Cisco IP Phone Security

- Security Features, page 1
- Documentation, Support, and Security Guidelines, page 4

Security Features

Security features ensure that calls are secure and authenticated.

Domain and Internet Setting

Configure Restricted Access Domains

If you enter domains, the Cisco IP Phone responds only to SIP messages only from the identified servers.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 In the **System Configuration** section, in the **Restricted Access Domains** field, enter fully qualified domain names (FQDNs) for each SIP server that you want the phone to respond to. Separate FQDNs with semicolons.

Example:

```
voiceip.com; voiceip1.com
```

Step 3 Click **Submit All Changes**.

Configure the Internet Connection Type

You can set the connection type to one of the following:

- Dynamic Host Configuration Protocol (DHCP)—Enables the phone to receive an IP address from the network DHCP server. The Cisco IP phone typically operates in a network where a DHCP server assigns IP addresses to devices. Because IP addresses are a limited resource, the DHCP server periodically renews the device lease on the IP address. If a phone loses the IP address for any reason, or if some other device on the network is assigned the same IP address, the communication between the SIP proxy and the phone is either severed or degraded. Whenever an expected SIP response is not received within a programmable amount of time after the corresponding SIP command is sent, the DHCP Timeout on Renewal parameter causes the device to request a renewal of its IP address. If the DHCP server returns the IP address that it originally assigned to the phone, the DHCP assignment is presumed to be operating correctly. Otherwise, the phone resets to try to fix the issue.
- Static IP—A static IP address for the phone.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 In the **IPv4 Settings** section, use the **Connection Type** drop-down list box to choose the connection type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP

Step 3 If you choose Static IP, configure these settings in the **Static IP Settings** section:

- **Static IP—**Static IP address of the phone
- **NetMask—**Netmask of the phone
- **Gateway—**Gateway IP address

Step 4 Click **Submit All Changes**.

DHCP Option Support

The following table lists the DHCP options that are supported on the Cisco IP Phone.

Network Standard	Description
DHCP option 1	Subnet mask
DHCP option 2	Time offset
DHCP option 3	Router
DHCP option 6	Domain name server
DHCP option 15	Domain name
DHCP option 41	IP address lease time

Network Standard	Description
DHCP option 42	NTP server
DHCP option 43	Vendor-specific information Can be used for TR.69 Auto Configurations Server (ACS) discovery.
DHCP option 60	Vendor class identifier
DHCP option 66	TFTP server name
DHCP option 125	Vendor-identifying vendor-specific information Can be used for TR.69 Auto Configurations Server (ACS) discovery.
DHCP option 150	TFTP server
DHCP option 159	Provisioning server IP
DHCP option 160	Provisioning URL

Configure the Challenge for the SIP INVITE Messages

The phone can challenge the SIP INVITE (initial) message in a session. The challenge restricts the SIP servers that are permitted to interact with the devices on a service provider network. This practice significantly increases the security of the VoIP network through prevention of malicious attacks against the device.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **SIP Settings** section, choose **Yes** from the **Auth INVITE** drop-down list box.

Step 3 Click **Submit All Changes**.

Transport Layer Security

Transport Layer Security (TLS) is a standard protocol for securing and authenticating communications over the Internet. SIP over TLS encrypts the SIP messages between the service provider SIP proxy and the end user. SIP over TLS encrypts only the signaling messages, not the media.

TLS has two layers:

- TLS Record Protocol—Layered on a reliable transport protocol, such as SIP or TCH, this layer ensures that the connection is private through use of symmetric data encryption and it ensures that the connection is reliable.

- TLS Handshake Protocol—Authenticates the server and client, and negotiates the encryption algorithm and cryptographic keys before the application protocol transmits or receives data.

The Cisco IP Phone uses UDP as the standard for SIP transport, but the phone also supports SIP over TLS for added security.

Configure SIP Over TLS Signaling Encryption

Procedure

Step 1 To enable TLS for the phone, in the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **SIP Settings** section, select **TLS** from the **SIP Transport** drop-down list box.

Step 3 Click **Submit All Changes**.

Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, reviewing security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to U.S. and local country laws that govern import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations can be found at https://www.bis.doc.gov/policiesandregulations/ear/index.htm.