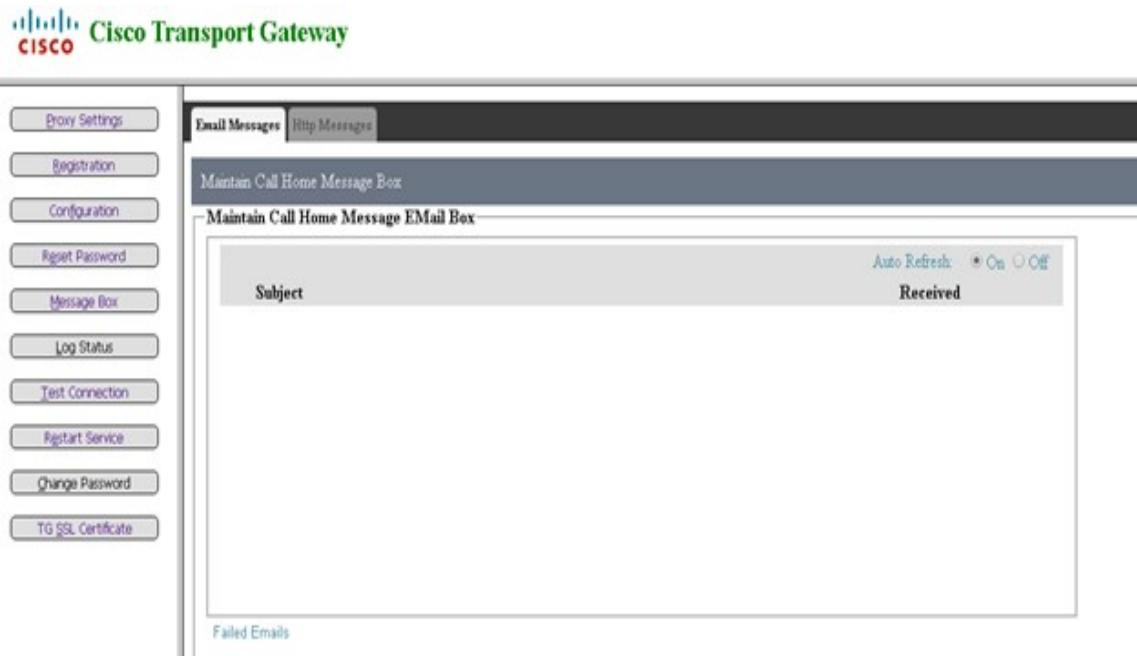


Figure 4-9 Message Box

Subject	Received
<input type="checkbox"/> System Notification From rbml-test-router 2 Test123	Sep 23 2015 03:06:50 PDT
<input type="checkbox"/> System Notification From rbml-test-router 0 Test123	Sep 23 2015 03:07:08 PDT
<input type="checkbox"/> System Notification From rbml-test-router 4 Test123	Sep 23 2015 03:06:45 PDT

Figure 4-10 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**.

The screenshot shows the 'Log Status' interface. On the left is a sidebar with buttons: Proxy Settings, Registration, Configuration, Agent Password, Message Box, Log Status (highlighted), Test Connection, Restart Service, Change Password, and TG SSL Certificate. The main area has a 'Log File' header. Below it is the 'Log Mode Status' section with a 'LogMode:' dropdown set to 'WARN' and a 'Change Mode' button. The 'Log Status' section contains a table with two columns: 'Date' and 'Logs'. The table has two rows: one with a checkbox, 'Fri Apr 29 15:30:08 EDT 2016', and 'StatusCTO.log'; the other with a checkbox, 'Fri Apr 29 15:38:11 EDT 2016', and 'wrapper.log'. At the bottom, there is a 'Support Email ID:' field, an 'Upload to support' button, and 'Zip' and 'View' buttons.

	Date	Logs
<input type="checkbox"/>	Fri Apr 29 15:30:08 EDT 2016	StatusCTO.log
<input type="checkbox"/>	Fri Apr 29 15:38:11 EDT 2016	wrapper.log

Figure 4-11 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 username and password is admin/admin. Select **Change Password** from the left menu navigation.

Figure 4-12 *Change Password*

Enter the answer to the security question, new password and also reenter the password to confirm. Click **Save** to save the changed password details.



Note

Security answer should match with the answer entered while configuration else the password change fails. If you have forgotten the answer to the security question, please contact the support team to reset the password and security question.

Using HTTPS for device to TG communication

If you want to use HTTPS for the communication from device to Transport Gateway, then install the TG SSL certificate. By default, the current version of TG comes with Self-signed certificate that was part of previous releases. This is retained for backward compatibility. If you have some of your devices which are leveraging this certificate from previous TG releases, then you can continue to use that. However we strongly encourage using this new feature – **TG SSL Certificate**

This option is available once the TG is registered. It enables the users to generate and install Cisco CA signed TG SSL certificates on TG. The generated Certificates will be used for all the HTTPS communication from device to TG. Once you have generated these certificates, self-signed certificates that were part of TG are no more valid. For more detailed usages of these certificates, refer to the [Frequently Asked Questions](#) section.

Step 1 Go to **TG SSL Certificate**, you will get the below screen.

- Step 2** Common Name (Server name/IP address of the TG) is auto populated, and it is editable. It is strongly recommended that you enter the fully qualified domain name (FQDN) of the host (hostname) as common name. This will avoid re-generating the certificates in case the IP address of this host changes.
- Step 3** Enter details of Organization, Department, City, State/Province.
- Step 4** Select Country and Key Size
- Step 5** Click **Generate** to generate and install TG SSL certificates automatically.

Column	Description
Common Name	The fully qualified domain name that clients will use to reach this TG.
Organization	The exact legal name of your organization.
Department	Department within your organization, which you want to appear in the certificate. It will be listed in the certificate's subject as Organizational Unit, or "ou."
City	The city where your organization is legally located.
Country	The country where your organization is legally located
Key Size	Key Size to be used in encryption. Key size smaller than 2048 are considered insecure

The installed Certificate can be viewed from your browser using “View Certificate” option.

Certificate Hierarchy

▼ Cisco Licensing Root CA

▼ TG SSL CA

ctgw.cisco.com

Certificate Fields

Subject

▼ Subject Public Key Info

Subject Public Key Algorithm

Subject's Public Key

▼ Extensions

Certificate Key Usage

Certificate Basic Constraints

Certificate Policies

Certificate Subject Key ID

Field Value

C = UNITED STATES
ST = CALIFORNIA
L = San Jose
O = Cisco System Inc
OU = IT
CN = ctgw.cisco.com



Note

This option will not be available in **CSSM Satellite OVA** images.

Transport Gateway Processing of Call Home Messages

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

- HTTP
- EMAIL

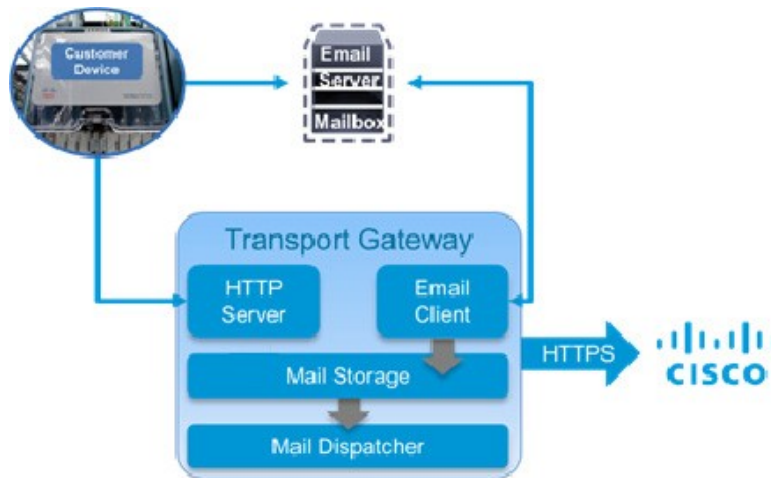


Figure 4-13 *Call Home message path through the Transport Gateway*

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 four hours. If messages cannot be sent to Cisco after four 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 under Registration tab.

Transport Gateway and SNTC Collectors

This section describes how to install Transport Gateway (TG) for SCH on Cisco hardware collector appliances. There are several supported host environments for the Transport Gateway application:

1. Customer-provided Windows or Linux host server
2. Customer-provided VMware ESX host server
3. Cisco hardware collector appliance (purchased via Smart Net Total Care)

Option 1 is covered in detail earlier in this chapter of the User Guide. Refer [Transport Gateway Requirements](#).

Option 2 applies to both SNTC and non-SNTC scenarios. For example, SNTC customers who have deployed the software version of the SNTC collector on a VMware host system may also install Transport Gateway as an additional VM on the same ESX host.

Option 3 scenarios as stated in below section.

Cisco Hardware Collector Appliance

The Transport Gateway application may be installed on Smart Net Total Care (SNTC) hardware collectors running CSPC version 2.4.1 or higher. In fact, SNTC hardware collectors purchased and shipped after December 2014 will include both Transport Gateway and the latest CSPC version in the factory software image. On these hardware collector appliances, Transport Gateway simply needs to be enabled using the steps described below:

Pre-Requisite:

- Cisco hardware collector appliance 2.4.1 or higher installed.
- Appropriate network IP configured.

Installing Transport Gateway on CSPC server:

SCH Transport Gateway is located at `/root/cstg/SCH.zip` of a CSPC server version 2.4.1 or higher.

-
- | | |
|---------------|---|
| Step 1 | Use console or SSH onto the CSPC server and login as super user. (If SSH is not enabled on the server than login as admin and enable ssh using command <code>ssh enable</code> .) |
| Step 2 | TG is stored in the SCH.zip file at <code>/root/cstg</code>
<code>[root@localhost collectorlogin]# cd /root/cstg</code> |
| Step 3 | Unzip <code>SCH.zip</code> file.
<code>[root@localhost cstg]# unzip SCH.zip</code> |
| Step 4 | Change director to SCH directory
<code>[root@localhost cstg]# cd SCH</code> |
| Step 5 | Install TG by running <code>install.sh</code> file.
<code>[root@localhost SCH]# nohup ./install.sh &</code> |

```

[root@localhost collectorlogin]# cd /root/cstg
[root@localhost cstg]# ls
SCH.zip
[root@localhost cstg]# unzip SCH.zip
Archive: SCH.zip
  creating: SCH/
  inflating: SCH/SCH-TG.tar.gz
  extracting: SCH/uninstall.sh
  inflating: SCH/install.sh
  inflating: SCH/info.xml
[root@localhost cstg]# cd SCH
[root@localhost SCH]# ls
info.xml  install.sh  SCH-TG.tar.gz  uninstall.sh
[root@localhost SCH]# nohup ./install.sh &
[1] 6641
[root@localhost SCH]# nohup: ignoring input and appending output to 'nohup.out'
^C
[1]+  Done                  nohup ./install.sh

```

Smart Call Home Transport Gateway is now installed and can be accessed by URL:

http://<ip-address>/transportgateway/



Note

If the URL does not load the UI page than there may be a need to update the IP Table. Execute the following commands to do IPtable updates on the server.

```

[root@localhost collectorlogin]# iptables -I INPUT -p tcp --dport 80 --syn -j ACCEPT
[root@localhost collectorlogin]# iptables -I INPUT -p tcp --dport 443 --syn -j ACCEPT

```

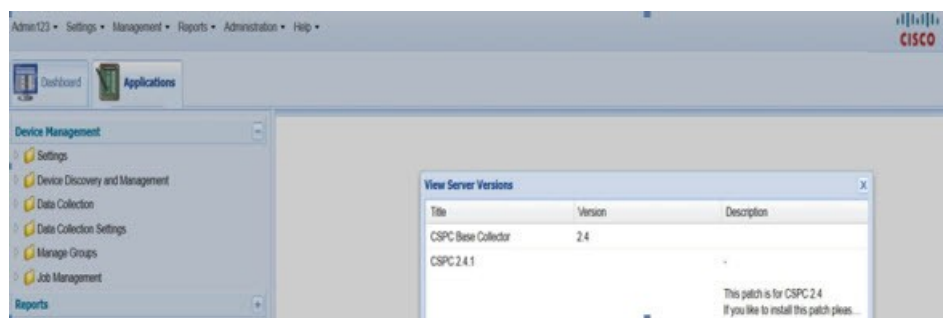
To further configure and customize the Transport Gateway, refer [SCH Deployment guide](#).

Earlier versions of the Cisco hardware collector appliance may be upgraded to CSPC 2.4.1 by using the software upgrade capability built into the appliance and documented here -

http://www.cisco.com/c/dam/en/us/td/docs/net_mgmt/inventory_and_reporting/CSPC_Quick_Start_Guide_for_SNTC.pdf

Once the CSPC version has been upgraded to 2.4.1 or later, the latest version of Transport Gateway may be downloaded from Software.cisco.com and install to the /root/cstg directory of the collector appliance.

To view the version of CSPC base collector, add-ons and other optional packages installed on CSPC on the **View Server Versions** screen. Once logged into CSPC, Select the **Help menu > About > View Versions**.



For more information about SNTC Deployment and/or the SNTC hardware collector appliance, please visit the [SNTC Support Community](#).

To Open a Support Case for Transport Gateway support:

1. Create a support case at the Cisco support website:
https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case?referring_site=shp_contacts_support_cases
2. Ensure to select the Product as "Smart Services Capabilities > Smart Call Home" so the right team is engaged.

To Open a Support Case for support on the collector appliance:

1. Create a support case at the Cisco support website:
https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case?referring_site=shp_contacts_support_cases
2. Ensure to select the Product as "Smart Services Capabilities > Collector and Inventory Uploads" so the right team is engaged.

Troubleshooting Cisco Transport Gateway Errors

Topics in this section include Transport Gateway problems dealing with:

- [Transport Gateway Configuration](#)
- [Transport Gateway Connectivity](#)
- [Transport Gateway Start Up](#)
- [Transport Gateway Operation](#)
- [Device to TG communication Troubleshooting](#)

Transport Gateway Configuration

The configuration scenario is related to specifying the IMAP folder name.

Cannot establish a connection to the Mail server Inbox

During configuration of the Transport Gateway, you want a connection to the mail server's Inbox but fails when trying to establish a connection

Symptom / Cause:

- The default mailbox folder name is INBOX for both the IMAP and POP3 protocol.

Fix:

Perform the following procedure to configure the Transport Gateway to receive Call Home mails from a mail folder other than 'Inbox'.

Step 1 Click **Configuration**.

- Step 2** Make sure you have selected the **IMAP** mail server type.
- Step 3** Provide the rest of the configurations and save the configurations.
- Step 4** Stop the service
- Step 5** Go to the following property in the
<TG_Install_Dir>/CSCOSchtg/tg/conf/an/properties/mailbox.properties
- Step 6** In the mailbox.properties file set the mail.imap.inbox value to the same target mailbox folder name as is noted in the mail server



Note The folder name might be a case sensitive based on your mail server configuration (e.g. Mail.imap.inbox=<folder name>)

- Step 7** Save the mailbox.properties file
- Step 8** Restart the Transport Gateway Service for immediate effect of the new mail folder configuration.



Note The default receiving mailbox folder name in the Transport Gateway cannot be modified while using the POP3 protocol. It can be done only when using the IMAP protocol.

Transport Gateway Connectivity

The following errors could be encountered when trying to obtain Transport Gateway connectivity:

- [Transport Gateway is not able to connect to the Cisco backend](#)
- [Cisco.com ID is invalid](#)
- [Unavailability of DNS results in failure](#)

Transport Gateway is not able to connect to the Cisco backend

When you click **Test Connection** on the Transport Gateway application, the following error message appears:

"The connection with the Cisco backend could not be established"

Symptom / Cause:

- User may not have configured the Transport Gateway with the correct proxy settings and proxy authentication.
- You may not have internet connectivity.
- The Cisco servers on the backend might be down.

Fix:

- Make sure your system has internet connectivity.
- If you are behind a firewall, then the respective proxy settings and proxy authentication information needs to be configured to the Transport Gateway.
- Delete the file **lb-truststore.jks** available at:
{TG_Install_Dir}\CSCOSchtg\tg\resources\security.
Restart TG service and try to test the connection again.

- Contact your IT representative for details on proxy settings, if they are not known.

Cisco.com ID is invalid

When you register the Transport Gateway and a message is displayed indicating that the Cisco.com ID is invalid.

Symptom / Cause:

- When you enter an invalid Cisco.com ID, the application will notify you about this problem via a pop-up message.
- To register a Transport Gateway a valid Cisco.com ID is required.

Fix:

- Verify if the entered Cisco.com ID is correct.
- If you do not have a valid Cisco.com ID then you can create a new Cisco.com ID via the Cisco.com Registration tool.

Unavailability of DNS results in failure

Symptom / Cause:

If the test connection fails due to unavailability of DNS

Fix:

-
- Step 1** Get the IP address of **tools.cisco.com**. Run the command *ping tools.cisco.com* from a host which has the internet connection.
- Step 2** Run the script *updateschurl.sh* (for Linux) OR *updateschurl.bat* (for Windows) in {TG_Install_Dir} /CSCOSchgtg/bin by passing the IP address obtained in Step1 as an argument.
Eg. *sh updateschurl.sh <IP address>*

Transport Gateway Start Up

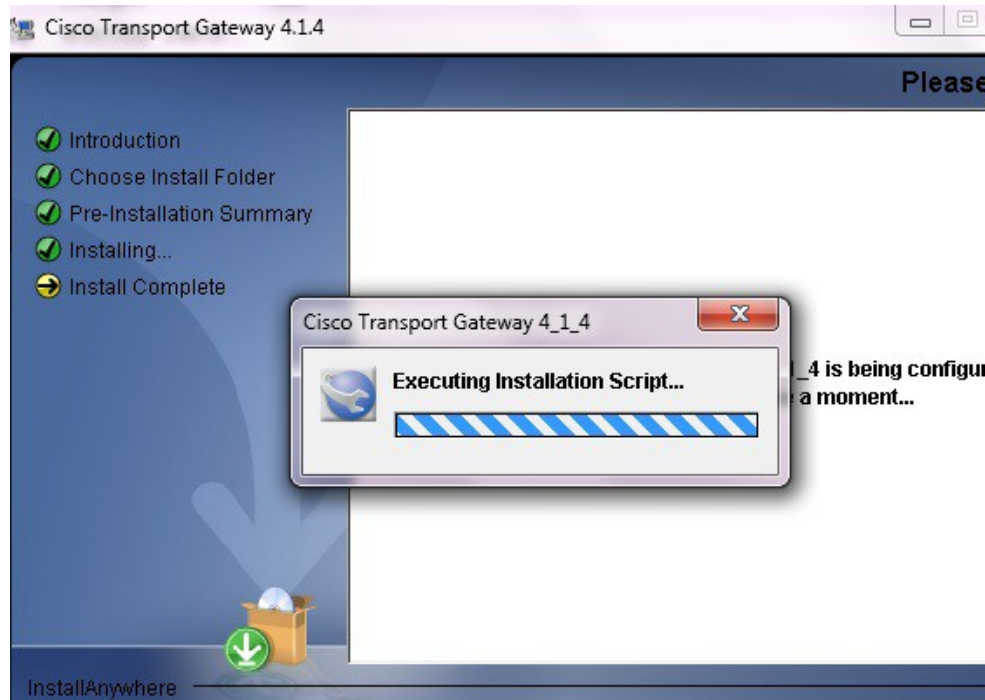
The following errors could be encountered when trying to start the Transport Gateway:

- [Transport Gateway Installation hangs](#)
- [Transport Gateway does not start in Windows Environment](#)
- [Transport Gateway does not start in Linux Environment](#)
- [Transport Gateway UI Does Not Load](#)
- [Transport Gateway does not start or remains in running mode for long time](#)

Transport Gateway Installation hangs

Symptom / Cause:

TG does not have the privileges to create a temporary folder as **Temp**, so hangs as shown in snapshot:



Fix:

- Kill the installation wizard using Windows Task manager.
- Create a folder name with name 'Temp' in the path:
`C:\Windows\system32\config\systemprofile\AppData\Local\`
- Install TG again. On the Installation wizard, click **Re-install**.

Transport Gateway does not start in Windows Environment

Symptom/Cause:

TG does not have the privileges to create a **Temp** folder and displays the following error on log.

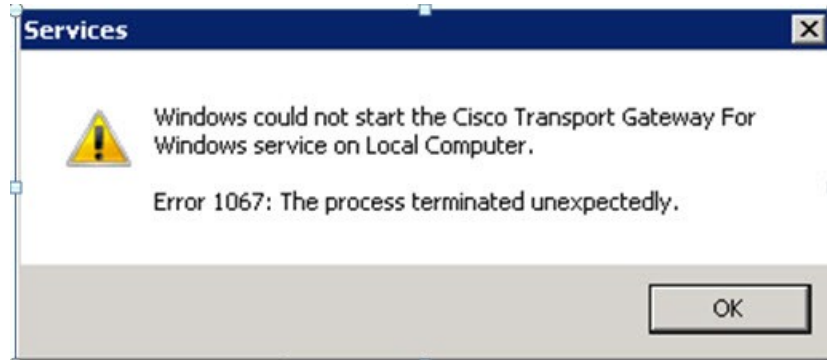
```
java.lang.IllegalStateException: Cannot create tmp dir in
C:\Windows\system32\config\systemprofile\AppData\Local\Temp\ for context
o.e.j.w.WebAppContext{/Transportgateway,null},C:\Program Files\Cisco Transport Gateway
4.1\CSCOSchtg\tg\WebContent at
org.eclipse.jetty.webapp.WebInfConfiguration.resolveTempDirectory(WebInfConfiguration.j
ava:309) at
org.eclipse.jetty.webapp.WebInfConfiguration.preConfigure(WebInfConfiguration.java:49)
at org.eclipse.jetty.webapp.WebAppContext.preConfigure(WebAppContext.java:430)
at org.eclipse.jetty.webapp.WebAppContext.doStart(WebAppContext.java:466)
at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:59)
at org.eclipse.jetty.server.handler.HandlerWrapper.doStart(HandlerWrapper.java:90)
at org.eclipse.jetty.server.Server.doStart(Server.java:262)
at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:59)
at
com.cisco.ca.csp.cso.conn.tg.httpserver.JettyHttpReceiver.doConnect(JettyHttpReceiver.j
ava:126)
at com.cisco.ca.csp.cso.conn.tg.service.RunTGService.<init>(RunTGService.java:115)
at com.cisco.ca.csp.cso.conn.tg.service.TGServiceMain.start(TGServiceMain.java:77)
at org.tanukisoftware.wrapper.WrapperManager.startInner(WrapperManager.java:2909)
```

```

at org.tanukisoftware.wrapper.WrapperManager.handleSocket (WrapperManager.java:3761)
at org.tanukisoftware.wrapper.WrapperManager.run (WrapperManager.java:4158) at
java.lang.Thread.run (Unknown Source)

```

Throws an error as in snapshot:



Fix:

- Create a folder name with name 'Temp' in the path:
`C:\Windows\system32\config\systemprofile\AppData\Local\`
- Start TG service.

Transport Gateway does not start in Linux Environment

Symptom / Cause:

- The Linux Environment does not have the required **libXp.so.6** library and receives the following error:

```

Exception in thread "main" java.lang.UnsatisfiedLinkError:
/opt/CSCOSchtg/_jvm/lib/i386/libawt.so: libXp.so.6: cannot open shared object file: No
such file or directory
    at java.lang.ClassLoader$NativeLibrary.load(Native Method)
    at java.lang.ClassLoader.loadLibrary0(Unknown Source)
    at java.lang.ClassLoader.loadLibrary(Unknown Source)
    at java.lang.Runtime.loadLibrary0(Unknown Source)
    at java.lang.System.loadLibrary(Unknown Source)
    at sun.security.action.LoadLibraryAction.run(Unknown Source)
    at java.security.AccessController.doPrivileged(Native Method)
    at sun.awt.NativeLibLoader.loadLibraries(Unknown Source)
    at sun.awt.DebugHelper.<clinit>(Unknown Source)
    at java.awt.Component.<clinit>(Unknown Source)
    at
com.cisco.zbase.app.transportgateway.service.ConfigureService.main(ConfigureService.ja
va:169)

```

Fix:

- TG expects the libXp.so.6 library to be available; need to install "xorg-x11-deprecated-libs" to fix this exception. Issue the following command:
- `[root@brontitall logs]# yum install xorg-x11-deprecated-libs`
- The issued command displays the following details:

```

Loading "fastestmirror" plugin
Loading mirror speeds from cached hostfile

```

```

* base: mirror.sanctuaryhost.com
* updates: ftp.lug.udel.edu
* addons: ftp.linux.ncsu.edu
* extras: mirrors.easynews.com
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package libXp.i386 0:1.0.0-8.1.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          Version           Repository Size
=====
Installing:
  libXp                i386          1.0.0-8.1.el5     base 23 k

Transaction Summary
=====
Install      1 Package(s)
Update      0 Package(s)
Remove      0 Package(s)

Total download size: 23 k
Is this ok [y/N]: y
Downloading Packages:
(1/1): libXp-1.0.0-8.1.el 100% |=====| 23 kB 0:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: libXp                                     ##### [1/1]

Installed: libXp.i386 0:1.0.0-8.1.el5
Complete!

```

Transport Gateway UI Does Not Load

Symptom:

Transport Gateway UI is not accessible on browser in Windows. The browser displays a message related to connection time out.

Cause:

Windows firewall might have blocked TG HTTP or HTTPs port.

Fix:

Check the firewall settings on the machine and configure firewall to allow TG HTTP or HTTPs port.

Symptom/Cause:

After installing the Transport Gateway in Linux, unable to load UI.

Fix:

Linux:

- Open hosts file from the location /etc/hosts
- Add new line to the existing entries [do not alter any existing entries]
 Entry : <<ip-address>> <<Hostname>> <<Domain-name>>
 Eg. x.x.x.x vm-xxxx-003 vm-xxx-003.cisco.com
- Save the entry and restart linux server
- Restart TG service and access the UI.

Symptom/Cause:

HTTP 500 Error: ClassNotFoundException: Unable to load UI

Fix:

Windows:

- Restart the Cisco Transport gateway Service from Windows service (Type services.msc in run prompt)
- Restart the machine after TG installation (Not Mandatory).

Symptom/Cause:

HTTP 500 Error: JasperException: Unable to load class for JSP

Fix:

Windows:

- Open Transportgateway Installation folder/directory and go to lib folder eg.C:\Program Files (x86)\Cisco Connectivity Transport Gateway 3.5\CSCOSchtg\tg\lib
- Perform this initial step : Restart the Cisco Transport gateway Service from Windows service (Type services.msc in run prompt).

Symptoms:

- TG is not accessible from the devices
- TG UI is not accessible from external hosts/machines

Cause:

- TG service would have bound to VMware Network Adapter IP address and this IP address is not reachable from other hosts or devices (This can happen if virtualization software like VMware workstation/player/fusion is installed on the same host/machine)
- IP address not reachable from other hosts or devices

Fix: Two troubleshooting scenarios:

Troubleshooting 1:

1. Find the IP address of the host where TG is installed. This IP address should be accessible from the other hosts or devices.
E.g. ipconfig on windows / ifconfig on linux
2. Edit the file
 <Install dir>CSCOSchtg\tg\conf\properties\jettyconfig.properties
3. Update jettyconfig.Host value with the IP address as derived from #1.
4. Update jettyconfig.auto.ip value to **false**.

5. Delete the file
`<Install dir>\CSCOSchtg\XML\ConfigHttp.xml`
6. Restart the TG service

Troubleshooting 2:

1. Find the IP address of the host where TG is installed. This IP address should be accessible from the other hosts or devices.
E.g. *ipconfig on windows / ifconfig on linux*
2. Launch the TG UI
3. Go to Http Settings under Configuration tab
4. Update the IP address as derived from #1.
5. Save the configurations
6. Restart TG service

Transport Gateway Uninstallation

Symptom:

Transport Gateway is not getting uninstalled completely

Fix:

Windows:

- Run **sc delete CONCSOSCHTG** from command prompt
- If TG is not getting uninstalled, run
REG DELETE HKEY_LOCAL_MACHINE\SOFTWARE\CONCSOSCHTG /f
from command prompt
- Remove the installation folder and restart the machine.

Transport Gateway does not start or remains in running mode for long time

If the Transport Gateway does not start or is in running state for longer time then follow a set of commands and manually start the TG service or check the status.

Symptom / Cause:

- The Transport Gateway is not started by following the steps of GUI.
- TG service is running

Fix: (for RDP)

- Browse to the **bin** folder of TG location
- To Start the TG service in the background execute `/opt/CSCOSchtg/tg/bin> ./start.script`
- To check whether the TG service is running or not execute
`/opt/CSCOSchtg/tg/bin> ./sh.script status`
- To stop the TG service execute
`/opt/CSCOSchtg/tg/bin> ./stop.script`

Transport Gateway Operation

For Linux after reboot

Symptom/Cause:

- TG service not running

Fix:

Start the service `./start.script` at `/opt/CSCOSchtg/tg/bin/`

Device to TG communication Troubleshooting

If using HTTP from device to TG:

1. Ensure TG is up and running
2. Ensure TG is reachable from device
 - Ping the TG host from device (either IP address OR host name as seen in "Device Service URL" under "HTTP Settings" of TG UI)
E.g. : ping {IP Address/Host}
 - Check if TG HTTP port is reachable from device
E.g. : telnet {IP Address/Host} {HTTP Port}
3. Ensure there are no ACLs or other security restrictions in your network which prevent the communications from device to TG.

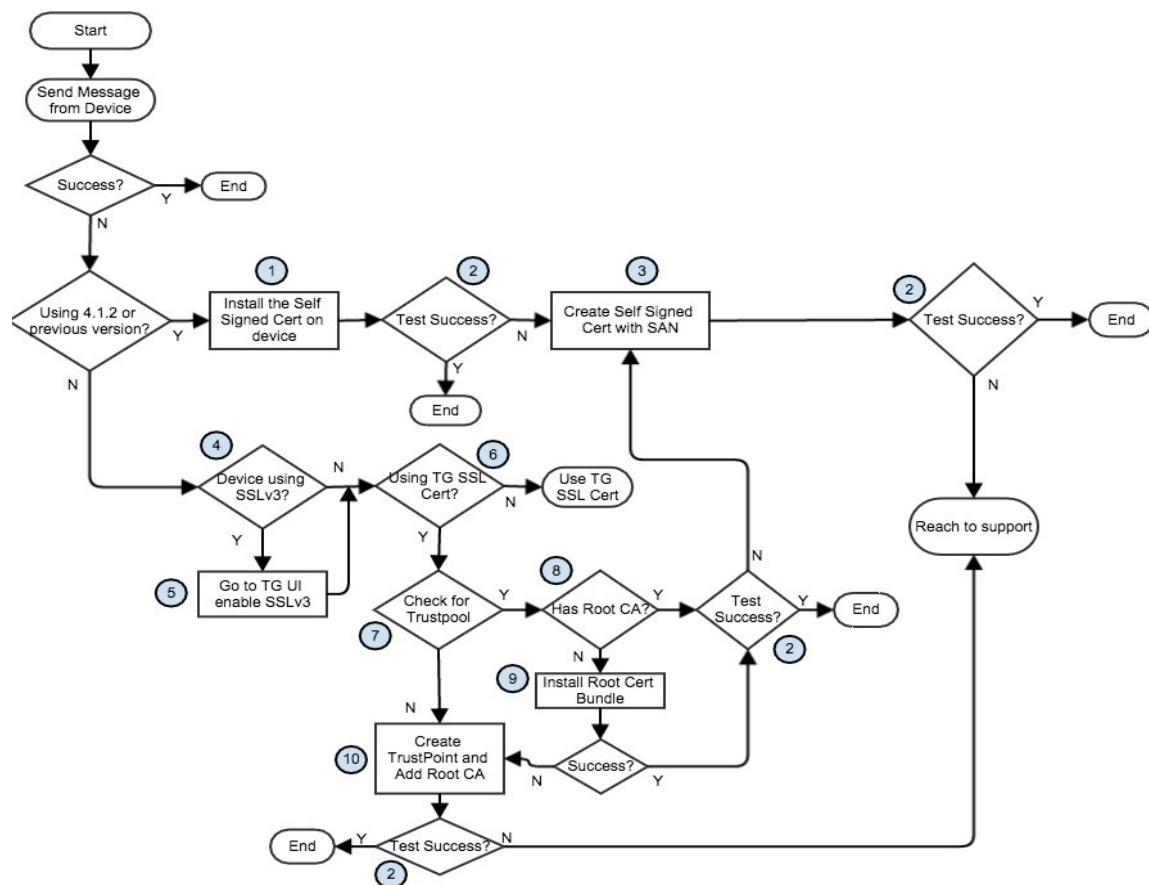
If using SMTP(Email) from device to TG:

1. Ensure you have successfully configured the Mailbox using "Mailbox Configuration" in TG UI.
2. Ensure device can connect to SMTP port on mail server
E.g. : telnet {IP address of mail server} {SMTP_PORT}
3. Ensure device IP address is allowed (white list) in the SMTP server relay list

If using HTTPS from device to TG:

Below flow chart will guide you to get the HTTPS working from device to TG. Please follow the numbers & their descriptions to understand how to verify at each step.

Figure 4-14 Using HTTPS from device to TG Flow Chart



1. Install the Self-signed certificate: Please follow the steps given below to install the Self-signed certificates that come along with TG on the device.

- Download [TG-HTTPS-Cert.zip](#) and unzip it to desired location
- Open the "tgserver.pem" file in a text editor
- Go to device console and issue the below commands:

```

configure terminal
crypto ca trustpoint cisco
enrollment terminal
revocation-check none
crypto ca authenticate cisco
  
```



Note

Copy and paste the base 64 encoded certificate from the text editor (obtained in step b). End with a blank line or type the word "quit" on a line.

2. **Test Success:** This step will help you to check if the HTTPS communication from device to TG is successful. As part of this step, you can trigger a message from device & check if it has reached TG. Refer to FAQs: [How to check if TG has received a message from device?](#)
3. **Create Self-signed Certificate with SAN:** This step will guide you to create a new Self-signed certificate with SAN (Subject Alternative Name) in it. Refer to [Appendix -A](#)
4. **Device Using SSLv3:** Here you will check if the device is using SSLv3 for SSL handshake. If your devices are using older OS images, then they might be using SSLv3. Refer to FAQs: [How to check if device is using SSLv3 for SSL handshake with TG?](#)
5. **Goto TG UI enable SSLv3:** If you detect device using SSLv3, then HTTPS from device to TG will not work. This is because from TG 4.1.3 SSLv3 is disabled due to security vulnerabilities. You will have to go to TG UI and enable it by accepting the security risks. You can do so by going to “Http Settings” tab under “Configuration” section of TG UI.
6. **Using TG SSL Cert:** If you have used the “TG SSL Certificate” feature to generate the Cisco CA signed certificates, then the answer is YES.
7. **Check for Trustpool:** Some devices have trustpool feature. Please follow the steps given in FAQ ([Frequently Asked Questions](#) to check if the device is having trustpool.- [How to verify if my device has trustpool or not?](#)
8. **Has Root CA:** Here you will check if the trustpool has the “Cisco Licensing Root CA” certificate in it. If yes, then the HTTPS communication from device to TG will work seamlessly. Please follow the steps given in FAQ ([My device has trustpool, but how do I know if the trustpool has the Cisco Licensing Root CA?](#)) to check if the trustpool is having Cisco Licensing Root CA.
9. **Install Root Cert Bundle:** If the device trustpool doesn’t have the Cisco Licensing Root CA, then you can install the latest Root Cert Bundle. Please follow the steps given in FAQ (TG SSL Certificates Frequently Asked Questions - [My device trustpool does not have the Cisco Licensing Root CA. How do I install it?](#)) on how to install the Root Cert Bundle.
10. **Create Trustpoint and Add Root CA:** Here you can add the Cisco Licensing Root CA certificate manually onto the device by creating a trust point. Please follow the steps given in FAQ (TG SSL Certificates Frequently Asked Questions - [My device trustpool does not have the Cisco Licensing Root CA. How do I install it?](#)) on how to create a trustpoint on device and add the certificate.

Frequently Asked Questions

[TG SSL Certificate FAQs](#)

[General TG Operational FAQs](#)

TG SSL Certificate FAQs

- Q.** What are the advantage of using SSL Certificate option?
- A.** If your devices are having the trust pool feature and the trust pool has “Cisco Licensing Root CA” certificate, then HTTPS from device to TG will work seamlessly without any manual intervention.
- Q.** How to verify if my device has trustpool or not?

- A.** Execute the below command on device console. If the device has trust pool, then it will display the certificates that are part of trust pool.

For **IOS/IOS-XE**: *crdc_ch1921#sh crypto pki trustpool*

For **NX-OS/IOS-XR**: *crdc_ch1921# show crypto ca trustpool*

- Q.** My device has trustpool, but how do I know if the trustpool has the Cisco Licensing Root CA?

- A.** Go to device console and execute the below command:

For **IOS/IOS-XE**:

```
crdc_ch1921#sh crypto pki trustpool | i Licensing Root CA
cn=Cisco Licensing Root CA
cn=Cisco Licensing Root CA
```

For **NX-OS/IOS-XR**:

```
crdc_ch1921#show crypto ca trust pool | i Licensing Root CA
cn=Cisco Licensing Root CA
cn=Cisco Licensing Root CA
```

- Q.** My device trustpool does not have the Cisco Licensing Root CA. How do I install it?

- A.**

- Goto device console
- Issue these commands

```
O2_bot#conf t
```

```
O2_bot(config)#crypto pki trustpool import url
http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
E.g.: O2_bot#conf t
```

```
O2_bot(config)#crypto pki trustpool import url
http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
Translating "www.cisco.com"...domain server (xx.xxx.xx.xxx) [OK]
```

```
Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
% PEM files import succeeded.
```

- Q.** My device does not have trustpool. How can I use this feature?

- A.** In this case you need to create the trustpoint. Download the [TG_SSL_Certificate.zip](#) file from Cisco.com and extract it. Open the "CiscoLicensingRootCA.cer" in a text editor.

Follow these commands on device console:

```
O2_bot#conf t
```

```
O2_bot(config)#crypto pki trustpoint {trust point name}
```

```
O2_bot(ca-trustpoint)#enrollment terminal
```

```
O2_bot(ca-trustpoint)#revocation-check none
```

```
O2_bot(ca-trustpoint)#exit
```

```
O2_bot(config)#crypto pki authenticate {trust point name}
```

```
<Paste the contents of the certificate from the text editor here>
```

E.g.:

```
O2_bot#conf t
O2_bot(config)#crypto pki trustpoint LicRoot
O2_bot(ca-trustpoint)#enrollment terminal
O2_bot(ca-trustpoint)#revocation-check none
O2_bot(ca-trustpoint)#exit
O2_bot(config)#crypto pki authenticate LicRoot
Enter the base 64 encoded CA certificate.
End with a blank line or the word ""quit"" on a line by itself
<Enter your certificate here>
```

Certificate has the following attributes:

```
Fingerprint MD5: 1468DC18 250BDFCF 769C29DF E1F7E5A8
Fingerprint SHA1: 5CA95FB6 E2980EC1 5AFB681B BB7E62B5 AD3FA8B8
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported"
```

Q. How to check if device is using SSLv3 for SSL handshake with TG?

A. Please run these commands on devices:

For IOS/IOS-XE:

```
debug ssl openssl errors
debug ssl openssl ext
debug ssl openssl msg
debug ssl openssl states
```

For IOS-XR:

```
debug ssl errors
debug ssl ext
debug ssl msg
debug ssl states
```

And then try to send the message from device again. Check the device logs for occurrences of below string:

SSL_connect:failed in SSLv3 read server hello A

If you find any matches, that means that device could be using SSLv3 for the SSL handshake.

General TG Operational FAQs

Q. How to check if TG is up and running?

A.

Linux:

- Go to {TG_Install_Dir}/CSCOSchtg/tg/bin/
- Execute command: *./sh.script status*

Windows:

- Go to services console

– Check if the TG service (Cisco Transport Gateway For Windows) is running

Q. How to check if TG has received a message from device?

A. Open the TG log file (StatusOfTG.log) and search for below lines:

Using **HTTP/S** between device and TG:

Received a message over HTTP/S on TG.....

Using **CSSM Satellite** image:

Received a SL message to be processed via Lindos.....

Using **SMTP** between device and TG:

com.cisco.ca.csp.cso.conn.tg.email.MailHandlerImpl - New Call Home message found!

Q. How to check if the TG message store has reached its limit?

A. Open the TG log file (StatusOfTG.log) and search for below command line:

isDiscOverflow :true

Q. How to check if the message has been successfully sent to Cisco from TG?

A. Open the TG log file (StatusOfTG.log) and search for below line: