CHAPTER 6

References

See the following items for additional information about Call Home feature and Smart Call Home service:

- For more information.
- Resources for Smart Call Home.
- Terminology.
- CA Root Certificate Update Process.

For More Information

For more information about Smart Call Home, there are several options available, you can:

- "Smart Call Home Service Introduction - http://www.cisco.com/en/US/products/ps7334/serv_home.html
- Smart Call Home presentation
- Catalyst 6500 Call Home Configuration Guide – http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00801609ea.html
- Catalyst 6500 Command Reference – http://cisco.com/en/US/products/hw/switches/ps708/products_command_reference_book09186a0080160cd0.html
- Generic Online Diagnostics on the Cisco Catalyst 6500 Series Switch – http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd801e659f.shtml
- Cisco Catalyst 6500 Series with Cisco IOS Software Modularity – http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletin0900aecd80313e15.html
- Embedded Event Manager (EEM) on the Cisco Catalyst 6500 Series – http://cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd805457c3.shtml
- Cisco 7600 Series Command References - http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX - http://www.cisco.com/en/US/partner/docs/routers/7600/ios/12.2SXF/configuration/guide/swcg.html

- CiscoDevice Diagnostics User Guide for PartnersSmart Call Home 4.2.4.1 7600 Series Technical References - http://www.cisco.com/en/US/products/hw/routers/ps368/prod_technical_reference_list.html
- Cisco 7600 White Papers - http://www.cisco.com/en/US/products/hw/routers/ps368/prod_white_papers_list.html
- Use the feedback box on the Smart Call Home web application
- Access the Smart Call Home Technical Overview – http://www.cisco.com/application/pdf/en/us/guest/products/ps7334/c1266/cdccont_0900aecd8063c595.pdf
- Contact Smart Call Home at email address – sch-support@cisco.com

Resources for Smart Call Home

For more information about Smart Call Home:

- Smart Call Home Support Community
  http://www.cisco.com/en/US/products/ps7334/serv_home.html
- Smart Call Home on Cisco.com
  http://www.cisco.com/en/US/products/ps10600/tsd_products_support_series_home.html
- Smart Call Home web application (portal)
  https://tools.cisco.com/sch

Terminology

The following list defines the different components, tools and terms used in Smart Call Home:

- **Call Home (CH)** – Product feature in IOS version 12.3(33)SXH that uses SMTP or HTTP connections established with a configurable destination to send formatted messages. The messages contain Inventory or Configuration information that are collected at scheduled intervals. Configuration, Diagnostics, Environmental, Inventory or System Log (syslog) information is collected during real-time events; Test, Inventory, Configuration Diagnostic and Environmental information are collected on-demand.

The IOS code incorporates device diagnostics (i.e. GOLD) that enables the sending of the following outbound alerts and alarms in email messages to Smart Call Home.

- **Call Home Alert Group** – Is a configurable Call Home feature that groups detectable events from one of the Configuration, Diagnostics, Environmental, Inventory or System Log categories for monitoring.
- **Call Home Profile** – Is a configurable Call Home feature that provides a structure to bundle together several Alert Groups, to select transport methods, to assign multiple destination addresses and to specify message format options.
- **Call Home message formats** – Are configurable formatting options used by the IOS Call Home feature when creating messages. The Short Text format is suitable for pagers or printed reports and the Long Text format contains Full formatted message information suitable for human reading. The XML Messages contain the same data as the Long Message, but with the addition of XML tagging and AML specific transport information to allow machine-readable parsing and routing of the message in the Smart Call Home System.

- **Call Home message type** – Is a field within an IOS Call Home message that indicates what type of message it contains: Configuration, Diagnostics, Environmental, Inventory, Test or System Log (syslog) information.
- **Call Home message sub-type** – Is a field within an IOS Call Home message that indicates that the message contains full or delta Configuration or Inventory information, Gold major, minor or normal Diagnostics information, minor or major Environmental information, Test or System Log (syslog) information.
- **Cisco.com profile** – Where information on Cisco contracts, case management permissions and user's company are kept for use by the Smart Call Home service.
- **Cisco Backend (CBE)** – Contains a collection of various tools and information:
  - Smart Call Home service.
  - Guided searches for the Smart Call Home reporting process.
  - Generation of customized reports for Smart Call Home users.
  - Device install-base data and their associated contracts.
  - Customer device-based troubleshooting tools.
- **Cisco Contracts**:

  Contract information is kept in the Cisco.com profile. A customer can register a device using one of the following types of branded contracts:
  - **Cisco Branded – Direct**: Customer bought product directly from Cisco and contacts Cisco directly if they need support.
  - **Cisco Branded – CBR (Cisco Branded Reseller)**: Customer bought product from Cisco reseller and customer contacts Cisco directly if they need support.
  - Other types of contracts will become supported in a future release.
- **Customer Specific Network Alerts** – Smart Call Home supports the following Call Home message types:
  - **Configuration** – Contains image name and feature, running and startup configs, SW features technologies and sub-technologies.
  - **Environment** – Contains information about environmental alarms for the device clock, VTT, power supply and modules. Depending on the type of alert, a notification is sent to the customer and a Service Request is generated.
  - **GOLD** – Contains information about diagnostic tests, what tests were run, their status, and results. Depending on the type of failure, a Service Request is generated.
  - **Inventory** – Contains information about the device, software, modules.
  - **Test** – Contains information that is common to all message types. The content of test messages is not processed by Smart Call Home and hence no specific message processing results will be available for test messages.
  - **Embedded Event Manager (EEM)** – Detects real time events and takes action based on a pre-defined rules policy. EEM has event detectors with which Call Home registers; the registration is dependent upon which alert-groups the EEM profile is configured. The profile can subscribe to alert-groups for the following type events:
    - GOLD diagnostic
    - Environmental
    - Configuration

    - Inventory

- **Generic Online Diagnostics (GOLD)** – Provides a common command-line interface (CLI) for manually generating Smart Call Home messages and scheduling run-time diagnostics.

  GOLD can detect faults in hardware and provides the triggers that proactively engage high-availability features and actions, such as the switch-hitter of modules or turning off modules or individual ports. The GOLD test suite also gives support personnel the tools to test the functioning of hardware modules and troubleshoot down to the field-replaceable unit (FRU) level.

- **Smart Call Home service**– Is a service that captures and processes Call Home diagnostics and inventory alarms that are sent from a device containing the Smart Call Home feature. This service provides proactive messaging that resolves issues before they become problems and for those problems that occur, resolving them faster using enhanced diagnostics

- **Smart Call Home Client** – A device that sends or forwards IOS Call Home or other supported messages to Smart Call Home using SMTP or HTTPS connections; the messages must be registered with the Smart Call Home system.

- **Smart Call Home supported messages** – Currently is an AML/XML message, created by a device using the IOS Call Home Feature, that contains Configuration (full), Diagnostics (major & minor), Environmental (major & minor), Inventory (full), Test or System Log information.

- **Transport Gateway (TG)** – Securely transports Call Home messages from the customer hardware to the Smart Call Home service on the Cisco Backend. A Smart Call Home software client that runs on a device under the Windows 2000, Windows 2003, Windows XP, Solaris or Linux operating systems. The Transport Gateway acts as an intermediary device and is capable of forwarding supported messages collected from Smart Call Home Client devices and sends them to the Smart Call Home System using an HTTPS connection.

CA Root Certificate Update Process

Periodically, Cisco updates security credentials to ensure the continued secure communications to the Smart Call Home back-end. This section applies to those who are using the HTTPS method for communicating to the back-end.

When there is a security credential update from Cisco, instructions will be sent via e-mail to SCH-registered user e-mail addresses that are linked to a valid CCO ID. Instructions for updating security credentials are as follows:

- HTTPS Certificate Process for Nexus 7000 Devices uses either the "chained" certificate content from this section of the Smart Call Home User Guide, or use the combined contents of the certificate files in the QuoVadisRootCA2.zip file.

HTTPS Certificate Process for Nexus 7000 Devices

There are two different time frames when you will be using HTTPS certificate content on your Nexus 7000 device, when you are:

- Adding the certificate to a Nexus 7000 device, for the first time; you will perform the steps and use the certificate data identified below in this document.
- When you are updating an expired security certificate on a Nexus 7000 device, you will use the script files and certificate data contained in the QuoVadisRootCA2.zip file.

Adding the Certificate to a Nexus 7000 Device

For Nexus 7000 devices, use the following instructions to install a security root certificates chain:

- Copy the root certificates chain below.
- Configure a trust-point and prepare to enroll the certificate via the terminal using copy and paste when prompted.

```
NX-7000(config)#crypto ca trustpoint cisco
NX-7000(config-trustpoint)#enroll terminal
NX-7000(config-trustpoint)#crypto ca authenticate cisco
Input (cut & paste) the CA certificate (chain) in PEM format.
```

IMPORTANT: PLEASE COPY THE CERTIFICATE CONTENT BELOW USING A PLAIN TEXT EDITOR AND PASTE THE CONTENT AS PLAIN TEXT; THIS REMOVES ANY POSSIBLE FORMATTING SYMBOLS, WHICH ALTER THE CERTIFICATE CONTENT.

Note Your copy of the security certificate should include each and every character, including the certificate markers. Remove any blank lines either after or before the certificate markers.

```
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
```

On the next line following the certificate content, end the input by entering **END OF INPUT:**

Hit **Enter**, a prompt appears asking "Do you accept this certificate? [yes/no]:"; enter **yes**

Exit configuration mode and save the configuration -

NX-7000(config)#**end**

NX-7000#**copy running-config startup-config**

Downloading a New Certificate for a Nexus 7000 Device

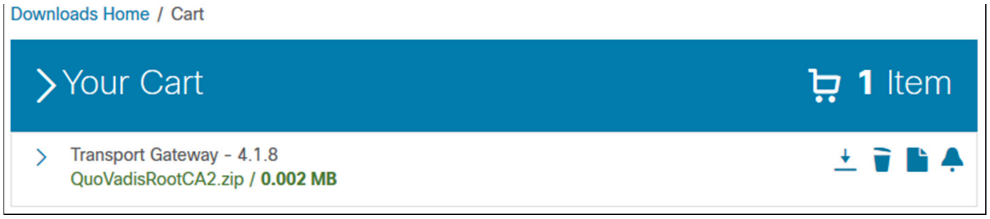
If you need the new certificate files that comprise the CA Root certificate, perform the following steps:

Go to the following URL:

https://software.cisco.com/download/home/282152778/type/283490182/release/4.1.8

On the Download Software window, click the **Download Now** button for the **QuoVadisRootCA2.zip** file

Figure 6-1 Downloading a certificate



Transport Gateway - 4.1.8
QuoVadisRootCA2.zip / 0.002 MB

Unzip the **QuoVadisRootCA2.zip** file to the directory of your choice.

Additional Information

For more information on the SSL certificate, see the information at the following URL:

https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

For technical support, **Email:** tac@cisco.com<mailto:tac@cisco.com>

Telephone:

US and Canada:	**+1-877-330-9746**	
Europe:	Austria	0800 006 206
	Belgium	0800 49913
	France	0805 119 745
	Germany	0800 589 1725
	Italy	800 085 681
	Netherlands	0800 0201 276
	Spain	800 600472

US and Canada:	**+1-877-330-9746**	
	Switzerland	0800 840011
	UK	0800 2795112

From the rest of the world, choose the appropriate phone number from http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html