# Cisco IP Phone Security



# 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.

#### Before you begin

Access the phone administration web page. See Access the Phone Web Page.

#### Procedure

**Step 1** Select **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 commas.

**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.

### Before you begin

Access the phone administration web page. See Access the Phone Web Page.

### Procedure

**Step 1** Select **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** In the **IPv6 Settings** section, use the **Connection Type** drop-down list box to choose the connection type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP

**Step 4** 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 5** 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 |

| Network Standard | Description |
|---|---|
| DHCP option 3 | Router |
| DHCP option 6 | Domain name server |
| DHCP option 15 | Domain name |
| DHCP option 41 | IP address lease time |
| DHCP option 42 | NTP server |
| DHCP option 43 | Vendor-specific information<br>Can be used for TR.69 Auto Configurations Server (ACS) discovery. |
| DHCP option 56 | NTP server<br>NTP server configuration with IPv6 |
| DHCP option 60 | Vendor class identifier |
| DHCP option 66 | TFTP server name |
| DHCP option 125 | Vendor-identifying vendor-specific information<br>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.

### Before you begin

Access the phone administration web page. See Access the Phone Web Page.

### Procedure

**Step 1** Select **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

### Before you begin

Access the phone administration web page. See Access the Phone Web Page.

### Procedure

**Step 1** Select **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**.

# Configure LDAP over TLS

You can configure LDAP over TLS (LDAPS) to enable secure data transmission between the server and a specific phone.

**Attention** Cisco recommends leaving the authentication method to the default value of **`None`**. Next to the server field is an authentication field that uses the values **`None`**, **`Simple`**, or **`DIGEST-MD5`**. There is no **`TLS`** value for authentication. The software determines the authentication method from the ldaps protocol in the server string.

### Before you begin

Access the phone administration web page. See Access the Phone Web Page.

**Procedure**

**Step 1** Select **Voice** > **Phone**.

**Step 2** In the **LDAP** section, enter a server address in the **Server** field.

For example, enter **`ldaps://<ldaps_server>[:port]`** .

where:

- **`ldaps://`**= The server string starts with **`ldaps://`** before you enter the IP address or domain name
- **`ldaps_server`** = IP address or domain name
- **`port`** = Port number. Default: 636

**Step 3** Click **Submit All Changes**.

# Phones Supported in this Document

This document supports these phones:

- Cisco IP Phone 7800 Series Multiplatform Phones:
  - Cisco IP Phone 7811 Multiplatform Phones
  - Cisco IP Phone 7821 Multiplatform Phones
  - Cisco IP Phone 7841 Multiplatform Phones
  - Cisco IP Phone 7851 Multiplatform Phones

In this document, the term *phone* or *Cisco IP Phone* refers to the above phones.

# 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.