Smart Call Home Security

Cisco® Smart Call Home–enabled devices perform proactive diagnostics on their own components to provide alerts and remediation advice when an issue is detected. Smart Call Home identifies problems on your devices before they can affect business operations and securely communicates vital device information to a Cisco data center, where it is analyzed against Cisco's deep knowledge base, which includes manufacturing and technical support information.

Introduction

The focus of this document is to address security considerations when deploying Cisco Smart Call Home. Additional resources for Smart Call Home are listed in the For More Information section of this document.

Call Home is a product feature embedded in the operating system of Cisco devices. It detects and notifies the user of a variety of fault conditions. The Call Home feature must be enabled during device configuration. Smart Call Home is a service capability that adds Cisco intellectual capital as well as automation and convenience features that enhance the basic Call Home functionality. Smart Call Home is included with most Cisco service contracts, including Cisco SMARTnet® and Smart Net Total Care. To use Smart Call Home, the device must be registered through the Smart Call Home portal.

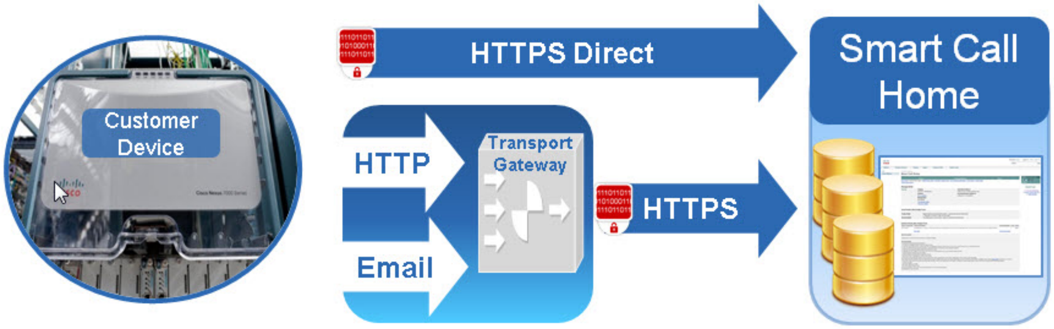
Information is delivered to network administrators and users through the Smart Call Home portal. The portal provides information about the devices on your network that have Smart Call Home enabled. This includes diagnostics, inventory, configuration, product alerts, and remediation recommendation information.

Secure Data Transport to the Cisco Data Center

Transport Options

Three transport options are available when using Smart Call Home (Figure 1): HTTPS direct, email using the transport gateway, and HTTP using the transport gateway.

Figure 1. Data Transport Options for Smart Call Home



HTTPS Direct

HTTPS direct is the recommended and most commonly used method. Very few devices do not support the HTTPS direct method. Those that do not need to use a transport gateway.

HTTP or SMTP to the Transport Gateway, HTTP to Cisco

Although the embedded nature of Call Home is a great benefit, it can also pose a challenge when security policy or network configuration does 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 7, 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 using HTTPS.

The transport gateway is not required when:

- All devices can send messages directly to Cisco.com using HTTPS
- 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 (see the Quick Start Guide for each supported product to understand what transport methods are possible)

The transport gateway is desirable when:

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

Security Considerations While Using a Transport Gateway

Using the transport gateway allows customers to send unencrypted traffic from the device to the transport gateway. Security policies can then be applied against that data before it departs the customer network premises. If using

SMTP to the transport gateway, customers can view their messages in the inbox of their mail server, or, during device configuration, they can add their email address and receive a copy of every message from the device. Using HTTP to the transport gateway, data packets can be analyzed (between the device and the transport gateway) using a packet analyzer.

Consider the following security information when using the transport gateway:

- The SMTP protocol is not encrypted, so the patch 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, is masked before leaving the device to mitigate exposure within the LAN or over the Internet.
- It is recommended that the transport gateway be 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, because 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 because the traffic is part of an existing session.
- As part of transport gateway registration, the transport gateway sends a registration request to the Cisco back end. The Cisco back end 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 back end after the initial registration.
- This communication is through HTTPS and using port 443; see Chapter 4 of the Smart Call Home User Guide 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 an HTTPS proxy server.

Data Privacy

Data Privacy Feature

One of the ways Smart Call Home helps customers identify and resolve problems more quickly is by automating interactions with the Cisco TAC. Call Home automatically uploads items that are frequently required by the TAC to resolve issues, including the saved and running configurations.

To limit privacy or compliance issues, the configuration upload feature is optional and turned off by default. When enabled, Call Home masks any sensitive data not relevant to the support process. Data is masked in the device so that it never traverses the LAN or the Internet. Masked data includes usernames, passwords, email addresses, and community strings.

Data Sent to Cisco

Data sent to Cisco from a Call Home–enabled device is different for each device. Table 1 summarizes the data sent to Cisco for analysis per type of Call Home message. For additional details about data descriptions per category, consult Chapter 3 of the Smart Call Home User Guide. For details regarding the Call Home output, such as CLI commands and their output that Call Home sends from the device, consult the configuration guide for that device, available at www.cisco.com/support.

Table 1. Summary of Data Sent to Cisco from Call Home

Category	Description
Environmental	• Company name, device host name, and serial number • Call Home message header and device output (attachments, such as 'show ' commands) • TAC case number (if applicable), technology, problem code, problem details, recommendation • Test description and effects of failure information • Total number of failures encountered when running the diagnostic test • Status that indicates failure or failure recovery
Configuration	• Running configuration • Startup configuration • Technology features • Configuration sanity analysis
Inventory	• Device and module serial numbers • Device host name • Device and module PIDs • Device and module hardware versions • Device software version • Device and module part numbers • Device and module top assembly numbers • Module card type • Date and time of configuration update • Failover status • Time-based license • System processor, image name, ROM version, memory, boot flash
Syslog	• Company name, device host name • Call Home message header and device output (attachments, such as 'show ' commands) • TAC case number (if applicable), technology, problem code, problem details, recommendation • Syslog error • Recommendations to resolve
Crash and diagnostic	• Company name, device host name, and serial number • Call Home message header and device output (attachments, such as 'show ' commands) • TAC case number (if applicable), technology, problem code, problem details, recommendation • Test description and effects of failure information • Total number of failures encountered when running the diagnostic test • Ending status of diagnostic or crash
Performance	• Company name, device host name • Call Home message header and device output (attachments, such as 'show ' commands) • Overview of performance issue with problem details and recommendation • Details on individual tests, including test name, recommendation, count (number of failures), and ending status
Snapshot	• CLI commands/outputs from last snapshot message received by Smart Call Home
Telemetry	• Company name, device host name • Call Home message header and device output (attachments, such as 'show ' commands) • Telemetry detection statistics, per interface • Firewall connections, connection per second • System resource data
Threat	• Threat detection rate • Threat detection statistics • Latest target and latest attacker
License	• License package • Installation status • License count • Status • Expiry date

Category	Description
	• Any comments associated to the device

Data Storage at the Cisco Data Center

Data Storage

Cisco is committed to protecting the privacy and confidentiality of the data it stores. To help ensure this, the following steps are taken:

- The Smart Call Home environment that processes your data is located behind the Cisco firewall and on a secure switched segment of the network.
- The installation process for all Cisco IT machines follows a rigorous standard of security; this includes the application of hardening scripts to protect these machines.
- The machines are kept in a lock-and-key facility where access is restricted to Cisco IT administrators only.
- Cisco intrusion detection systems are deployed throughout the corporate network and the restricted network on which the data is stored.
- The uploaded network information is uncompressed and decrypted only on Cisco production machines inside the Cisco firewalls.

The data is protected with strict authentication and access control measures within the Cisco firewall. The database is secured using a role-based security model implemented natively through Oracle application schema grants and privileges and a robust audit logging configuration. Application-level access to the data is protected through a single sign-on mechanism that is well accepted in the industry.

All access to data center data is through CA SiteMinder-based authentication. Data is stored according to Cisco corporate IT best practices and data protection and retention policies.

Storage Policies

Raw upload data is archived per Cisco enterprise retention policies. The raw data is converted, processed, and stored in the data center database from which the portal reports are generated. After the data is processed and analyzed, it is made available for display in the portal. Processed data is archived for at least five years.

Backup and Recovery

Installed base data resides at a Cisco data center. Cisco backs up information daily, and the information is encrypted and stored locally.

Cisco Processes to Verify and Audit the Security of Its Systems

Cisco uses a combination of static analysis at major releases and regular vulnerability testing to make sure products and services undergo security risk analysis, security standards compliance testing, and vulnerability scans. Any issues discovered by these processes are reported, and corrective action is handled through the standard Cisco Defect and Enhancements Tracking System process.

Controlling Access to the Portal Data and Offline Reports

Smart Call Home Portal Security

The Smart Call Home portal allows you to review processed information about your own devices. Your company's data is logically segregated from data from all other companies when viewing reports in the portal. The portal has the following security mechanisms in place:

- Unique, authorized Cisco.com ID and password, linked to the entitled company of the user
- Customer administration of user access to your Smart Call Home portal
- Server-authenticated SSL v3
- Secured session management with expiration
- Hierarchical role-based access control
- Event logging and monitoring, such as failed logins and invalid resource access attempts

Your designated customer administrator controls access to the Smart Call Home portal. The administrator can register new users and deregister existing users (for example, if the user leaves the company or changes job responsibility). The process to register or remove users is documented in the Smart Call Home User Guide.

Conclusion

Cisco takes the security of your data very seriously. If you need further details about Smart Call Home and how we implement our security architecture, contact your Cisco sales representative or your Cisco authorized partner. They will be happy to set up a technical meeting to discuss your questions and provide details about your specific situation.

For More Information

Read more about Smart Call Home and subscribe to the Smart Call Home Support Community to receive updated support information.

Read more about Cisco security policy, including privacy compliance, data retention, and data storage, in the Cisco Privacy and Security Compliance portal.

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 04/14