Sicherheit von Cisco IP-Telefonen

- Domänen- und Interneteinstellungen, auf Seite 1
- Configure the Challenge for SIP INVITE Messages (Anfrage für SIP-Einladungsnachrichten konfigurieren), auf Seite 4
- Transport Layer Security, auf Seite 5
- HTTPS-Bereitstellung, auf Seite 7
- Firewall aktivieren, auf Seite 10
- Konfigurieren Sie Ihre Firewall mit zusätzlichen Optionen, auf Seite 12
- Verschlüsselungsliste konfigurieren, auf Seite 14
- Verifizierung des Host-Namens für SIP über TLS aktivieren, auf Seite 17
- Client-initiierten Modus für Sicherheitsverhandlungen in der Medienebene aktivieren, auf Seite 18
- 802.1X-Authentifizierung, auf Seite 20
- Proxyserver einrichten, auf Seite 21
- Übersicht über die Cisco Produktsicherheit, auf Seite 27

Domänen- und Interneteinstellungen

Domänen mit beschränktem Zugriff konfigurieren

Sie können das Telefon so konfigurieren, dass es nur über die angegebenen Server registriert, bereitgestellt wird, Firmware-Upgrades durchführt und Berichte sendet. Alle Registrierungen, Bereitstellung, Upgrades und Berichte, die die angegebenen Server nicht verwenden, können nicht auf dem Telefon ausgeführt werden. Wenn Sie die zu verwendenden Server angeben, stellen Sie sicher, dass die in den folgenden Feldern eingegebenen Server in der Liste aufgeführt sind:

- **Profilregel**, **Profilregel B**, **Profilregel C** und **Profilregel D** auf der Registerkarte **Bereitstellung**
- **Upgrade-Regel** und **Upgrade-Regel für Cisco-Headset** auf der Registerkarte **Bereitstellung**
- **Berichtsregel** auf der Registerkarte **Bereitstellung**
- **Benutzerdefinierte CA-Regel** auf der Registerkarte **Bereitstellung**
- **Proxy** und **ausgehender Proxy** auf der Registerkarte **Durchwahl(n)**

Vorbereitungen

Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Voice** > **System** aus.

Schritt 2 Suchen die das Feld **Domänen mit eingeschränktem Zugriff** im Abschnitt **Systemkonfiguration** und geben Sie für jeden Server den vollständigen Domänennamen (FQDNs) ein. Trennen Sie die FQDNs durch Kommata.

Beispiel:

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

Sie können diesen Parameter in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Schritt 3 Klicken Sie auf **Submit All Changes**.

DHCP-Optionen konfigurieren

Sie können die Reihenfolge festlegen, in der Ihr Telefon die DHCP-Optionen verwendet. Hilfe zu DHCP-Optionen finden Sie unter Unterstützung der DHCP-Option, auf Seite 3.

Vorbereitungen

Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Voice** > **Bereitstellung** aus.

Schritt 2 Legen Sie im Abschnitt **Konfigurationsprofil** die Parameter **Zu verwendende DHCP-Option** und **Zu verwendende DHCPv6-Option** wie in Tabelle Parameter für die Konfigurierung der DHCP-Optionen, auf Seite 2 beschrieben fest.

Schritt 3 Klicken Sie auf **Submit All Changes**.

Parameter für die Konfigurierung der DHCP-Optionen

Die folgende Tabelle definiert die Funktion und den Gebrauch der Parameter für die Konfiguration der DHCP-Optionen im Abschnitt „Konfigurationsprofil“ auf der Registerkarte „Sprache > Bereitstellung“ auf der Telefon-Weboberfläche. Außerdem wird die Syntax der Zeichenfolge definiert, die in der

Telefon-Konfigurationsdatei mit dem XML-Code (cfg.xml) hinzugefügt wird, um einen Parameter zu konfigurieren.

Tabelle 1: Parameter für die Konfigurierung der DHCP-Optionen

Parameter	Beschreibung
DHCP Option To Use (Zu verwendende DHCP-Option)	Durch Kommas getrennte DHCP-Optionen, die zum Abrufen der Firmware und Profile verwendet werden. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>` • Geben Sie auf der Telefon-Webseite die durch Kommas getrennten DHCP-Optionen ein. **Beispiel**: 66,160,159,150,60,43,125 Standard: 66,160,159,150,60,43,125
Zu verwendende DHCPv6-Option	DHCPv6-Optionen, durch Kommas getrennt, wird zum Abrufen von Firmware und Profilen verwendet. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>` • Geben Sie auf der Telefon-Webseite die durch Kommas getrennten DHCP-Optionen ein. **Beispiel**: 17,160,159 Standard: 17.160.159

Unterstützung der DHCP-Option

Die folgende Tabelle listet de DHCP-Optionen auf, die von Multiplattform-Telefonen unterstützt werden.

Netzwerkstandard	Beschreibung
DHCP-Option 1	Subnetzmaske
DHCP-Option 2	Time offset (Zeitoffset)
DHCP-Option 3	Router
DHCP-Option 6	Domänennamenserver
DHCP-Option 15	Domänenname
DHCP-Option 41	IP-Adressen-Leasezeit

Netzwerkstandard	Beschreibung
DHCP-Option 42	NTP-Server
DHCP-Option 43	Anbieterspezifische Informationen Kann für die Erkennung des TR.69-ACS-Servers (Auto Configurations Server) verwendet werden.
DHCP-Option 56	NTP-Server NTP-Server-Konfiguration mit IPv6
DHCP-Option 60	VCI (Vendor Class Identifier)
DHCP-Option 66	TFTP-Servername
DHCP-Option 125	Anbieterspezifische Informationen Kann für die Erkennung des TR.69-ACS-Servers (Auto Configurations Server) verwendet werden.
DHCP-Option 150	TFTP-Server
DHCP-Option 159	Bereitstellungsserver-IP
DHCP-Option 160	Bereitstellungs-URL

Configure the Challenge for SIP INVITE Messages (Anfrage für SIP-Einladungsnachrichten konfigurieren)

Sie können das Telefon so einrichten, dass die (anfängliche) SIP-Einladungsnachricht in einer Sitzung angefragt wird. Die Anfrage beschränkt die SIP-Server, die mit den Geräten in einem Service-Provider-Netzwerk interagieren dürfen. Diese Vorgehensweise verhindert bösartige Angriffe auf das Telefon. Wenn Sie diese Funktion aktivieren wird de Autorisierung für anfängliche eingehende Einladungsanfragen vom SIP-Proxy erforderlich.

Sie können die Parameter auch in der Konfigurationsdatei des Telefons mit XML-Code (cfg.xml) konfigurieren.

Vorbereitungen

Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Sprache** > **Durchwahl(n)** aus, wobei n eine Durchwahlnummer ist.

Schritt 2 Wählen Sie im Abschnitt **SIP-EinstellungenJa** aus der Liste **Autorisierung EINLADUNG** aus, um diese Funktion zu aktiveren oder wählen Sie **Nein**, um Sie zu deaktivieren.

Sie können diesen Parameter in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Standard: **Nein**

Schritt 3 Klicken Sie auf **Submit All Changes**.

Transport Layer Security

TLS ist ein Standardprotokoll für das Sichern und Authentifizieren der Kommunikation über das Internet. SIP over TLS verschlüsselt die SIP-Signal-Nachrichten zwischen dem Serviceanbieter-SIP-Proxy und dem Endnutzer.

Das Cisco IP-Telefon verwendet UDP als Standard für den SIP-Transport, aber unterstützt auch SIP über TLS, um die Sicherheit zu erhöhen.

Die folgende Tabelle beschreibt die zwei TLS-Ebenen.

Tabelle 2: TLS-Ebenen

Protokoll Name	Beschreibung
TLS-Datensatz-Protokoll	Diese Ebene ist auf einem zuverlässigen Transportprotokoll geschichtet, wie z. B. SIP oder TCH, und gewährleistet, dass die Verbindung durch die Verwendung einer symmetrischen Datenverschlüsselung privat ist und gewährleistet, dass die Verbindung zuverlässig ist.
TLS-Handshake-Protokoll	Authentifiziert den Server und den Client, und verhandelt die Verschlüsselungsalgorithmus und die kryptographischen Tasten, bevor das Anwendungsprotokoll Daten sendet oder empfängt.

Signalverschlüsselung mit SIP über TLS

Sie können zusätzliche Sicherheit konfigurieren, wenn Sie Signalmeldungen mit SIP über TLS verschlüsseln.

Vorbereitungen

Auf Weboberfläche des Telefons zugreifen. Siehe Transport Layer Security, auf Seite 5

Prozedur

Schritt 1 Wählen Sie **Sprache** > **Durchwahl(n)** aus, wobei n eine Durchwahlnummer ist.

Schritt 2 Wählen Sie unter **SIP-Einstellungen** die Option **TLS** aus der Dropdown-Liste **SIP-Transport** aus.

Sie können diesen Parameter in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

.

Verfügbare Optionen:

- UDP
- TCP
- TLS
- Auto

Standard: **UDP**.

Schritt 3 Klicken Sie auf **Submit All Changes**.

LDAP über TLS konfigurieren

Sie können LDAP über TLS (LDAPS) konfigurieren, um eine sichere Datenübertragung zwischen dem Server und einem bestimmten Telefon zu ermöglichen.

Achtung Cisco empfiehlt den Standardwert für die Authentifizierungsmethode auf **Keine** zu belassen. Neben dem Serverfeld befindet sich ein Authentifizierungsfeld, das die Werte **Keine**, **Einfach** oder **DIGEST-MD5** verwendet. Es gibt keinen **TLS**-Wert für die Authentifizierung. Die Software bestimmt die Methode des Authentifizierungsverfahrens aus dem LDAPS-Protokoll in der Serverzeichenfolge.

Sie können die Parameter auch in der Konfigurationsdatei des Telefons mit XML-Code (cfg.xml) konfigurieren.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Voice** > **Telefon** aus.

Schritt 2 Geben Sie im Abschnitt **LDAP** eine Serveradresse im Feld **Server** ein.

Sie können diesen Parameter ebenfalls in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Geben Sie beispielsweise `ldaps://<ldaps_server>[:port]` ein.

Dabei gilt:

- **ldaps://**= Der Anfang der Zeichenfolge der Serveradresse.
- **ldaps_server** = IP-Adresse oder Domänenname
- **port** = Portnummer. Standard: 636

Schritt 3 Klicken Sie auf **Submit All Changes**.

StartTLS konfigurieren

Sie können die Option „Transport Layer Security starten“ (StartTLS) für die Kommunikation zwischen dem Telefon und dem LDAP-Server aktivieren. Sie verwendet denselben Netzwerk-Port (Standard: 389) für sichere und unsichere Kommunikation. Wenn der LDAP-Server StartTLS unterstützt, verschlüsselt TLS die Kommunikation. Andernfalls ist die Kommunikation unverschlüsselt.

Vorbereitungen

- Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Sprache** > **Telefon** aus.

Schritt 2 Geben Sie im Abschnitt **LDAP** eine Serveradresse im Feld **Server** ein.

Geben Sie beispielsweise `ldap://<ldap_server>[:port]` ein.

Dabei gilt:

- **`ldap://`** = Der Anfang der Zeichenfolge der Serveradresse, Schema der URL.
- **`ldap_server`** = IP-Adresse oder Domänenname
- **`port`** = Portnummer.

Sie können diesen Parameter ebenfalls in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Schritt 3 Legen Sie das Feld **StartTLS aktivieren** auf **Ja** fest.

Sie können diesen Parameter ebenfalls in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Schritt 4 Klicken Sie auf **Submit All Changes**.

Verwandte Themen

Parameter für das LDAP-Verzeichnis

HTTPS-Bereitstellung

Das Telefon unterstützt HTTPS für die Bereitstellung, um die Sicherheit der Remoteverwaltung von Geräten zu erhöhen. Jedes Telefon besitzt neben einem Sipura CA-Server-Stammzertifikat ein eindeutiges SSL-Clientzertifikat (und den zugehörigen privaten Schlüssel). Das Serverstammzertifikat ermöglicht es dem Telefon, autorisierte Bereitstellungsserver zu erkennen und nicht autorisierte Server abzulehnen. Auf der anderen Seite ermöglicht das Clientzertifikat dem Bereitstellungsserver, das jeweilige Gerät zu identifizieren, das die Anforderung sendet.

Damit ein Serviceanbieter die Bereitstellung über HTTPS verwalten kann, muss für jeden Bereitstellungsserver, mit dem sich ein Telefon über HTTPS resynchronisiert, ein Serverzertifikat generiert werden. Das Serverzertifikat muss mit dem Cisco Server CA-Stammschlüssel signiert sein, dessen Zertifikat auf allen bereitgestellten Geräten vorhanden ist. Um ein signiertes Serverzertifikat zu erhalten, muss der Serviceanbieter eine Zertifikatsignieranforderung an Cisco senden. Cisco signiert das Serverzertifikat und sendet es zur Installation auf dem Bereitstellungsserver an den Serviceanbieter zurück.

Das Bereitstellungsserverzertifikat muss das Feld „Common Name“ (CN) und den FQDN des Hosts, auf dem der Server ausgeführt wird, im Betreff enthalten. Es kann nach dem FQDN des Hosts optionale Informationen enthalten, die durch einen Schrägstrich (/) getrennt angegeben werden. Die folgenden Beispiele sind CN-Einträge, die vom Telefon als gültig akzeptiert werden:

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

Zusätzlich zur Überprüfung des Serverzertifikats prüft das Telefon die IP-Adresse des Servers anhand einer DNS-Suche des Servernamens, der im Serverzertifikat angegeben ist.

Anfordern eines signierten Serverzertifikats

Das Utility OpenSSL kann eine Zertifikatsignieranforderung generieren. Das folgende Beispiel zeigt den Befehl **openssl**, der ein Paar aus einem öffentlichen und einem privaten 1024-Bit-RSA-Schlüssel und eine Zertifikatsignieranforderung erzeugt:

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

Dieser Befehl generiert den privaten Schlüssel in der Datei **privkey.pem** und die zugehörige Zertifikatsignieranforderung in der Datei **provserver.csr**. Der Serviceanbieter behält den gemeinen Schlüssel **privkey.pem** und sendet **provserver.csr** zum Signieren an Cisco. Nach dem Empfang der Datei **provserver.csr** generiert Cisco die Datei **provserver.crt**, das signierte Zertifikat.

Prozedur

Schritt 1 Navigieren Sie zu https://software.cisco.com/software/cda/home und melden Sie sich mit Ihren CCO-Anmeldeinformationen an.

Hinweis Wenn ein Telefon zum ersten Mal mit einem Netzwerk verbunden wird oder auf die Werkseinstellungen zurückgesetzt wurde und es kein DHCP-Optionen-Setup gibt, kontaktiert das Telefon einen Geräte-Aktivierungsserver für berührungsfreie Bereitstellung. Neue Telefone verwenden „activate.cisco.com“ anstelle von „webapps.cisco.com“ für die Bereitstellung. Telefone mit Firmware-Versionen vor 11.2(1) verwenden weiterhin „webapps.cisco.com“. Wir empfehlen Ihnen, beide Domänennamen in Ihrer Firewall zuzulassen.

Schritt 2 Wählen Sie **Zertifikatverwaltung** aus.

Auf der Registerkarte **CSR signieren** wird die CSR-Datei aus dem vorherigen Schritt zum Signieren hochgeladen.

Schritt 3 Wählen Sie im Dropdown-Listenfeld **Produkt auswählen** die Option **SPA1xx Firmware 1.3.3 und neuer bzw. SPA232D Firmware 1.3.3 und neuer bzw. SPA5xx Firmware 7.5.6 und neuer bzw. CP-78xx-3PCC/CP-88xx-3PCC** aus.

Schritt 4 Klicken Sie im Feld **CSR-Datei** auf **Durchsuchen**, und wählen Sie die zu signierende CSR-Datei aus.

Schritt 5 Wählen Sie die Verschlüsselungsmethode aus:

- MD5
- SHA1
- SHA256

Cisco empfiehlt die SHA256-Verschlüsselung.

Schritt 6 Wählen Sie im Dropdown-Listenfeld **Anmeldedauer** die entsprechende Dauer (z. B. 1 Jahr) aus.

Schritt 7 Klicken Sie auf **Zertifikatanforderung signieren**.

Schritt 8 Wählen Sie eine der folgenden Optionen aus, um das signierte Zertifikat zu erhalten:

- **E-Mail-Adresse des Empfängers eingeben**: Wenn Sie das Zertifikat per E-Mail erhalten möchten, geben Sie Ihre E-Mail-Adresse in dieses Feld ein.
- **Herunterladen**: Wenn Sie das signierte Zertifikat herunterladen möchten, wählen Sie diese Option aus.

Schritt 9 Klicken Sie auf **Senden**.

Das signierte Serverzertifikat wird entweder per E-Mail an die zuvor angegebene E-Mail-Adresse gesendet oder heruntergeladen.

CA-Client-Stammzertifikat für Multiplattform-Telefone

Cisco stellt dem Serviceanbieter auch ein CA-Client-Stammzertifikat für Multiplattform-Telefone bereit. Dieses Stammzertifikat zertifiziert die Echtheit des Clientzertifikats, das jedes Telefon besitzt. Die Multiplattform-Telefone unterstützen auch von Drittanbietern signierte Zertifikate, z. B. von Verisign, Cybertrust usw.

Verwenden Sie die Bereitstellungsmakrovariable $CCERT, um festzustellen, ob ein Telefon über ein individuelles Zertifikat verfügt. Je nachdem, ob ein eindeutiges Clientzertifikat vorhanden ist, wird der Variablenwert zu „Installiert“ oder „Nicht installiert“ erweitert. Bei Verwendung eines generischen Zertifikats kann die Seriennummer des Geräts dem Feld „User-Agent“ im HTTP-Anfrage-Header entnommen werden.

HTTPS-Server können so konfiguriert werden, dass sie SSL-Zertifikate von sich verbindenden Clients anfordern. Wenn die entsprechende Funktion aktiviert ist, kann der Server das CA-Client-Stammzertifikat für Multiplattform-Telefone, das Cisco bereitstellt, verwenden, um das Clientzertifikat zu überprüfen. Der Server kann die Zertifikatinformationen dann einem CGI-Skript zur weiteren Verarbeitung übergeben.

Der Speicherort des Zertifikatspeichers ist nicht bei allen Systemen gleich. In einer Apache-Installation lauten die Dateipfade zur Speicherung des vom Bereitstellungsserver signierten Zertifikats, des zugehörigen privaten Schlüssels und des CA-Client-Stammzertifikats für Multiplattform-Telefone wie folgt:

```
# 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
```

Weitere Informationen finden Sie in der Dokumentation zu einem HTTPS-Server.

Die Cisco Stammzertifizierungsstelle für Clientzertifikate signiert jedes eindeutige Zertifikat. Das entsprechende Stammzertifikat wird den Serviceanbietern für die Clientauthentifizierung zur Verfügung gestellt.

Redundante Bereitstellungsserver

Der Bereitstellungsserver kann als IP-Adresse oder als vollständiger Domänenname (FQDN) angegeben werden. Die Verwendung eines FQDN erleichtert die Bereitstellung redundanter Bereitstellungsserver. Wenn der Bereitstellungsserver durch einen FQDN identifiziert wird, versucht das Telefon, den FQDN über DNS zu einer IP-Adresse aufzulösen. Für die Bereitstellung werden nur DNS A-Einträge unterstützt. Die DNS SRV-Adressauflösung ist für die Bereitstellung nicht verfügbar. Das Telefon fährt mit der Verarbeitung von A-Einträgen fort, bis ein Server antwortet. Wenn kein Server, der den A-Einträgen zugeordnet ist, antwortet, meldet das Telefon dem Syslog-Server einen Fehler.

Syslog-Server

Wenn ein Syslog-Server auf dem Telefon unter Verwendung der <Syslog Server>-Parameter konfiguriert wird, werden bei Resynchronisierungs- und Upgrade-Vorgängen Meldungen an den Syslog-Server gesendet. Meldungen können zu Beginn einer Remotedateianforderung (Laden des Konfigurationsprofils oder der Firmware) und nach Abschluss des Vorgangs (Erfolgs- oder Fehlermeldung) generiert werden.

Die protokollierten Meldungen werden in den folgenden Parametern konfiguriert und per Makro zu den tatsächlichen Syslog-Meldungen erweitert:

Firewall aktivieren

Wir haben die Telefonsicherheit verbessert, indem wir das Betriebssystem abgesichert haben. Durch die Absicherung wird sichergestellt, dass das Telefon über eine Firewall verfügt, um es vor bösartigem eingehenden Datenverkehr zu schützen. Die Firewall verfolgt die Ports für ein- und ausgehende Daten. Sie erkennt eingehenden Datenverkehr von unerwarteten Quellen und blockiert den Zugriff. Ihre Firewall ermöglicht den gesamten ausgehenden Datenverkehr.

Die Firewall kann normalerweise blockierte Ports dynamisch entsperren. Die ausgehende TCP-Verbindung oder der UDP-Fluss entsperrt den Port für die Rückgabe und den fortgesetzten Datenverkehr. Der Port wird nicht blockiert, während der Fluss aktiv ist. Der Port kehrt in den Status „blockiert“ zurück, wenn der Fluss endet oder veraltet ist.

Die Legacy-Einstellung, IPv6-Multicast-Pingt **Sprache** > **System** > **IPv6-Einstellungen** > **Broadcast-Echo** funktioniert weiterhin unabhängig von den neuen Firewall-Einstellungen.

Änderungen der Firewall-Konfiguration führen in der Regel nicht zu einem Neustart des Telefons. Ein Soft-Neustart des Telefons hat in der Regel keine Auswirkungen auf den Firewall-Betrieb.

Die Firewall ist standardmäßig aktiviert. Wenn sie deaktiviert ist, können Sie sie über die Seite „Telefon“ aktivieren.

Vorbereitungen

Auf Weboberfläche des Telefons zugreifen

Prozedur

Schritt 1 Wählen Sie **Sprache** > **System** > **Sicherheitseinstellungen** aus.

Schritt 2 Wählen Sie in der Dropdown-Liste **Firewall** die Option **Aktiviert** aus.

Sie können diesen Parameter ebenfalls in der Konfigurationsdatei (cfg.xml) konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Die zulässigen Werte sind Deaktiviert|Aktiviert. Der Standardwert ist Aktiviert.

Schritt 3 Klicken Sie auf **Submit All Changes**.
Dadurch wird die Firewall mit ihren standardmäßig geöffneten UDP- und TCP-Ports aktiviert.

Schritt 4 Wählen Sie **Deaktiviert**, um die Firewall zu deaktivieren, wenn Sie möchten, dass Ihr Netzwerk zu seinem vorherigen Verhalten zurückkehrt.

Die folgende Tabelle beschreibt die standardmäßigen offenen UDP-Ports.

Tabelle 3: Standardmäßige offene UDP-Ports der Firewall

Standardmäßiger offener UDP-Port	Beschreibung
DHCP/DHCPv6	DHCP-Client-Port 68 DHCPv6-Client-Port 546
SIP/UDP	Konfigurieren Sie den Port in **Sprache** > **Durchwahl<n>** > **SIP-Einstellungen** > **SIP-Port** (Beispiel: 5060), wenn **Leitungen aktivieren** auf **`Ja`** und **SIP-Transport** auf **`UDP`** oder **`Automatisch`** festgelegt ist.
RTP/RTCP	UDP-Portbereich von **`RTP Port Min.`** bis **`RTP Port Max. + 1`**
PFS (Peer-Firmware-Freigabe)	Port 4051, wenn **Upgrade aktivieren** und **Peer-Firmware-Freigabe** auf **`Ja`** gesetzt ist.
TFTP-Clients	Ports 53240-53245. Sie benötigen diesen Portbereich, wenn der Remote-Server einen anderen Port als den Standard-TFTP-Port 69 verwendet. Sie können die Option deaktivieren, wenn der Server den Standard-Port 69 verwendet. Siehe Konfigurieren Sie Ihre Firewall mit zusätzlichen Optionen, auf Seite 12.
TR-069	UDP/STUN-Port 7999, wenn die Option **TR-069 aktivieren** auf **`Ja`** gesetzt ist.

Die folgende Tabelle beschreibt die standardmäßigen offenen TCP-Ports.

Tabelle 4: Standardmäßige offene TCP-Ports der Firewall

Standardmäßiger offener TCP-Port	Beschreibung
Webserver	Port, der über den Webserver-Port konfiguriert wurde (Standard 80), wenn **Webserver aktivieren** auf **Ja** gesetzt ist.
PFS (Peer-Firmware-Freigabe)	Ports 4051 und 6970, wenn **Upgrade aktivieren** und **Peer-Firmware-Freigabe** und **Ja** gesetzt sind.
TR-069	HTTP/SOAP-Port in TR-069 Verbindungsanforderungs-URL, wenn **TR-069 aktivieren** auf **Ja** gesetzt wurde. Der Port wird zufällig aus dem Bereich 8000-9999 ausgewählt.

Konfigurieren Sie Ihre Firewall mit zusätzlichen Optionen

Sie können zusätzliche Optionen im Feld **Firewall-Optionen** konfigurieren. Geben Sie das Schlüsselwort für jede Option in das Feld ein und trennen Sie die Schlüsselwörter durch Kommas (,). Einige Schlüsselwörter verfügen über Werte. Trennen Sie die Werte durch Doppelpunkte (:).

Vorbereitungen

Auf Weboberfläche des Telefons zugreifen

Prozedur

Schritt 1 Gehen Sie zu **Sprache** > **System** > **Sicherheitseinstellungen**.

Schritt 2 Wählen Sie **Aktiviert** für das Feld **Firewall** aus.

Schritt 3 Geben Sie im Feld **Firewall-Optionen** die Schlüsselwörter ein. Die Liste der Ports gilt für IPv4- und IPv6-Protokolle.

Wenn Sie die Schlüsselwörter eingeben,

- trennen Sie die Schlüsselwörter durch Kommas (,).
- trennen Sie die Werte der Schlüsselwörter mit Doppelpunkten (:).

Tabelle 5: Optionale Firewall-Einstellungen

Schlüsselwörter für Firewall-Optionen	Beschreibung
Feld ist leer.	Die Firewall wird mit standardmäßig geöffneten Ports ausgeführt.

Schlüsselwörter für Firewall-Optionen	Beschreibung
NO_ICMP_PING	Die Firewall blockiert eingehende ICMP/ICMPv6-**`Echo`**-Anforderungen (Ping). Diese Option kann einige Arten von Traceroute-Anforderungen an das Telefon aufheben. Windows **`tracert`** ist ein Beispiel. Beispielhafter Eintrag für **Firewall-Optionen** mit einer Kombination von Optionen: NO_ICMP_PING,TCP:12000,UDP:8000:8010 Die Firewall wird mit den Standardeinstellungen und den folgenden zusätzlichen Optionen ausgeführt: • Löscht eingehende ICMP/ICMPv6-**`Echo`**-Anforderungen (Ping). • Öffnet TCP-Port 12000 (IPv4 und IPv6) für eingehende Verbindungen. • Öffnet den UDP-Portbereich 8000-8010 (IPv4 und IPv6) für eingehende Anforderungen.
NO_ICMP_UNREACHABLE	Das Telefon sendet ICMP/ICMPv6-`Ziel nicht erreichbar` für UDP-Ports nicht. **Hinweis** Die Ausnahme besteht darin, das `Ziel nicht erreichbar` immer für Ports im RTP-Portbereich zu senden. Diese Option kann einige Arten von **`Traceroute`**-Anforderungen an das Gerät aufheben. Beispiel: Linux **`traceroute`** kann unterbrochen werden.
NO_CISCO_TFTP	• Das Telefon öffnet den TFTP-Client-Portbereich (UDP 53240:53245) nicht. • Anforderungen an nicht standardmäßige (nicht 69) TFTP-Server-Ports schlagen fehl. • Anforderungen an den Standard-TFTP-Server-Port 69 funktionieren.
Die folgenden Schlüsselwörter und Optionen gelten, wenn auf dem Telefon benutzerdefinierte Apps ausgeführt werden, die eingehende Anforderungen verarbeiten.	
UDP:<xxx>	Öffnet den UDP-Port <xxx>.
UDP:<xxx:yyy>	Öffnet den UDP-Portbereich, einschließlich <xxx to yyy>. Sie können bis zu 5 UDP-Portoptionen (einzelne Durchwahlen und Portbereiche) haben. Sie können beispielsweise über 3 UDP verfügen:<xxx> und 2 UDP:<xxx:yyy>.

Schlüsselwörter für Firewall-Optionen	Beschreibung
TCP:<xxx>	Öffnet den TCP-Port <xxx>.
TCP:<xxx:yyy>	Öffnet den TCP-Portbereich, einschließlich <xxx to yyy>. Sie können bis zu 5 TCP-Portoptionen (einzelne Durchwahlen und Portbereiche) haben. Sie können beispielsweise über 4 TCP verfügen:<xxx> und einen TCP:<xxx:yyy>

Sie können diesen Parameter ebenfalls in der Konfigurationsdatei (cfg.xml) konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Schritt 4 Klicken Sie auf **Submit All Changes**.

Verschlüsselungsliste konfigurieren

Sie können die Verschlüsselungspakete angeben, die von den TLS-Anwendungen des Telefons verwendet werden. Die angegebene Verschlüsselungsliste gilt für alle Anwendungen, die das TLS-Protokoll verwenden. Die TLS-Anwendungen auf Ihrem Telefon umfassen Folgendes:

- Kunden-CA-Bereitstellung
- E911-Geolokation
- Firmware/Cisco-Headset-Upgrade
- LDAPS
- LDAP (StartTLS)
- Bilddownload
- Logo-Download
- Wörterbuch-Download
- Bereitstellung
- Bericht-Upload
- PRT-Upload
- SIP über TLS
- TR-069
- WebSocket-API
- XML-Dienste
- XSI-Dienste

Sie können die Verschlüsselungspakete auch mit dem TR-069-Parameter (`Device.X_CISCO_SecuritySettings.TLSCipherList`) oder mit der Konfigurationsdatei (cfg.xml) angeben. Geben Sie in der Konfigurationsdatei eine Zeichenfolge in folgendem Format eingeben:

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

Vorbereitungen

Für Zugriff auf die Telefonverwaltung über die Weboberfläche siehe Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Voice** > **System** aus.

Schritt 2 Geben Sie im Abschnitt **Sicherheitseinstellungen** das Verschlüsselungspaket oder die Kombination aus Verschlüsselungspaketen im Feld **TLS-Verschlüsselungsliste** ein.

Beispiel:

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

Unterstützt die Verschlüsselungspakete mit RSA-Authentifizierung, schließt jedoch die Verschlüsselungspakete aus, die keine Verschlüsselung und Authentifizierung bieten.

Hinweis Eine gültige Verschlüsselungsliste muss dem Format entsprechen, das unter https://www.openssl.org/docs/man1.1.1/man1/ciphers.html beschrieben wird. Ihr Telefon unterstützt nicht alle auf der OpenSSL-Webseite aufgeführten Verschlüsselungszeichenfolgen. Die unterstützten Zeichenfolgen finden Sie unter Unterstützte Zeichenfolgen für Verschlüsselung, auf Seite 16.

Bei einem leeren oder ungültigen Wert im Feld **TLS-Verschlüsselungsliste** unterscheiden sich die verwendeten Verschlüsselungspakete je nach Anwendung. In der folgenden Liste sind die Pakete aufgeführt, die von den Anwendungen verwendet werden, wenn dieses Feld einen leeren oder einen ungültigen Wert enthält.

- Webserver-(HTTPS)-Anwendungen verwenden die folgenden Verschlüsselungspakete:
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**
  - **DES-CBC3-SHA**
- XMPP verwendet die Verschlüsselungsliste **HIGH:MEDIUM:AES:@STRENGTH**.
- SIP, TR-069 und andere Anwendungen, die die Curl-Bibliothek verwenden, verwenden die **STANDARD**-Verschlüsselungszeichenfolge. Die **DEFAULT**-Verschlüsselungszeichenfolge enthält die folgenden Verschlüsselungssuites, die vom Telefon unterstützt werden:

```
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
```

Schritt 3 Klicken Sie auf **Submit All Changes**.

Unterstützte Zeichenfolgen für Verschlüsselung

Die unterstützten Zeichenfolgen für Verschlüsselung, die im Folgenden aufgeführt sind, basieren auf den Standards OpenSSL 1.1.1d.

Tabelle 6: Unterstützte Zeichenfolgen für Verschlüsselung (OpenSSL 1.1.1d)

Zeichenfolgen	Zeichenfolgen	Zeichenfolgen
STANDARD	kECDHE, kEECDH	CAMELLIA128, CAMELLIA256, Camellia
COMPLEMENTOFDEFAULT	ECDHE, EECDH	CHACHA20
ALLE	ECDH	SEED
COMPLEMENTOFALL	AECDH	MD5
HOCH	aRSA	SHA1, SHA
MITTEL	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	

Zeichenfolgen	Zeichenfolgen	Zeichenfolgen
DHE, EDH	AESCCM, AESCCM8	
ADH	ARIA128, ARIA256, ARIA	

Verifizierung des Host-Namens für SIP über TLS aktivieren

Sie können eine erhöhte Telefonsicherheit auf einer Telefonleitung aktivieren, wenn Sie TLS verwenden. Die Telefonleitung kann den Host-Namen überprüfen, um festzustellen, ob die Verbindung sicher ist.

Über eine TLS-Verbindung kann das Telefon den Host-Namen überprüfen, um die Serveridentität zu überprüfen. Das Telefon kann sowohl den „Subject Alternative Name (SAN)“ als auch den „Common Name (CN)“ überprüfen. Wenn der Host-Name des gültigen Zertifikats mit dem Host-Namen übereinstimmt, der für die Kommunikation mit dem Server verwendet wird, wird die TLS-Verbindung erstellt. Andernfalls schlägt die TLS-Verbindung fehl.

Das Telefon überprüft immer den Host-Namen für die folgenden Anwendungen:

- LDAPS
- LDAP (StartTLS)
- XMPP
- Image-Upgrade über HTTPS
- XSI über HTTPS
- Dateidownload über HTTPS
- TR-069

Wenn eine Telefonleitung SIP-Nachrichten über TLS transportiert, können Sie die Leitung so konfigurieren, dass die Überprüfung des Host-Namens mit dem Feld **TLS-Name validieren** auf der Registerkarte **Durchwahl(n)** aktiviert oder umgangen wird.

Vorbereitungen

- Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe Auf Weboberfläche des Telefons zugreifen.
- Setzen Sie auf der Registerkarte **Durchwahl(n)SIP-Transport** auf **TLS**.

Prozedur

Schritt 1 Gehen Sie zu **Sprache** > **Durchwahl(n)**.

Schritt 2 Setzen Sie im Abschnitt **Proxy und Registrierung** das Feld **TLS-Name validieren** auf **Ja**, um die Überprüfung des Host-Namens zu aktivieren, oder auf **Nein**, um die Überprüfung des Host-Namens zu umgehen.

Sie können diesen Parameter ebenfalls in der Konfigurationsdatei (cfg.xml) konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

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

Die zulässigen Werte sind Ja oder Nein. Die Standardeinstellung ist Ja.

Schritt 3 Klicken Sie auf **Submit All Changes**.

Client-initiierten Modus für Sicherheitsverhandlungen in der Medienebene aktivieren

Um Mediensitzungen zu schützen, können Sie das Telefon so konfigurieren, dass Sicherheitsverhandlungen auf Medienebene mit dem Server eingeleitet werden. Der Sicherheitsmechanismus entspricht den in RFC 3329 genannten Standards und seinen Erweiterungsentwürfen für *Sicherheitsmechanismen für Medien* (siehe https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2). Der Transport von Verhandlungen zwischen dem Telefon und dem Server kann das SIP-Protokoll über UDP, TCP und TLS verwenden. Sie können die Sicherheitsverhandlungen auf Medienebene einschränken, wenn das signalisierende Transportprotokoll TLS ist.

Sie können die Parameter ebenfalls in der Konfigurationsdatei (cfg.xml) konfigurieren. Zur Konfiguration der einzelnen Parameter siehe Syntax der Zeichenfolge in Parameter für die Medienebene-Sicherheitsverhandlung, auf Seite 18.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Sprache** > **Durchwahl(n)** aus.

Schritt 2 Legen Sie im Abschnitt **SIP-Einstellungen** die Felder **MediaSec-Anfrage** und **MediaSec nur über TLS** wie in Parameter für die Medienebene-Sicherheitsverhandlung, auf Seite 18 beschrieben fest.

Schritt 3 Klicken Sie auf **Submit All Changes**.

Parameter für die Medienebene-Sicherheitsverhandlung

In der folgenden Tabelle werden die Funktionen und die Verwendung der Parameter für die Medienebene-Sicherheitsverhandlung im Abschnitt **SIP-Einstellungen** in der Registerkarte **Voice**> **Ext (n)** in der Telefon-Weboberfläche definiert. Außerdem wird die Syntax der Zeichenfolge definiert, die in der Telefon-Konfigurationsdatei mit dem XML-Code (cfg.xml) hinzugefügt wird, um einen Parameter zu konfigurieren.

Tabelle 7: Parameter für die Medienebene-Sicherheitsverhandlung

Parameter	Beschreibung
MediaSec-Anforderung	Gibt an, ob das Telefon Medienebene-Sicherheitsverhandlungen mit dem Server initiiert. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>` • Legen Sie in der Telefon-Weboberfläche dieses Feld nach Bedarf auf **Ja** oder **Nein** fest. Zulässige Werte: Ja|Nein • **Ja**: vom Client initiierter Modus. Das Telefon initiiert Medienplan-Sicherheitsverhandlungen. • **Nein**: Server initiierter Modus. Der Server initiiert Sicherheitsverhandlungen in der Medienebene. Das Telefon initiiert keine Verhandlungen, kann aber Aushandlungsanfragen vom Server bearbeiten, um sichere Anrufe zu initiieren. Standard: Nein
MediaSec nur über TLS	Gibt das signalisierende Transportprotokoll an, über das die Medienebene-Sicherheitsverhandlung angewendet wird. Bevor Sie dieses Feld auf **Ja** festlegen, müssen Sie sicherstellen, dass das signalisierende Transportprotokoll TLS ist. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>` • Legen Sie in der Telefon-Weboberfläche dieses Feld nach Bedarf auf **Ja** oder **Nein** fest. Zulässige Werte: Ja|Nein • **Ja**: das Telefon initiiert oder bearbeitet Sicherheitsverhandlungen in der Medienebene nur, wenn das signalisierende Transportprotokoll TLS ist. • **Nein**: das Telefon initiiert und bearbeitet Medienplan-Sicherheitsverhandlungen, unabhängig vom Signalisierungs-Transportprotokoll. Standard: Nein

802.1X-Authentifizierung

Cisco IP-Telefone verwenden zum Identifizieren des LAN-Switches und zum Bestimmen von Parametern wie z.B. VLAN- Zuweisung und Inline-Stromanforderungen das Cisco Discovery Protocol (CDP). CDP identifiziert lokal verbundene Arbeitsstationen nicht. Cisco IP-Telefons stellen eine Durchlaufmethode bereit. Diese Methode ermöglicht einer Arbeitsstation, die mit Cisco IP-Telefon verbunden ist, EAPOL-Meldungen an den 802.1X-Authentifikator auf dem LAN-Switch zu übermitteln. Die Durchlaufmethode stellt sicher, dass das IP-Telefon nicht als LAN-Switch agiert, um einen Datenendpunkt zu authentifizieren, bevor das Telefon auf das Netzwerk zugreift.

Cisco IP-Telefons stellen auch eine Proxy-EAPOL-Logoff-Methode bereit. Wenn der lokal verbundene PC vom IP-Telefon getrennt wird, erkennt der LAN-Switch nicht, dass die physische Verbindung unterbrochen wurde, da die Verbindung zwischen dem LAN-Switch und dem IP-Telefon aufrechterhalten wird. Um eine Gefährdung der Netzwerkintegrität zu verhindern, sendet das IP-Telefon im Auftrag des nachgelagerten PCs eine EAPOL-Logoff-Meldung an den Switch, die den LAN-Switch veranlasst, den Authentifizierungseintrag für den nachgelagerten PC zu löschen.

Für die Unterstützung der 802.1X-Authentifizierung sind mehrere Komponenten erforderlich:

- Cisco IP-Telefon: Das Telefon initiiert die Anforderung, um auf das Netzwerk zuzugreifen. Das Cisco IP-Telefon enthält ein 802.1X Supplicant. Dieses Supplicant ermöglicht Netzwerkadministratoren die Verbindung von IP-Telefonen mit den LAN-Switch-Ports zu steuern. Die aktuelle Version des 802.1X Supplicant verwendet EAP-FAST und EAP-TLS für die Netzwerkauthentifizierung.
- Cisco Secure Access Control Server (ACS) (oder ein anderer Authentifizierungsserver eines Drittanbieters): Der Authentifizierungsserver und das Telefon müssen beide mit einem Shared Secret konfiguriert werden, mit dem das Telefon authentifiziert werden kann.
- Ein LAN-Switch, der 802.1X unterstützt: Der Switch fungiert als Authentifikator und übermittelt die Nachrichten zwischen Telefon und Authentifizierungsserver. Nach dem Meldungsaustausch gewährt oder verweigert der Switch dem Telefon den Zugriff auf das Netzwerk.

Um 802.1X zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

- Konfigurieren Sie die anderen Komponenten, bevor Sie die 802.1X-Authentifizierung auf dem Telefon aktivieren.
- PC-Port konfigurieren: Der 802.1X-Standard berücksichtigt VLANs nicht und empfiehlt deshalb, dass an einem Switch-Port nur ein Gerät authentifiziert werden sollte. Dennoch unterstützen einige Switches die Multidomain-Authentifizierung. Die Switch-Konfiguration bestimmt, ob Sie einen PC an einen PC-Port des Telefon anschließen können.
  - Ja: Wenn Sie einen Schalter verwenden, der Multidomain-Authentifizierung unterstützt, können Sie den PC-Port aktivieren und einen PC daran anschließen. In diesem Fall unterstützen Cisco IP-Telefone Proxy-EAPOL-Logoff, um die Authentifizierung zwischen dem Switch und dem angeschlossenen PC zu überwachen.
  - Nein: Wenn der Switch 802.1X-Authentifizierung-kompatible Geräte an demselben Port nicht unterstützt, sollten Sie den PC-Port deaktivieren, wenn die 802.1X-Authentifizierung aktiviert ist. Wenn Sie diesen Port nicht deaktivieren und versuchen, einen PC anzuschließen, verweigert der Switch den Netzwerkzugriff auf das Telefon und den PC.
- Sprach-VLAN konfigurieren: Da VLANs von 802.1X-Standard nicht berücksichtigt werden, sollten Sie diese Einstellung basierend auf der Switch-Unterstützung konfigurieren.

- Aktiviert: Wenn Sie einen Switch verwenden, der die Authentifizierung in mehreren Domänen unterstützt, können Sie das Sprach-VLAN weiterhin verwenden.
- Deaktiviert: Wenn der Switch die Authentifizierung in mehreren Domänen nicht unterstützt, deaktivieren Sie das Sprach-VLAN und weisen Sie den Port dem systemeigenen VLAN zu.

802.1X-Authentifizierung aktivieren

Sie können die 802.1X-Authentifizierung auf dem Telefon aktivieren. Wenn die 802.1X-Authentifizierung aktiviert ist, verwendet das Telefon die 802.1X-Authentifizierung, um den Netzwerkzugang anzufordern. Wenn die 802.1X-Authentifizierung deaktiviert ist, verwendet das Telefon CDP, um VLAN- und Netzwerkzugang zu erhalten. Sie können den Transaktionsstatus auch im Menü des Telefonbildschirms sehen.

Prozedur

Schritt 1 Führen Sie eine der folgenden Aktionen aus, um die 802.1X-Authentifizierung zu aktivieren:

- Wählen Sie auf der Weboberfläche des Telefons **Sprache** > **System** aus und setzen Sie das Feld **802.1X-Authentifizierung** auf **Ja**. Klicken Sie anschließend auf **Alle Änderungen annehmen**.
- Geben Sie in der Konfigurationsdatei (cfg.xml) eine Zeichenfolge in folgendem Format eingeben:

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

- Drücken Sie auf dem Telefon **Anwendungen** > **Netzwerkkonfiguration** > **Ethernetkonfiguration** > **802.1X-Authentifizierung**. Setzen Sie anschließend das Feld **Geräteauthentifizierung** mit der **Auswahl**-Taste auf **Ein** und drücken Sie **Senden**.

Schritt 2 (Optional) Wählen Sie **Transaktionsstatus** aus, um Folgendes anzuzeigen:

- **Transaktionsstatus**: Status der 802.1X-Authentifizierung anzeigen. Der Status kann folgendes sein
  - *Wird authentifiziert*: Zeigt an, dass der Authentifizierungsvorgang in Bearbeitung ist.
  - *Authentifiziert*: Zeigt an, dass das Telefon authentifiziert wurde.
  - *Deaktiviert*: Zeigt an, dass die 802.1X-Authentifizierung auf diesem Telefon deaktiviert wurde.
- **Protokoll**: Zeigt die EAP-Methode an, die für die 802.1X-Authentifizierung verwendet wird. Das Protokoll kann EAP-FAST oder EAP-TLS sein.

Schritt 3 Drücken Sie **Zurück**, um das Menü zu verlassen.

Proxyserver einrichten

Sie können das Telefon so konfigurieren, dass es einen Proxyserver verwendet, um die Sicherheit zu erhöhen. Ein Proxyserver fungiert als Firewall zwischen dem Telefon und dem Internet. Nach erfolgreicher Konfiguration wird das Telefon über den Proxyserver mit dem Internet verbunden, um das Telefon vor Cyber-Angriffen zu schützen.

Sie können einen Proxyserver einrichten, indem Sie entweder ein automatisches Konfigurationsskript verwenden oder den Hostserver (Host-Name oder IP-Adresse) und den Port des Proxyservers manuell konfigurieren.

Nach der Konfiguration gilt die HTTP-Proxyfunktion für alle Anwendungen, die das HTTP-Protokoll verwenden. Die Anwendungen umfassen Folgendes:

- GDS (Integration des Aktivierungscodes)
- EDOS-Geräteaktivierung
- Onboarding für Webex Cloud (über EDOS und GDS)
- Zertifikatauthentifizierung
- Bereitstellung
- Firmware-Upgrade
- Telefonstatusbericht
- PRT-Upload
- XSI-Dienste
- Webex-Dienste

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe Auf Weboberfläche des Telefons zugreifen.

Prozedur

Schritt 1 Wählen Sie **Sprache** > **System** aus.

Schritt 2 Konfigurieren Sie im Abschnitt **HTTP-Proxyeinstellungen** den Parameter **Proxymodus** und andere entsprechend Ihrer Anforderung. Detaillierte Verfahren finden Sie in den folgenden Schritten.

Schritt 3 Führen Sie einen der folgenden Schritte aus:

- Der **Proxymodus** lautet **Automatisch**:
  - Wenn **Automatische Erkennung verwenden (WPAD)** dem Wert **Ja** entspricht, ist keine weitere Aktion erforderlich. Das Telefon ruft anhand des WPAD-Protokolls (Web Proxy Auto-Discovery) automatisch eine PAC-Datei (Proxy Auto-Configuration) ab.
  - Wenn **Automatische Erkennung verwenden (WPAD)** auf **Nein** festgelegt ist, geben Sie eine gültige URL in **PAC-URL** ein.
- Der **Proxymodus** lautet **Manuell**:
  - Wenn **Proxyserver erfordert Authentifizierung** auf **Nein** festgelegt ist, geben Sie einen Proxyserver in **Proxyhost** und einen Proxyport in **Proxyport** ein.
  - Wenn **Proxyserver erfordert Authentifizierung** auf **Ja** festgelegt ist, geben Sie einen Proxyserver in **Proxyhost** und einen Proxyport in **Proxyport** ein. Geben Sie einen Benutzernamen in **Benutzername** und ein Kennwort in **Kennwort** ein.
- Falls der **Proxymodus** auf **Aus** festgelegt ist, ist die HTTP-Proxyfunktion auf dem Telefon deaktiviert.

Sie können die Parameter ebenfalls in der Konfigurationsdatei (cfg.xml) des Telefons konfigurieren. Zur Konfiguration der einzelnen Parameter siehe Syntax der Zeichenfolge in Parameter für HTTP-Proxyeinstellungen, auf Seite 23.

Schritt 4 Klicken Sie auf **Submit All Changes**.

Parameter für HTTP-Proxyeinstellungen

In der folgenden Tabelle werden die Funktionen und die Verwendung der HTTP-Proxyparameter im Abschnitt **HTTP-Proxyeinstellungen** auf der Registerkarte **Sprache** > **System** auf der Telefon-Weboberfläche definiert. Außerdem wird die Syntax der Zeichenfolge definiert, die in der Telefon-Konfigurationsdatei mit dem XML-Code (cfg.xml) hinzugefügt wird, um einen Parameter zu konfigurieren.

Tabelle 8: Parameter für HTTP-Proxyeinstellungen

Parameter	Beschreibung und Standardwert
Proxymodus	Gibt den vom Telefon verwendeten HTTP-Proxymodus an oder deaktiviert die HTTP-Proxyfunktion. • Auto Das Telefon ruft automatisch eine PAC-Datei (Proxy Auto-Configuration) ab, um einen Proxyserver auszuwählen. In diesem Modus können Sie festlegen, ob das WPAD-Protokoll (Web Proxy Auto-Discovery) verwendet werden soll, um eine PAC-Datei abzurufen oder eine gültige URL der PAC-Datei manuell einzugeben. Weitere Informationen zu den Parametern finden Sie unter Automatische Erkennung verwenden (WPAD) und PAC-URL. • Manuell Sie müssen einen Server (Host-Name oder IP-Adresse) und einen Port eines Proxyservers manuell angeben. Weitere Informationen zu den Parametern finden Sie unter Proxyhost und Proxyport. • Aus Sie deaktivieren die HTTP-Proxyfunktion auf dem Telefon. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<Proxy_Mode ua="rw">Off</Proxy_Mode>` • Wählen Sie auf der Weboberfläche des Telefons einen Proxymodus aus, oder deaktivieren Sie die Funktion. Zulässige Werte: „Automatisch“, „Manuell“ und „Aus“ Standardeinstellung: Aus

Parameter	Beschreibung und Standardwert
Automatische Erkennung verwenden (WPAD)	Legt fest, ob das Telefon das WPAD-Protokoll (Web Proxy Auto-Discovery) verwendet, um eine PAC-Datei abzurufen. Das WPAD-Protokoll verwendet DHCP oder DNS oder beide Netzwerkprotokolle, um automatisch eine PAC-Datei (Proxy Auto-Configuration) zu suchen. Die PAC-Datei wird verwendet, um einen Proxyserver für eine bestimmte URL auszuwählen. Diese Datei kann lokal oder in einem Netzwerk gehostet werden. • Die Parameterkonfiguration wird wirksam, wenn der **Proxymodus** auf **Automatisch** festgelegt ist. • Wenn Sie den Parameter auf **Nein** festlegen, müssen Sie eine PAC-URL angeben. Weitere Informationen zum Parameter finden Sie unter PAC-URL. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<Use_Auto_Discovery__WPAD_ ua="rw">Yes</Use_Auto_Discovery__WPAD_>` • Wählen Sie auf der Weboberfläche des Telefons die Option „Ja“ oder „Nein“ aus. Zulässige Werte: Ja und Nein Standard: Ja
PAC-URL	URL einer PAC-Datei. Beispiel: `http://proxy.department.branch.example.com` Nur TFTP, HTTP und HTTPS werden unterstützt. Wenn Sie den **Proxymodus** auf **Automatisch** und **Automatische Erkennung verwenden (WPAD)** auf **No** festlegen, müssen Sie diesen Parameter konfigurieren. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<PAC_URL ua="rw">http://proxy.department.branch.example.com/pac</PAC_URL>` • Geben Sie auf der Weboberfläche des Telefons eine gültige URL ein, die zu einer PAC-Datei führt. Standard: leer

Parameter	Beschreibung und Standardwert

Proxyhost	IP-Adresse oder Host-Name des Proxyhostservers, worauf das Telefon zugreifen soll. Zum Beispiel:
	`proxy.example.com`
	Das Schema (`http://` oder `https://`) ist nicht erforderlich.
	Wenn Sie den **Proxymodus** auf **Manuell** festlegen, müssen Sie diesen Parameter konfigurieren.
	Führen Sie eine der folgenden Aktionen aus:
	• Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein:
	`<Proxy_Host ua="rw">proxy.example.com</Proxy_Host>`
	• Geben Sie auf der Weboberfläche des Telefons eine IP-Adresse oder den Host-Namen des Proxyservers ein.
	Standard: leer

Proxyport	Portnummer des Proxyhostservers. Wenn Sie den **Proxymodus** auf **Manuell** festlegen, müssen Sie diesen Parameter konfigurieren. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<Proxy_Port ua="rw">3128</Proxy_Port>` • Geben Sie auf der Weboberfläche des Telefons einen Serverport ein. Standard: 3128

Parameter	Beschreibung und Standardwert
Proxyserver erfordert Authentifizierung	Legt fest, ob der Benutzer die für den Proxyserver erforderlichen Anmeldeinformationen für die Authentifizierung (Benutzername und Kennwort) angeben muss. Dieser Parameter wird entsprechend dem tatsächlichen Verhalten des Proxyservers konfiguriert. Wenn Sie den Parameter auf **Ja** festlegen, müssen Sie den **Benutzernamen** und das **Kennwort** konfigurieren. Weitere Informationen zu den Parametern finden Sie unter Benutzername und Kennwort. Die Parameterkonfiguration wird wirksam, wenn der **Proxymodus** auf **Manuell** festgelegt ist. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<Proxy_Server_Requires_Authentication ua="rw">No</Proxy_Server_Requires_Authentication>` • Legen Sie auf der Weboberfläche des Telefons dieses Feld nach Bedarf auf „Ja“ oder „Nein“ fest. Zulässige Werte: Ja und Nein Standard: Nein
Benutzername	Benutzername für einen authentifizierten Benutzer auf dem Proxyserver. Wenn **Proxymodus** auf **Manuell** und **Proxyserver erfordert Authentifizierung** auf **Ja** festgelegt ist, müssen Sie den Parameter konfigurieren. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<Proxy_Username ua="rw">Example</Proxy_Username>` • Geben Sie auf der Weboberfläche des Telefons den Benutzernamen ein. Standard: leer

Parameter	Beschreibung und Standardwert
Kennwort	Kennwort des angegebenen Benutzernamens für die Proxyauthentifizierung. Wenn **Proxymodus** auf **Manuell** und **Proxyserver erfordert Authentifizierung** auf **Ja** festgelegt ist, müssen Sie den Parameter konfigurieren. Führen Sie eine der folgenden Aktionen aus: • Geben Sie in der Konfigurationsdatei des Telefons eine Zeichenfolge mit XML (cfg.xml) in folgendem Format ein: `<Proxy_Password ua="rw">Example</Proxy_Password>` • Geben Sie auf der Weboberfläche des Telefons ein gültiges Kennwort für die Proxyauthentifizierung des Benutzers ein. Standard: leer

Übersicht über die Cisco Produktsicherheit

Dieses Produkt enthält Verschlüsselungsfunktionen und unterliegt den geltenden Gesetzen in den USA oder des jeweiligen Landes bezüglich Import, Export, Weitergabe und Nutzung des Produkts. Die Bereitstellung von Verschlüsselungsprodukten durch Cisco gewährt Dritten nicht das Recht, die Verschlüsselungsfunktionen zu importieren, zu exportieren, weiterzugeben oder zu nutzen. Importeure, Exporteure, Vertriebshändler und Benutzer sind für die Einhaltung aller jeweils geltenden Gesetze verantwortlich. Durch die Verwendung dieses Produkts erklären Sie, alle geltenden Gesetze und Vorschriften einzuhalten. Wenn Sie die geltenden Gesetze nicht einhalten können, müssen Sie das Produkt umgehend zurückgeben.

Weitere Angaben zu den Exportvorschriften der USA finden Sie unter https://www.bis.doc.gov/policiesandregulations/ear/index.htm.