Smart Call Home

Deploying theTransport Gateway on Cisco Unified Computing System and Red Hat Linux

Deployment Guide

For further information, questions and comments please contact ask-smart-services@cisco.com

Contents

Introduction **3**
Purpose and scope 3
When to use the Transport Gateway 3
Transport Gateway solution **4**
Test environment 4
Operating System installation and configuration 4
Configure proxy settings and register 5
Configure HTTP settings 6
Configuring a Nexus 7000 using the HTTP transport 7
Validating the HTTP transport 7
Conclusion **8**
For More Information **8**

Introduction

Purpose and scope

This document demonstrates how to create a self-contained Transport Gateway, an optional proxy for Cisco® Smart Call Home messages.

The validation includes:

- Installation of Red Hat Linux, including all required packages
- Configuring Linux to support the Transport Gateway
- Obtaining and installing the Transport Gateway
- Registering the Transport Gateway

When to use the Transport Gateway

While the embedded nature of Call Home is a great benefit, it can also pose a challenge when security policy or network configuration do not allow direct communication between Call Home on managed devices and the Smart Call Home servers at Cisco.com.

In those cases, an optional Transport Gateway is available to act as a proxy for Smart Call Home messages. The Transport Gateway is a software package obtained from Cisco.com that can be installed on 64 bit Windows Server 2008 R2, Windows XP, and Redhat Enterprise Linux. It is typically installed on a server and placed in the network where it can receive messages from managed devices and relay those messages to the Smart Call Home servers at Cisco.com.

The Transport Gateway is not required when:

- All devices can send messages directly to Cisco.com using HTTPS
- The encryption capabilities of all managed devices meet the customer's security requirements

The Transport Gateway is required when:

- Managed devices do not have direct access to Cisco.com
- An HTTP proxy server is required to reach Cisco.com
- Encryption is required for devices that support SMTP communication only

The Transport Gateway is desirable when:

- The customer wishes to inspect unencrypted traffic on the LAN while securely communicating over the Internet
- The customer wishes all outbound traffic to be sourced from a single device
- The customer does not wish to install a certificate on every managed device
- The customer wishes to use SMTP on the LAN while communicating securely over the Internet

Transport Gateway solution

In this solution, a Transport Gateway is installed on a Cisco UCS® C200 running Red Hat Enterprise Linux 6.1. The Transport Gateway receives messages from test devices and uses a HTTP proxy server to communicate with Cisco.com. A Cisco Nexus® 7000 is configured to send messages to the Transport Gateway using HTTP.

Test environment

The test lab contains the following devices:

- Cisco Nexus 1000v, 2000, 3000, 5000, 6000, 7000
- Cisco UCSM managing UCS-B and UCS-C Series Rack Servers
- Cisco MDS 9100 Series Multilayer Fabric Switches
- Cisco Integrated Services Router (ISR)
- Cisco ASA 5500 Series Next-Generation Firewall

All interfaces, including management and switch virtual interfaces (SVI), share a single subnet. When possible, Smart Call Home is configured to communicate via the management interface. All outbound traffic passes through a Cisco ASA. All of the devices are covered under active Cisco SMARTnet® contracts and all supported devices are registered with Smart Call Home.

Note: HTTP (port 80) and HTTPS (port 443) must be allowed through the local firewall.

The Cisco.com account used to register and manage devices and the Transport Gateway in Smart Call Home represents a customer with a Cisco SMARTnet or Smart Net Total Care contract. The user's profile contains all of the SMARTnet contracts covering lab devices.

In this example, the vSphere console and virtual media are used to install the operating system. A secure remote session is used to upload and install the Transport Gateway software.

Operating System installation and configuration

Step 1. Download and install 64-bit RedHat Enterprise Linux version 6.5. When prompted, choose the Basic Server option. Otherwise, use all default values.

Step 2. Download the Linux installer for the Transport Gateway from Cisco.com using your browser and Cisco.com ID.

Step 3. Once the operating system is fully installed, copy the installer zip file to the Linux server using a secure copy (SCP) client. In this example, the installer was copied to /root/Downloads.

Step 4. Connect to the server using a secure shell (SSH) client and logon as root or other privileged user account in accordance with your security policies. In this example, the Transport Gateway installation is performed as root.

Step 5. Unzip the installer zip file and change to the SCH-TG directory.

Step 6. Run the command **chmod +x install.sh**

Step 7. Run the install.sh file (**./install.sh**).

Figure 1. Installation commands

```
[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
```

Configure proxy settings and register

Step 1. In the secure shell, execute **/opt/CSCOSchtg/tg/bin/start.script** to start the Transport Gateway service.

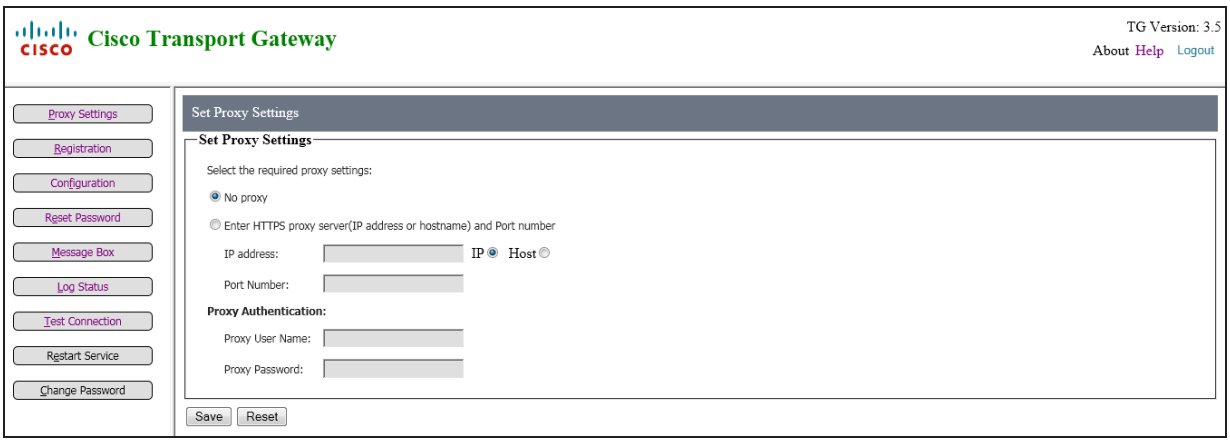
Note: The Transport Gateway service is registered as a daemon but must be started manually following a reboot.

Step 2. In a browser, go to **http://<ip-address>/Transportgateway** to access the Transport Gateway application.

Step 3. Log in with the default username and password **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. Using a proxy is optional.

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

Figure 2. Configure HTTPS proxy



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 (Figure 3).

Step 7. Enter the password associated with the automatically populated Cisco.com ID (optional), 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 change to **Registered**.

Figure 3. Registered Transport Gateway

Configure HTTP settings

The Transport Gateway uses two methods to process Call Home messages: sending the Call Home message directly to the HTTP server in the Transport Gateway or using an external mail server. In this scenario, we use HTTP to send Call Home messages from the device to the Transport Gateway. To configure the HTTP settings:

Step 1. Click **Configuration** and then click the **HTTP Settings** tab (Figure 4).

Step 2. Check the Send Call Home Messages checkbox to upload Call Home messages to Cisco.com.

Note: The “Send Call Home Messages” option must be checked in order to realize the full benefits of Smart Call Home.

Step 3. 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. To do this, click **Restart Service** in the Transport Gateway application GUI.

Figure 4. HTTP Settings

Configuring a Nexus 7000 using the HTTP transport

Configure a device to send messages through the Transport Gateway using the HTTP protocol. If possible, choose a device that is already registered with Smart Call Home and verify that the device can send an inventory message to the Smart Call Home servers before modifying the configuration. Remove any existing destination-profile http targets and enter a new command with the Device Service URL (from HTTP settings configuration window, Figure 10). In the example we use:

```
destination profile CiscoTAC-1 http http://10.88.114.86:80/Transportgateway/services/DeviceRequestHandler
```

Validating the HTTP transport

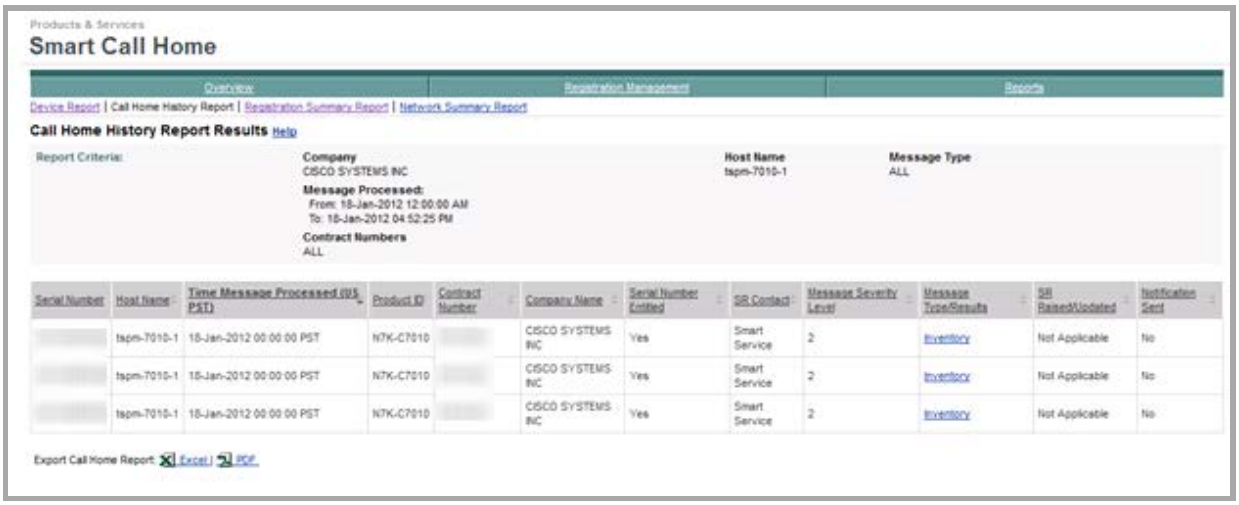
To test the path, send an inventory message from the device through the Transport Gateway. To do this, issue the command **callhome test inventory** (Figure 5) on the device.

Figure 5. Testing the path through the Transport Gateway

```
tspm-7010-1#
tspm-7010-1#
tspm-7010-1# callhome test inventory
trying to send test callhome inventory message
successfully sent test callhome inventory message
warning:
email configuration incomplete for destination profile:full_txt
email configuration incomplete for destination profile:short_txt
tspm-7010-1#
```

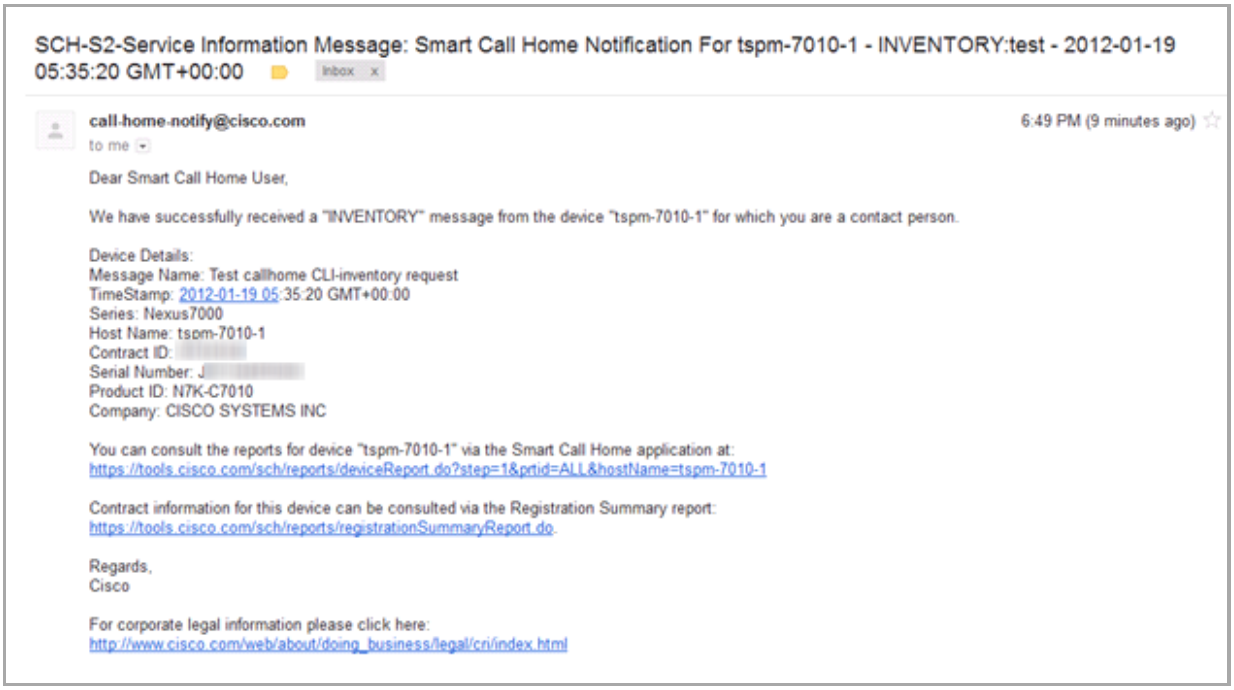
To verify that an inventory message was received from the test device, browse to the Smart Call Home portal. Click the **Reports** link, and then click the **Call Home History Report** link. Fill in the appropriate parameters and click **Run Report** to verify that an inventory message was received from the test device.

Figure 6. Call Home history report results



All admin contacts for the test device receive an email indicating that an inventory message was received. By default this email is delivered to the user that initially registers the test device (Figure 7).

Figure 7. Example inventory email


SCH-S2-Service Information Message: Smart Call Home Notification For tspm-7010-1 - INVENTORY:test - 2012-01-19 05:35:20 GMT+00:00

Inbox ×

call-home-notify@cisco.com 6:49 PM (9 minutes ago)

to me

Dear Smart Call Home User,

We have successfully received a "INVENTORY" message from the device "tspm-7010-1" for which you are a contact person.

Device Details:
Message Name: Test callhome CLI-inventory request
TimeStamp: 2012-01-19 05:35:20 GMT+00:00
Series: Nexus7000
Host Name: tspm-7010-1
Contract ID:
Serial Number: J
Product ID: N7K-C7010
Company: CISCO SYSTEMS INC

You can consult the reports for device "tspm-7010-1" via the Smart Call Home application at:
https://tools.cisco.com/sch/reports/deviceReport.do?step=1&prtid=ALL&hostName=tspm-7010-1

Contract information for this device can be consulted via the Registration Summary report:
https://tools.cisco.com/sch/reports/registrationSummaryReport.do.

Regards,
Cisco

For corporate legal information please click here:
http://www.cisco.com/web/about/doing_business/legal/cri/index.html

Conclusion

The Transport Gateway is an optional component of Smart Call Home that is used to securely proxy messages when direct connectivity from a managed device to Cisco.com is not possible.

In this guide, we

- explored the need for the Transport Gateway in varying environments
- validated the installation and configuration of the Transport Gateway on Cisco UCS and Red Hat Linux

For More Information

The Cisco Smart Call Home website offers a full range of online resources to help you use Smart Call Home. Join the Cisco Support Community for Smart Call Home to learn more about the capability by interacting with networking peers and experts worldwide. Chapter four of the *Smart Call Home User Guide* provides additional information about the options in the Transport Gateway application.

For more information about Cisco SMARTnet Service, visit www.cisco.com/go/smartnet or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 7/14