Cisco IP Phone Security

Domain and Internet Setting

Configure Restricted Access Domains

You can configure the phone to register, provision, firmware upgrade, and send reports using only the specified servers. Any registration, provisioning, upgrade, and report that don't use the specified servers can't be performed on the phone. If you specify the servers to use, ensure that the servers you enter in the following fields are included in the list:

- **Profile Rule**, **Profile Rule B**, **Profile Rule C**, and **Profile Rule D** on the **Provisioning** tab
- **Upgrade Rule** and **Cisco Headset Upgrade Rule** on the **Provisioning** tab
- **Report Rule** on the **Provisioning** tab
- **Custom CA Rule** on the **Provisioning** tab
- **Proxy** and **Outbound Proxy** on the **Ext (n)** tab

Before you begin

Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **System**.

Step 2 In the **System Configuration** section, locate the **Restricted Access Domains** field and enter fully qualified domain names (FQDNs) for each server. Separate FQDNs with commas.

Example:

```
voiceip.com, voiceip1.com
```

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Restricted_Access_Domains ua="na">voiceip.com, voiceip1.com</Restricted_Access_Domains>
```

Step 3 Click **Submit All Changes**.

Configure the DHCP Options

You can set the order in which your phone uses the DHCP options. For help with DHCP Options, see DHCP Option Support, on page 3.

Before you begin

Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **Provisioning**.

Step 2 In the **Configuration Profile** section, set the **DHCP Option To Use** and **DHCPv6 Option To Use** parameters as described in the Parameters for DHCP Options Configuration, on page 2 table.

Step 3 Click **Submit All Changes**.

Parameters for DHCP Options Configuration

The following table defines the function and usage of parameters for DHCP Options Configuration in the Configuration Profile section under the Voice>Provisioning tab in the phone web interface. It also defines

the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Table 1: Parameters for DHCP Options Configuration

Parameter	Description
DHCP Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>` • In the phone web page, enter the DHCP options separated by commas. **Example**: 66,160,159,150,60,43,125 Default: 66,160,159,150,60,43,125
DHCPv6 Option To Use	DHCPv6 options, delimited by commas, used to retrieve firmware and profiles. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>` • In the phone web page, enter the DHCP options separated by commas. **Example**: 17,160,159 Default: 17,160,159

DHCP Option Support

The following table lists the DHCP options that are supported on the multiplatform phones.

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
DHCP option 42	NTP server
DHCP option 43	Vendor-specific information Can be used for TR.69 Auto Configurations Server (ACS) discovery.

Network Standard	Description
DHCP option 56	NTP server 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 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 SIP INVITE Messages

You can set up the phone to challenge the SIP INVITE (initial) message in a session. The challenge restricts the SIP servers that are permitted to interact with devices on a service provider network. This practice prevents malicious attacks against the phone. When you enable this feature, authorization is required for initial incoming INVITE requests from the SIP proxy.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **SIP Settings** section, select **Yes** from the **Auth INVITE** list to enable this feature or select **No** to disable it.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Auth_INVITE_1>Yes</Auth_INVITE_1_>
```

Default: **No**.

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 signaling messages between the service provider SIP proxy and the end user.

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

The following table describes the two TLS layers.

Table 2: TLS Layers

Protocol Name	Description
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.

Encrypt Signaling with SIP Over TLS

You can configure added security when you encrypt signaling messages with SIP over TLS.

Before you begin

Access the Phone Web Interface. See Transport Layer Security, on page 5

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** list.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<SIP_Transport_1_ ua="na">TLS</SIP_Transport_1_>
```

.

Options available:

- UDP
- TCP
- TLS
- Auto

Default: **UDP**.

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.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

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

Procedure

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

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

You can also configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_Server ua="na">ldaps://10.45.76.79</LDAP_Server>
```

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

where:

- **ldaps://**= The start of the server address string.
- **ldaps_server** = IP address or domain name
- **port** = Port number. Default: 636

Step 3 Click **Submit All Changes**.

Configure StartTLS

You can enable Start Transport Layer Security (StartTLS) for the communications between the phone and the LDAP server. It uses the same network port (default 389) for both secure and insecure communications. If the LDAP server supports StartTLS, TLS encrypts the communications. Otherwise, the communications are in plaintext.

Before you begin

- Access the phone administration web page. See Access the Phone Web Interface.

Procedure

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

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

For example, enter `ldap://<ldap_server>[:port]`.

Where:

- **`ldap://`** = The start of the server address string, scheme of the URL
- **`ldap_server`** = IP address or domain name
- **`port`** = Port number

You can also configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_Server ua="na">ldap://<ldap_server>[:port]</LDAP_Server>
```

Step 3 Set the **StartTLS Enable** field to **Yes**.

You can also configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_StartTLS_Enable ua="na">Yes</LDAP_StartTLS_Enable>
```

Step 4 Click **Submit All Changes**.

Related Topics

Parameters for LDAP Directory

HTTPS Provisioning

The phone supports HTTPS for provisioning for increased security in managing remotely deployed units. Each phone carries a unique SLL Client Certificate (and associated private key), in addition to a Sipura CA server root certificate. The latter allows the phone to recognize authorized provisioning servers, and reject non-authorized servers. On the other hand, the client certificate allows the provisioning server to identify the individual device that issues the request.

For a service provider to manage deployment by using HTTPS, a server certificate must be generated for each provisioning server to which a phone resyncs by using HTTPS. The server certificate must be signed by the Cisco Server CA Root Key, whose certificate is carried by all deployed units. To obtain a signed server certificate, the service provider must forward a certificate signing request to Cisco, which signs and returns the server certificate for installation on the provisioning server.

The provisioning server certificate must contain the Common Name (CN) field, and the FQDN of the host running the server in the subject. It might optionally contain information following the host FQDN, separated by a slash (/) character. The following examples are of CN entries that are accepted as valid by the phone:

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

In addition to verifying the server certificate, the phone tests the server IP address against a DNS lookup of the server name that is specified in the server certificate.

Get a Signed Server Certificate

The OpenSSL utility can generate a certificate signing request. The following example shows the **openssl** command that produces a 1024-bit RSA public/private key pair and a certificate signing request:

```
openssl req -new -out provserver.csr
```

This command generates the server private key in **privkey.pem** and a corresponding certificate signing request in **provserver.csr**. The service provider keeps the **privkey.pem** secret and submits **provserver.csr** to Cisco for signing. Upon receiving the **provserver.csr** file, Cisco generates **provserver.crt**, the signed server certificate.

Procedure

Step 1 Navigate to https://software.cisco.com/software/cda/home and log in with your CCO credentials.

Note When a phone connects to a network for the first time or after a factory reset, and there are no DHCP options set up, it contacts a device activation server for zero touch provisioning. New phones use "activate.cisco.com" instead of "webapps.cisco.com" for provisioning. Phones with firmware release earlier than 11.2(1) continues to use "webapps.cisco.com". We recommend that you allow both the domain names through your firewall.

Step 2 Select **Certificate Management**.

On the **Sign CSR** tab, the CSR of the previous step is uploaded for signing.

Step 3 From the **Select Product** drop-down list box, select **SPA1xx firmware 1.3.3 and newer/SPA232D firmware 1.3.3 and newer/SPA5xx firmware 7.5.6 and newer/CP-78xx-3PCC/CP-88xx-3PCC**.

Step 4 In the **CSR File** field, click **Browse** and select the CSR for signing.

Step 5 Select the encryption method:

- MD5
- SHA1
- SHA256

Cisco recommends that you select SHA256 encryption.

Step 6 From the **Sign in Duration** drop-down list box, select the applicable duration (for example, 1 year).

Step 7 Click **Sign Certificate Request**.

Step 8 Select one of the following options to receive the signed certificate:

- **Enter Recipient's Email Address**—If you wish to receive the certificate via email, enter your email address in this field.

- **Download**—If you wish to download the signed certificate, select this option.

Step 9 Click **Submit**.

The signed server certificate is either emailed to the email address previously provided or downloaded.

Multiplatform Phone CA Client Root Certificate

Cisco also provides a Multiplatform Phone Client Root Certificate to the service provider. This root certificate certifies the authenticity of the client certificate that each phone carries. The Multiplatform Phones also support third-party signed certificates such as those provided by Verisign, Cybertrust, and so on.

To determine if a phone carries an individualized certificate, use the $CCERT provisioning macro variable. The variable value expands to either Installed or Not Installed, according to the presence or absence of a unique client certificate. In the case of a generic certificate, it is possible to obtain the serial number of the unit from the HTTP request header in the User-Agent field.

HTTPS servers can be configured to request SSL certificates from connecting clients. If enabled, the server can use the Multiplatform Phone Client Root Certificate that Cisco supplies to verify the client certificate. The server can then provide the certificate information to a CGI for further processing.

The location for certificate storage may vary. For example, in an Apache installation, the file paths for storage of the provisioning server-signed certificate, its associated private key, and the Multiplatform Phone CA client root certificate are as follows:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

For specific information, refer to the documentation for an HTTPS server.

The Cisco Client Certificate Root Authority signs each unique certificate. The corresponding root certificate is made available to service providers for client authentication purposes.

Redundant Provisioning Servers

The provisioning server can be specified as an IP address or as a Fully Qualified Domain Name (FQDN). The use of an FQDN facilitates the deployment of redundant provisioning servers. When the provisioning server is identified through an FQDN, the phone attempts to resolve the FQDN to an IP address through DNS. Only DNS A-records are supported for provisioning; DNS SRV address resolution is not available for provisioning. The phone continues to process A-records until a server responds. If no server that is associated with the A-records responds, the phone logs an error to the syslog server.

Syslog Server

If a syslog server is configured on the phone through use of the <Syslog Server> parameters, the resync and upgrade operations send messages to the syslog server. A message can be generated at the start of a remote file request (configuration profile or firmware load), and at the conclusion of the operation (indicating either success or failure).

The logged messages are configured in the following parameters and macro expanded into the actual syslog messages:

Enable the Firewall

We have improved phone security by hardening the operating system. Hardening ensures that the phone has a firewall to protect it from malicious incoming traffic. The firewall tracks the ports for incoming and outgoing data. It detects incoming traffic from unexpected sources and blocks the access. Your firewall allows all outgoing traffic.

The firewall may dynamically unblock normally blocked ports. The outgoing TCP connection or UDP flow unblocks the port for return and continued traffic. The port is kept unblocked while flow is alive. The port reverts to blocked state when flow terminates or ages out.

The legacy setting, IPv6 Multicast Ping **Voice** > **System** > **IPv6 Settings** > **Broadcast Echo** continues to work independently of the new firewall settings.

Firewall configuration changes generally don't result in a phone restart. Phone soft restarts generally don't affect firewall operation.

The firewall is enabled by default. If it is disabled, you can enable it from the phone web page.

Before you begin

Access the Phone Web Interface

Procedure

Step 1 Select **Voice** > **System** > **Security Settings**.

Step 2 In the **Firewall** drop down list, select **Enabled**.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Firewall ua="na">Enabled</Firewall>
```

The allowed values are Disabled|Enabled. The default value is Enabled.

Step 3 Click **Submit All Changes**.
This enables the firewall with its default open UDP and TCP ports.

Step 4 Select **Disabled** to disable the firewall if you wish your network to return to its prior behavior.

The following table describes the default open UDP ports.

Table 3: Firewall Default Open UDP Ports

Default Open UDP Port	Description
DHCP/DHCPv6	DHCP client Port 68 DHCPv6 client Port 546
SIP/UDP	Configure the Port in **Voice** > **Ext<n>** > **SIP Settings** > **SIP Port** (example: 5060), when **Line Enable** is set to **`Yes`**, and **SIP Transport** is set to **`UDP`** or **`Auto`**.
RTP/RTCP	UDP port range from **`RTP Port Min`** to **`RTP Port Max+1`**
PFS (Peer Firmware Sharing)	Port 4051, when **Upgrade Enable** and **Peer Firmware Sharing** are set to **`Yes`**.
TFTP clients	Ports 53240-53245. You need this port range if the remote server uses a port other than the standard TFTP port 69. You may turn it off if the server uses standard port 69. See Configure Your Firewall with Additional Options, on page 11.
TR-069	UDP/STUN port 7999, when **Enable TR-069** is set to **`Yes`**.

The following table describes the default open TCP ports.

Table 4: Firewall Default Open TCP Ports

Default Open TCP Port	Description
Web server	Port configured via Web Server Port (default 80), when **Enable Web Server** is set to **`Yes`**.
PFS (Peer Firmware Sharing)	Ports 4051 and 6970, when both **Upgrade Enable** and **Peer Firmware Sharing** are set to **`Yes`**.
TR-069	HTTP/SOAP port in TR-069 Connection Request URL, when **Enable TR-069** is set to **`Yes`**. The port is chosen randomly from the range 8000-9999.

Configure Your Firewall with Additional Options

You can configure additional options in the **Firewall Options** field. Type the keyword for each option in the field, and separate the keywords by commas (,). Some keywords have values. Separate the values by colons (:).

Before you begin

Access the Phone Web Interface

Procedure

Step 1 Go to **Voice** > **System** > **Security Settings**.

Step 2 Select **Enabled** for the **Firewall** field.

Step 3 In the **Firewall Options** field, enter the keywords. The list of ports applies to both IPv4 and IPv6 protocols.

When you enter the keywords,

- separate the keywords with commas (,).
- separate keywords values with colons (:).

Table 5: Firewall Optional Settings

Firewall Options Keywords	Description
Field is empty.	The firewall runs with default open ports.
NO_ICMP_PING	The firewall blocks incoming ICMP/ICMPv6 **`Echo`** requests (Ping). This option may break some types of traceroute requests to the phone. Windows **`tracert`** is one example. Example **Firewall Options** entry with a combination of options: NO_ICMP_PING,TCP:12000,UDP:8000:8010 The firewall runs with default settings and the following additional options: • Drops incoming ICMP/ICMPv6 **`Echo`** (Ping) requests. • Opens TCP port 12000 (IPv4 and IPv6) for incoming connections. • Opens UDP port range 8000-8010 (IPv4 and IPv6) for incoming requests.
NO_ICMP_UNREACHABLE	The phone doesn't send ICMP/ICMPv6 `Destination Unreachable` for UDP ports. **Note** The exception is to always send `Destination Unreachable` for ports in the RTP port range. This option may break some types of **`traceroute`** requests to the device. For example, Linux **`traceroute`** may break.
NO_CISCO_TFTP	• The phone doesn't open TFTP-client port-range (UDP 53240:53245). • Requests to non-standard (non 69) TFTP server ports fail. • Requests to standard TFTP server port 69 work.
The following keywords and options apply when the phone runs custom apps that handle incoming requests.	

Firewall Options Keywords	Description
UDP:<xxx>	Opens UDP port <xxx>.
UDP:<xxx:yyy>	Opens UDP port-range, <xxx to yyy>, inclusive. You can have up to 5 UDP port options (single ports and port ranges). For example, you can have 3 UDP:<xxx> and 2 UDP:<xxx:yyy>.
TCP:<xxx>	Opens TCP port <xxx>.
TCP:<xxx:yyy>	Opens TCP port-range <xxx to yyy>, inclusive. You can have up to 5 TCP port options (single ports and port ranges). For example, you can have 4 TCP:<xxx> and one TCP:<xxx:yyy>.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Firewall_Config ua="na">NO_ICMP_PING</Firewall_Config>
```

Step 4 Click **Submit All Changes**.

Configure the Cipher List

You can specify the cipher suites that the phone TLS applications use. The specified cipher list applies to all the applications that use the TLS protocol. The TLS applications on your phone include:

- Customer CA Provisioning
- E911 Geolocation
- Firmware/Cisco Headset Upgrade
- LDAPS
- LDAP (StartTLS)
- Picture Download
- Logo Download
- Dictionary Download
- Provisioning
- Report Upload
- PRT Upload
- SIP over TLS
- TR-069
- WebSocket API
- XML Services

- XSI Services

You can also specify the cipher suites with the TR-069 parameter (`Device.X_CISCO_SecuritySettings.TLSCipherList`) or with the the configuration file (cfg.xml). Enter a string in the configuration file in this format:

```
<TLS_Cipher_List ua="na">RSA:!aNULL:!eNULL</TLS_Cipher_List>
```

Before you begin

Access the phone administration web page, see Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **System**.

Step 2 In the **Security Settings** section, enter the cipher suite or the combination of cipher suites in the **TLS Cipher List** field.

Example:

```
RSA:!aNULL:!eNULL
```

supports those cipher suites using RSA authentication, but excludes those cipher suites offering no encryption and authentication.

Note A valid cipher list must follow the format defined at https://www.openssl.org/docs/man1.1.1/man1/ciphers.html. Your phone doesn't support all the cipher strings listed on the OpenSSL web page. For the supported strings, see Supported Cipher Strings, on page 15.

If the value in the **TLS Cipher List** field is blank or invalid, the cipher suites used vary with applications. See the following list for the suites that the applications use when this field is with a blank or an invalid value.

- Web Server (HTTPS) applications use the following cipher suites:
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**
  - **DES-CBC3-SHA**
- XMPP uses the cipher list **HIGH:MEDIUM:AES:@STRENGTH**.
- SIP, TR-069, and other applications using the curl library use the **DEFAULT** cipher string. The **DEFAULT** cipher string contains the following cipher suites that the phone support:

```
DEFAULT Cipher Suites (28 suites):
        ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        ECDHE_RSA_WITH_AES_256_GCM_SHA384
        DHE_RSA_WITH_AES_256_GCM_SHA384
        ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        ECDHE_RSA_WITH_AES_128_GCM_SHA256
```

```
DHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE_RSA_WITH_AES_256_CBC_SHA384
DHE_RSA_WITH_AES_256_CBC_SHA256
ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE_RSA_WITH_AES_128_CBC_SHA256
DHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDHE_RSA_WITH_AES_256_CBC_SHA
DHE_RSA_WITH_AES_256_CBC_SHA
ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE_RSA_WITH_AES_128_CBC_SHA
DHE_RSA_WITH_AES_128_CBC_SHA
RSA_WITH_AES_256_GCM_SHA384
RSA_WITH_AES_128_GCM_SHA256
RSA_WITH_AES_256_CBC_SHA256
RSA_WITH_AES_128_CBC_SHA256
RSA_WITH_AES_256_CBC_SHA
RSA_WITH_AES_128_CBC_SHA
EMPTY_RENEGOTIATION_INFO_SCSV
```

Step 3 Click **Submit All Changes**.

Supported Cipher Strings

The supported cipher strings listed following is based on the OpenSSL 1.1.1d standards.

Table 6: Supported Cipher Strings (OpenSSL 1.1.1d)

Strings	Strings	Strings
DEFAULT	kECDHE, kEECDH	CAMELLIA128, CAMELLIA256, CAMELLIA
COMPLEMENTOFDEFAULT	ECDHE, EECDH	CHACHA20
ALL	ECDH	SEED
COMPLEMENTOFALL	AECDH	MD5
HIGH	aRSA	SHA1, SHA
MEDIUM	aDSS, DSS	SHA256, SHA384
eNULL, NULL	aECDSA, ECDSA	SUITEB128, SUITEB128ONLY, SUITEB192
aNULL	TLSv1.2, TLSv1, SSLv3	
kRSA, RSA	AES128, AES256, AES	
kDHE, kEDH, DH	AESGCM	
DHE, EDH	AESCCM, AESCCM8	
ADH	ARIA128, ARIA256, ARIA	

Enable Hostname Verification for SIP over TLS

You can enable increased phone security on a phone line if you use TLS. The phone line can verify the hostname to determine if the connection is secure.

Over a TLS connection, the phone can verify the hostname to check the server identity. The phone can check both the Subject Alternative Name (SAN) and the Subject Common Name (CN). If the hostname on the valid certificate matches the hostname that is used to communicate with the server, the TLS connection establishes. Otherwise, the TLS connection fails.

The phone always verifies the hostname for the following applications:

- LDAPS
- LDAP (StartTLS)
- XMPP
- Image upgrade over HTTPS
- XSI over HTTPS
- File download over HTTPS
- TR-069

When a phone line transports SIP messages over TLS, you can configure the line to enable or bypass the hostname verification with the **TLS Name Validate** field on the **Ext(n)** tab.

Before you begin

- Access the phone administration web page. See Access the Phone Web Interface.
- On the **Ext(n)** tab, set **SIP Transport** to **TLS**.

Procedure

Step 1 Go to **Voice** > **Ext(n)**.

Step 2 In the **Proxy and Registration** section, set the **TLS Name Validate** field to **Yes** to enable the hostname verification, or **No** to bypass the hostname verification.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
```

The allowed values are Yes or No. The default setting is Yes.

Step 3 Click **Submit All Changes**.

Enable Client-Initiated Mode for Media Plane Security Negotiations

To protect media sessions, you can configure the phone to initiate media plane security negotiations with the server. The security mechanism follows the standards stated in RFC 3329 and its extension draft *Security Mechanism Names for Media* (See https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2). The transport of negotiations between the phone and the server can use SIP protocol over UDP, TCP, and TLS. You can limit that media plane security negotiation is applied only when the signaling transport protocol is TLS.

You can also configure the parameters in the configuration file (cfg.xml). To configure each parameter, see the syntax of the string in Parameters for Media Plane Security Negotiation, on page 17.

Before you begin

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

Procedure

Step 1 Select **Voice** > **Ext (n)**.

Step 2 In the **SIP Settings** section, set the **MediaSec Request** and **MediaSec Over TLS Only** field as defined in Parameters for Media Plane Security Negotiation, on page 17

Step 3 Click **Submit All Changes**.

Parameters for Media Plane Security Negotiation

The following table defines the function and usage of the parameters for media plane security negotiation in the **SIP Settings** section under the **Voice**> **Ext (n)** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 7: Parameters for Media Plane Security Negotiation

Parameter	Description
MediaSec Request	Specifies whether the phone initiates media plane security negotiations with the server. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>` • In the phone web interface, set this field to **Yes** or **No** as needed. Allowed values: Yes|No • **Yes**—Client-initiated Mode. The phone initiates media plane security negotiations. • **No**—Server-initiated Mode. The server initiates media plane security negotiations. The phone doesn't initiate negotiations, but can handle negotiation requests from the server to establish secure calls. Default: No
MediaSec Over TLS Only	Specifies the signaling transport protocol over which media plane security negotiation is applied. Before setting this field to **Yes**, ensure that the signaling transport protocol is TLS. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>` • In the phone web interface, set this field to **Yes** or **No** as needed. Allowed values: Yes|No • **Yes**—The phone initiates or handles media plane security negotiations only when the signaling transport protocol is TLS. • **No**—The phone initiates and handles media plane security negotiations regardless of the signaling transport protocol. Default: No

802.1X Authentication

Cisco IP Phones use Cisco Discovery Protocol (CDP) to identify the LAN switch and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations.

Cisco IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco IP Phone to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the IP phone does not act as the LAN switch to authenticate a data endpoint before accessing the network.

Cisco IP Phones also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the IP phone, the LAN switch does not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

Support for 802.1X authentication requires several components:

- Cisco IP Phone: The phone initiates the request to access the network. Cisco IP Phones contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server): The authentication server and the phone must both be configured with a shared secret that authenticates the phone.
- A LAN switch supporting 802.1X: The switch acts as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure PC Port: The 802.1X standard does not consider VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the phone.
    - Yes: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC.
    - No: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the phone and the PC.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
    - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
    - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

Enable 802.1X Authentication

You can enable 802.1X authentication on the phone. When 802.1X authentication is enabled, the phone uses 802.1X authentication to request network access.When 802.1X authentication is turned off, the phone uses CDP to acquire VLAN and network access. You can also view the transaction status on the phone screen menu.

Procedure

Step 1 Perform one of the following actions to enable 802.1X authentication:

- In the phone web interface, select **Voice** > **System** and set the **Enable 802.1X Authentication** field to **Yes**. Then, click **Submit All Changes**.
- In the configuration file (cfg.xml), entering a string in this format:

```
<Enable_802.1X_Authentication ua="rw">Yes</Enable_802.1X_Authentication>
```

- On the phone, press **Applications** > **Network configuration** > **Ethernet configuration** > **802.1X authentication**. Then, toggle the **Device authentication** field to **On** with the **Select** button and press **Submit**.

Step 2 (Optional)Select **Transaction status** to view the following:

- **Transaction status**: Displays the state of 802.1x authentication. The state can be
  - *Authenticating*: Indicates that the authentication process is in progress.
  - *Authenticated*: Indicates that the phone is authenticated.
  - *Disabled*: Indicates that 802.1x authentication is disabled on the phone.
- **Protocol**: Displays the EAP method that is used for 802.1x authentication. The protocol can be EAP-FAST or EAP-TLS.

Step 3 Press **Back** to exit the menu.

Set Up a Proxy Server

You can configure the phone to use a proxy server to enhance security. A proxy server acts as a firewall between the phone and Internet. After successful configuration, the phone connects to Internet through the proxy server which protects the phone from cyber attack.

You can set up a proxy server by either using an automatic configuration script or manually configuring the host server (hostname or IP address) and port of the proxy server.

When configured, the HTTP proxy feature applies to all the applications that use the HTTP protocol. The applications include the following:

- GDS (Activation Code Onboarding)
- EDOS Device Activation

- Onboarding to Webex Cloud (via EDOS and GDS)
- Certificate Authentication
- Provisioning
- Firmware Upgrade
- Phone Status Report
- PRT Upload
- XSI Services
- Webex Services

Before you begin

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

Procedure

Step 1 Select **Voice** > **System**.

Step 2 In the section **HTTP Proxy Settings**, configure the parameter **Proxy Mode** and others according to your requirement. Detailed procedures are provided in the following steps.

Step 3 Do one of the following actions:

- **Proxy Mode** is **Auto**:
  - If **Use Auto Discovery (WPAD)** is **Yes**, no further action is required. The phone will automatically retrieve a Proxy Auto-Configuration (PAC) file by the Web Proxy Auto-Discovery (WPAD) protocol.
  - If **Use Auto Discovery (WPAD)** is **No**, enter a valid URL in **PAC URL**.
- **Proxy Mode** is **Manual**:
  - If **Proxy Server Requires Authentication** is **No**, enter a proxy server in **Proxy Host** and a proxy port in **Proxy Port**.
  - If **Proxy Server Requires Authentication** is **Yes**, enter a proxy server in **Proxy Host** and a proxy port in **Proxy Port**. And enter a username in **Username** and a password in **Password**.
- **Proxy Mode** is **Off**, the HTTP proxy feature is disabled on the phone.

You can also configure the parameters in the phone configuration file (cfg.xml). To configure each parameter, see the syntax of the string in the Parameters for HTTP Proxy Settings, on page 22.

Step 4 Click **Submit All Changes**.

Parameters for HTTP Proxy Settings

The following table defines the function and usage of the HTTP proxy parameters in the **HTTP Proxy Settings** section under the **Voice** > **System** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 8: Parameters for HTTP Proxy Settings

Parameter	Description and Default Value
Proxy Mode	Specifies the HTTP proxy mode that the phone uses, or disables the HTTP proxy feature. • Auto The phone automatically retrieves a Proxy Auto-Configuration (PAC) file to select a proxy server. In this mode, you can determine whether to use Web Proxy Auto-Discovery (WPAD) protocol to retrieve a PAC file or manually enter a valid URL of the PAC file. For details about the parameters, see Use Auto Discovery (WPAD) and PAC URL. • Manual You must manually specify a server (hostname or IP address) and a port of a proxy server. For details about the parameters, see Proxy Host and Proxy Port. • Off You disable the HTTP proxy feature on the phone. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Proxy_Mode ua="rw">Off</Proxy_Mode>` • On the phone web interface, select a proxy mode or disable the feature. Allowed values: Auto, Manual, and Off Default: Off

Parameter	Description and Default Value
Use Auto Discovery (WPAD)	Determines whether the phone uses the Web Proxy Auto-Discovery (WPAD) protocol to retrieve a PAC file. WPAD protocol uses DHCP or DNS, or both network protocols to locate a Proxy Auto-Configuration (PAC) file automatically. PAC file is used to select a proxy server for a given URL. This file can be hosted locally or on a network. • The parameter configuration takes effect when **Proxy Mode** is set to **Auto**. • If you set the parameter to **No**, you must specify a PAC URL. For details about the parameter, see PAC URL. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Use_Auto_Discovery__WPAD_ ua="rw">Yes</Use_Auto_Discovery__WPAD_>` • On the phone web interface, select Yes or No as needed. Allowed values: Yes and No Default: Yes
PAC URL	URL of a PAC file. For example, `http://proxy.department.branch.example.com` TFTP, HTTP, and HTTPS are supported. If you set the **Proxy Mode** to **Auto** and **Use Auto Discovery (WPAD)** to **No**, you must configure this parameter. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<PAC_URL ua="rw">http://proxy.department.branch.example.com/pac</PAC_URL>` • On the phone web interface, enter a valid URL that locates to a PAC file. Default: Empty

Parameter	Description and Default Value

Proxy Host	IP address or hostname of the proxy host server for the phone to access. For example:
	`proxy.example.com`
	The scheme (`http://` or `https://`) is not required.
	If you set the **Proxy Mode** to **Manual**, you must configure this parameter.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	`<Proxy_Host ua="rw">proxy.example.com</Proxy_Host>`
	• On the phone web interface, enter an IP address or hostname of the proxy server.
	Default: Empty

Proxy Port	Port number of the proxy host server. If you set the **Proxy Mode** to **Manual**, you must configure this parameter. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Proxy_Port ua="rw">3128</Proxy_Port>` • On the phone web interface, enter a server port. Default: 3128
Proxy Server Requires Authentication	Determines whether the user needs to provide the authentication credentials (username and password) that the proxy server requires. This parameter is configured according to the actual behaviour of the proxy server. If you set the parameter to **Yes**, you must configure **Username** and **Password**. For details about the parameters, see Username and Password. The parameter configuration takes effect when **Proxy Mode** is set to **Manual** . Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Proxy_Server_Requires_Authentication ua="rw">No</Proxy_Server_Requires_Authentication>` • On the phone web interface, set this field Yes or No as needed. Allowed values: Yes and No Default: No

Parameter	Description and Default Value
Username	Username for a credential user on the proxy server. If **Proxy Mode** is set to **Manual** and **Proxy Server Requires Authentication** is set to **Yes**, you must configure the parameter. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Proxy_Username ua="rw">Example</Proxy_Username>` • On the phone web interface, enter the username. Default: Empty
Password	Password of the specified username for the proxy authentication purpose. If **Proxy Mode** is set to **Manual** and **Proxy Server Requires Authentication** is set to **Yes**, you must configure the parameter. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Proxy_Password ua="rw">Example</Proxy_Password>` • On the phone web interface, enter a valid password for the proxy authentication of the user. Default: Empty

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.