Sicherheit von Cisco IP-Telefonen

Übersicht der Sicherheit des Cisco IP-Telefon

Die Sicherheitsfunktionen schützen vor mehreren Gefahren, beispielsweise der Gefährdung der Identität des Telefons und der Daten. Diese Funktionen erstellen und halten authentifizierte Kommunikationsstreams zwischen dem Telefon und dem Cisco Unified Communications Manager-Server aufrecht, und stellen sicher, dass das Telefon nur digital signierte Dateien verwendet.

In Cisco Unified Communications Manager Version 8.5(1) und höheren Versionen ist Security by Default implementiert. Diese Komponente stellt die folgenden Sicherheitsfunktionen für Cisco IP-Telefons ohne CTL-Client bereit:

- Signierung der Konfigurationsdateien für das Telefon
- Verschlüsselung der Telefonkonfigurationsdatei
- HTTPS mit Tomcat und andere Webservices

Hinweis Für sichere Signalübertragungs- und Medienfunktionen muss der CTL-Client jedoch weiterhin ausgeführt werden, und es ist weiterhin die Verwendung von Hardware-eToken erforderlich.

Weitere Informationen zu den Sicherheitsfunktionen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Nachdem Sie die für die CAPF (Certificate Authority Proxy Function) erforderlichen Aufgaben ausgeführt haben, wird auf den Telefonen ein LSC (Locally Significant Certificate) installiert. Sie können ein LSC in der Cisco Unified Communications Manager Administration-Verwaltung konfigurieren. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Ein LSC kann für EAP-TLS mit WLAN-Authentifizierung nicht als Benutzerzertifikat verwendet werden.

Alternativ dazu können Sie die Installation eines LSC auch im Menü „Sicherheits-Setup“ des Telefons veranlassen. In diesem Menü können Sie ein LSC auch aktualisieren und entfernen.

Cisco IP-Telefon 7800-Serie entspricht dem FIPS (Federal Information Processing Standard). Um ordnungsgemäß zu funktionieren, ist für den FIPS-Modus eine RSA-Schlüssellänge von mindestens 2048 Bit erforderlich. Wenn das RSA-Serverzertifikat nicht 2048 Bit oder mehr umfasst, wird das Telefon nicht beim Cisco Unified Communications Manager registriert und die Meldung `Telefon konnte nicht registriert werden erscheint. Die Größe des Zertifikatsschlüssels ist nicht FIPS-konform.` wird auf dem Telefon angezeigt.

Sie können im FIPS-Modus keine privaten Schlüssel (LSC oder MIC) verwenden.

Wenn das Telefon über ein vorhandenen LSC mit weniger als 2.048 Bits verfügt, müssen Sie die LSC-Schlüssellänge auf 2048 Bit oder mehr aktualisieren, bevor Sie FIPS aktivieren.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager
Einrichten eines LSC (Locally Significant Certificate), auf Seite 7

Sicherheitsverbesserungen für Ihr Telefonnetzwerk

Sie können Cisco Unified Communications Manager 11.5(1) und 12.0(1) ermöglichen, in einer Umgebung mit verbesserter Sicherheit zu arbeiten. Mit diesen Verbesserungen wird Ihr Telefonnetzwerk unter Anwendung einer Reihe von strengen Sicherheits- und Risikomanagementkontrollen betrieben, um Sie und die Benutzer zu schützen.

Cisco Unified Communications Manager 12.5 (1) unterstützt keine Umgebung mit verbesserter Sicherheit. Deaktivieren Sie FIPS, bevor Sie ein Upgrade auf Cisco Unified Communications Manager 12.5(1) vornehmen oder Ihr TFTP-Dienst wird nicht ordnungsgemäß funktionieren.

Die Umgebung mit verbesserter Sicherheit bietet die folgenden Funktionen:

- Kontaktsuchen-Authentifizierung
- TCP als Standardprotokoll für Remote-Audit-Protokolle
- FIPS-Modus
- Verbesserte Richtlinie für Anmeldeinformationen
- Unterstützung für die SHA-2-Hash-Familie für digitale Signaturen
- Unterstützung für eine RSA-Schlüsselgröße von 512 und 4096 Bits.

Mit Cisco Unified Communications Manager Version 14.0 und Cisco IP-Telefon-Firmware Version 14.0 und höher unterstützen die Telefone die SIP-OAuth-Authentifizierung.

OAuth wird für Proxy Trivial File Transfer Protocol (TFTP) mit Cisco Unified Communications ManagerVersion 14.0 (1) SU1 oder höher und Cisco IP-Telefon-Firmware Version 14.1 (1) unterstützt. Proxy-TFTP und OAuth für Proxy-TFTP werden für Mobile Remote Access (MRA) nicht unterstützt.

Weitere Informationen zur Sicherheit finden Sie unter:

- *Systemkonfigurationshandbuch für Cisco Unified Communications Manager*, Version 14.0(1) oder höher (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

- *Sicherheitsüberblick für die Cisco IP-Telefon 7800- und 8800-Serien*(https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html)
- *Sicherheitshandbuch für Cisco Unified Communications Manager*(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)
- SIP-OAuth: *Funktionskonfigurationshandbuch für Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

Hinweis Ihr Cisco IP-Telefon kann nur eine begrenzte Anzahl an Identity Trust List(ITL-)Dateien speichern. ITL-Dateien dürfen die Begrenzung von 64000 nicht überschreiten. Begrenzen Sie daher die Anzahl an Dateien, die Cisco Unified Communications Manager an das Telefon senden kann.

Die aktuellen Sicherheitsfunktionen auf dem Telefon anzeigen

Weitere Informationen zu den Sicherheitsfunktionen und zur Sicherheit von Cisco Unified Communications Manager und des Cisco IP-Telefon, finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Drücken Sie **Anwendungen** .

Schritt 2 Wählen Sie **Administratoreinstellungen** > **Sicherheitskonfiguration** aus.

Die meisten Sicherheitsfunktionen sind nur verfügbar, wenn eine Zertifikatvertrauensliste (CTL) auf dem Telefon installiert ist.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Sicherheitsprofile anzeigen

Alle Cisco IP-Telefons, die Cisco Unified Communications Manager unterstützen, verwenden ein Sicherheitsprofil, das definiert, ob das Telefon nicht geschützt, authentifiziert oder verschlüsselt ist. Weitere Informationen zum Konfigurieren des Sicherheitsprofils und das Übernehmen des Profils auf dem Telefon finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Wählen Sie in der Cisco Unified Communications Manager-Verwaltung **System** > **Sicherheit** > **Telefonsicherheitsprofil** aus.

Schritt 2 Überprüfen Sie die Einstellung „Sicherheitsmodus“.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Unterstützte Sicherheitsfunktionen

Die folgende Tabelle enthält eine Übersicht der Sicherheitsfunktionen, die von der Cisco IP Phone 7800-Serie unterstützt werden. Weitere Informationen zu diesen Funktionen und zur Sicherheit von Cisco Unified Communications Manager und des Cisco IP Phone finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Tabelle 1: Überblick der Sicherheitsfunktionen

Funktion	Beschreibung
Imageauthentifizierung	Signierte Binärdateien (mit der Erweiterung SBN) verhindern Manipulationen des Firmware-Images, bevor es auf ein Telefon geladen wird. Wenn das Image manipuliert wurde, kann das Telefon nicht authentifiziert werden und das Image wird abgelehnt.
Installation des Zertifikats am Kundenstandort	Jedes Cisco IP Phone erfordert ein eindeutiges Zertifikat für die Geräteauthentifizierung. Die Telefone enthalten ein MIC (Manufacturing Installed Certificate), aber für zusätzliche Sicherheit können Sie in Cisco Unified Communications Manager Administration angeben, dass ein Zertifikat über die CAPF (Certificate Authority Proxy Function) installiert werden muss. Sie können ein LSC (Locally Significant Certificate) auch über das Menü Sicherheitskonfiguration auf dem Telefon installieren.
Geräteauthentifizierung	Die Geräteauthentifizierung erfolgt zwischen dem Cisco Unified Communications Manager-Server und dem Telefon, wenn jede Entität das Zertifikat der anderen Entität akzeptiert. Bestimmt, ob eine sichere Verbindung zwischen dem Telefon und Cisco Unified Communications Manager hergestellt wird, und erstellt, falls erforderlich, mit dem TLS-Protokoll einen sicheren Signalpfad zwischen den Entitäten. Cisco Unified Communications Manager registriert Telefone nur, wenn diese von Cisco Unified Communications Manager authentifiziert werden können.

Funktion	Beschreibung
Dateiauthentifizierung	Überprüft digital signierte Dateien, die das Telefon herunterlädt. Das Telefon überprüft die Signatur, um sicherzustellen, dass die Datei, nachdem sie erstellt wurde, nicht manipuliert wurde. Dateien, die nicht authentifiziert werden können, werden nicht in den Flash-Speicher auf dem Telefon geschrieben. Das Telefon weist diese Dateien ohne weitere Verarbeitung zurück.
Signalisierungsauthentifizierung	Verwendet das TLS-Protokoll, um sicherzustellen, dass die Signalpakete während der Übermittlung nicht manipuliert wurden.
MIC (Manufacturing Installed Certificate)	Auf jedem Cisco IP-Telefon ist ein eindeutiges, vom Hersteller installiertes Zertifikat (Manufacturing Installed Certificate, MIC) vorhanden, das für die Geräteauthentifizierung verwendet wird. Das MIC ist ein permanenter Identitätsnachweis für das Telefon und ermöglicht Cisco Unified Communications Manager, das Telefon zu authentifizieren.
Sichere SRST-Referenz	Nachdem Sie eine SRST-Referenz für die Sicherheit konfiguriert und die abhängigen Geräte in der Cisco Unified Communications Manager-Verwaltung zurückgesetzt haben, fügt der TFTP-Server das SRST-Zertifikat zur Datei cnf.xml hinzu und sendet diese Datei an das Telefon. Ein sicheres Telefon verwendet eine TLS-Verbindung, um mit dem SRST-fähigen Router zu kommunizieren.
Medienverschlüsselung	Verwendet SRTP, um sicherzustellen, dass die Medienstreams zwischen den unterstützten Geräten sicher sind und die Daten nur von den vorgesehenen Geräten empfangen und gelesen werden können. Erstellt ein primäres Medien-Schlüsselpaar für die Geräte, verteilt die Schlüssel an die Geräte und schützt die Schlüssel, während diese übertragen werden.
CAPF (Certificate Authority Proxy Function)	Implementiert Teile des Prozesses für die Zertifikatsgenerierung, die für das Telefon zu verarbeitungsintensiv sind, und interagiert mit dem Telefon bei der Schlüsselgenerierung und Zertifikatsinstallation. CAPF kann konfiguriert werden, um Zertifikate im Auftrag des Telefons von kundenspezifischen Zertifizierungsstellen anzufordern oder Zertifikate lokal zu generieren.
Sicherheitsprofile	Definiert, ob das Telefon nicht sicher oder verschlüsselt ist.

Funktion	Beschreibung
Verschlüsselte Konfigurationsdateien	Ermöglicht Ihnen, den Datenschutz für Telefonkonfigurationsdateien sicherzustellen.
Die Webserverfunktionalität für ein Telefon deaktivieren	Sie können den Zugriff auf eine Telefon-Webseite verhindern, auf der verschiedene Statistiken für ein Telefon angezeigt werden.
Telefonhärtung	Weitere Sicherheitsoptionen, die in der Cisco Unified Communications Manager-Verwaltung festgelegt werden: • PC-Port deaktivieren • PC-Sprach-VLAN-Zugriff deaktivieren • Zugriff auf die Webseiten für ein Telefon deaktivieren **Hinweis** Sie können die aktuellen Einstellungen für die Optionen PC-Port deaktiviert, GARP aktiviert und Sprach-VLAN aktiviert im Menü Telefonkonfiguration anzeigen.
802.1X-Authentifizierung	Cisco IP-Telefon kann die 802.1X-Authentifizierung zur Anfrage und Ausführung des Netzwerkzugriffs verwenden.
AES 256-Verschlüsselung	Telefone, die mit Cisco Unified Communications Manager Version 10.5(2) oder höher verbunden sind, unterstützen die AES 256-Verschlüsselung für TLS und SIP für die Signalisierung und Medienverschlüsselung. Diese Telefone können TLS 1.2-Verbindungen mit AES-256-basierten Schlüsseln, die mit SHA-2 (Secure Hash Algorithm) und FIPS (Federal Information Processing Standards) konform sind, initiieren und unterstützen. Die neuen Schlüssel: • Für TLS-Verbindungen: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Für sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.

Funktion	Beschreibung
Elliptic Curve Digital Signature Algorithm (ECDSA)-Zertifikate	Als Teil der Common Criteria(CC-)Zertifizierung hat Cisco Unified Communications Manager ECDSA-Zertifikate in Version 11.0 hinzugefügt. Dies betrifft alle Voice Operating System-(VOS-)Produkte ab Version CUCM 11.5 und höher.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager
Anrufsicherheit, auf Seite 8
802.1x-Authentifizierung, auf Seite 11
Sicherheitsprofile anzeigen, auf Seite 3

Einrichten eines LSC (Locally Significant Certificate)

Diese Aufgabe bezieht sich auf das Einrichten eines LSC mit der Methode der Authentifizierungszeichenfolge.

Vorbereitungen

Stellen Sie sicher, dass die Sicherheitskonfiguration von Cisco Unified Communications Manager und CAPF (Certificate Authority Proxy Function) vollständig ist:

- Die CTL- oder ITL-Datei hat ein CAPF-Zertifikat.
- Überprüfen Sie in der Cisco Unified Communications Operating System-Verwaltung, ob das CAPF-Zertifikat installiert ist.
- CAPF wird ausgeführt und ist konfiguriert.

Weitere Informationen zu diesen Einstellungen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Prozedur

Schritt 1 Sie benötigen den CAPF-Authentifizierungscode, der während der Konfiguration von CAPF festgelegt wurde.

Schritt 2 Drücken Sie auf dem Telefon auf **Anwendungen** .

Schritt 3 Wählen Sie **Administratoreinstellungen** > **Sicherheits-Setup** aus.

Hinweis Sie können den Zugriff auf das Menü „Einstellungen“ mit dem Feld „Zugriff auf Einstellungen“ im Fenster „Telefonkonfiguration“ in der Cisco Unified Communications Manager-Verwaltung steuern.

Schritt 4 Wählen Sie **LSC** aus und drücken Sie **Auswählen** oder **Aktualisieren**.

Das Telefon fordert eine Authentifizierungszeichenfolge an.

Schritt 5 Geben Sie die Authentifizierungscode ein und drücken Sie **Senden**.

Das Telefon installiert, aktualisiert oder entfernt das LSC, abhängig davon, wie CAPF konfiguriert ist. Während des Verfahrens werden mehrere Meldungen im LSC-Optionsfeld im Menü Sicherheitskonfiguration angezeigt,

damit Sie den Status überwachen können. Wenn das Verfahren abgeschlossen ist, wird Installiert oder Nicht installiert auf dem Telefon angezeigt.

Der Prozess zum Installieren, Aktualisieren oder Entfernen des LSC kann längere Zeit dauern.

Wenn das Telefon erfolgreich installiert wurde, wird die Meldung `Installiert` angezeigt. Wenn das Telefon `Nicht installiert` anzeigt, ist möglicherweise die Autorisierungszeichenfolge ungültig oder das Telefon ist nicht für Updates aktiviert. Wenn der CAPF-Vorgang die LSC löscht, zeigt das Telefon `Nicht installiert` an. Der CAPF-Server protokolliert die Fehlermeldungen. Der Pfad zu den Protokollen und die Bedeutung der Fehlermeldungen werden in der CAPF-Serverdokumentation beschrieben.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Aktivieren des FIPS-Modus

Prozedur

Schritt 1	Wählen Sie in Cisco Unified Communications Manager Administration **Gerät** > **Telefon** aus, und navigieren Sie zum Telefon.
Schritt 2	Navigieren Sie zum produktspezifischen Konfigurationsbereich.
Schritt 3	Legen Sie das Feld **FIPS-Modus** auf „Aktiviert“ fest.
Schritt 4	Wählen Sie **Konfiguration übernehmen**.
Schritt 5	Wählen Sie **Speichern**.
Schritt 6	Starten Sie das Telefon neu.

Anrufsicherheit

Wenn die Sicherheit für ein Telefon implementiert wird, können sichere Anrufe auf dem Telefondisplay mit Symbolen gekennzeichnet werden. Sie können auch bestimmen, ob das verbundene Telefon sicher und geschützt ist, wenn zu Beginn des Anrufs ein Sicherheitssignal ausgegeben wird.

In einem sicheren Anruf sind alle Anrufsignale und Medienstreams verschlüsselt. Ein sicherer Anruf bietet eine hohe Sicherheitsstufe und stellt die Integrität und den Datenschutz des Anrufs sicher. Wenn ein aktiver Anruf verschlüsselt wird, ändert sich das Anrufstatus-Symbol rechts neben der Anrufdauer in das folgende Symbol:  .

Hinweis Wenn der Anruf über nicht-IP-Anrufabschnitte, beispielsweise ein Festnetz, geleitet wird, ist der Anruf möglicherweise nicht sicher, auch wenn er im IP-Netzwerk verschlüsselt wurde und ein Schloss-Symbol angezeigt wird.

Zu Beginn eines sicheren Anrufs wird ein Sicherheitssignal ausgegeben, das angibt, dass das andere verbundene Telefon ebenfalls sicheres Audio empfangen und senden kann. Wenn Sie mit einem nicht sicheren Telefon verbunden sind, wird kein Sicherheitssignal ausgegeben.

Hinweis Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Sichere Konferenzen, Cisco Extension Mobility und gemeinsam genutzte Leitungen können über eine sichere Konferenzbrücke konfiguriert werden.

Wenn ein Telefon in Cisco Unified Communications Manager als sicher (verschlüsselt und vertrauenswürdig) konfiguriert wird, kann es den Status „Geschützt“ erhalten. Anschließend kann das geschützte Telefon so konfiguriert werden, dass es zu Beginn eines Anrufs einen Signalton ausgibt.

- Geschütztes Gerät: Um den Status eines sicheren Telefons in „Geschützt“ zu ändern, aktivieren Sie das Kontrollkästchen „Geschütztes Gerät“ im Fenster „Telefonkonfiguration“ in Cisco Unified Communications Manager Administration (**Gerät** > **Telefon**).
- Sicherheitssignal ausgeben: Damit das geschützte Telefon ein Signal ausgibt, das angibt, ob der Anruf sicher oder nicht sicher ist, legen Sie die Einstellung Sicherheitssignal ausgeben auf True fest. Die Einstellung Sicherheitssignal ausgeben ist standardmäßig auf False festgelegt. Sie legen diese Option in der Cisco Unified Communications Manager-Verwaltung fest (**System** > **Serviceparameter**). Wählen Sie den Server und anschließend den Unified Communications Manager-Service aus. Wählen Sie im Fenster Serviceparameterkonfiguration die Option unter Funktion - Sicherheitssignal aus. Der Standardwert ist False.

Sichere Konferenzanruf-ID

Sie können einen sicheren Konferenzanruf initiieren und die Sicherheitsstufe der Teilnehmer überwachen. Ein sicherer Konferenzanruf wird mit diesem Prozess initiiert:

1. Ein Benutzer startet die Konferenz auf einem sicheren Telefon.
2. Cisco Unified Communications Manager weist dem Anruf eine sichere Konferenzbrücke zu.
3. Während Teilnehmer hinzugefügt werden, überprüft Cisco Unified Communications Manager den Sicherheitsmodus aller Telefone und hält die Sicherheitsstufe für die Konferenz aufrecht.
4. Das Telefon zeigt die Sicherheitsstufe des Konferenzanrufs an. Eine sichere Konferenz zeigt das Sicherheitssymbol rechts neben **Konferenz** auf dem Telefon an.

Hinweis Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Für geschützte Telefone sind einige Funktionen, beispielsweise Konferenzanrufe, gemeinsam genutzte Leitungen und die Anschlussmobilität, nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

Die folgende Tabelle enthält Informationen zu den Änderungen der Konferenzsicherheitsstufe, abhängig von der Sicherheitsstufe des Telefons des Initiators und der Verfügbarkeit von sicheren Konferenzbrücken.

Tabelle 2: Sicherheitseinschränkungen für Konferenzanrufe

Sicherheitsstufe des Telefons des Initiators	Verwendete Funktion	Sicherheitsstufe der Teilnehmer	Ergebnisse der Aktion
Nicht sicher	Konferenz	Sicher	Nicht sichere Konferenzbrücke Nicht sichere Konferenz
Sicher	Konferenz	Mindestens ein Mitglied ist nicht sicher.	Sichere Konferenzbrücke Nicht sichere Konferenz
Sicher	Konferenz	Sicher	Sichere Konferenzbrücke Verschlüsselungsstufe der sicheren Konferenz
Nicht sicher	MeetMe	Die minimale Sicherheitsstufe ist verschlüsselt.	Der Initiator erhält die Meldung `Sicherheitsstufe nicht erfüllt, Anruf abgelehnt.`
Sicher	MeetMe	Die minimale Sicherheitsstufe ist nicht sicher.	Sichere Konferenzbrücke Die Konferenz nimmt alle Anrufe an.

Sichere Anruf-ID

Ein sicherer Anruf wird initiiert, wenn Ihr Telefon und das Telefon des anderen Teilnehmers für sichere Anrufe konfiguriert ist. Das andere Telefon kann sich im gleichen Cisco IP-Netzwerk oder in einem Netzwerk außerhalb des IP-Netzwerks befinden. Sichere Anrufe sind nur zwischen zwei Telefonen möglich. Konferenzanrufe sollten sichere Anrufe unterstützen, nachdem eine sichere Konferenzbrücke konfiguriert wurde.

Ein sicherer Anruf wird mit diesem Prozess initiiert:

1. Der Benutzer initiiert einen Anruf auf einem geschützten Telefon (Sicherheitsmodus).
2. Das Telefon zeigt das Sicherheitssymbol auf dem Telefondisplay an. Dieses Symbol zeigt an, dass das Telefon für sichere Anrufe konfiguriert ist. Dies bedeutet jedoch nicht, dass das andere verbundene Telefon ebenfalls geschützt ist.
3. Der Benutzer hört einen Signalton, wenn der Anruf mit einem anderen sicheren Telefon verbunden wird, der angibt, dass beide Enden der Konversation verschlüsselt und geschützt sind. Wenn der Anruf mit einem nicht sicheren Telefon verbunden wird, hört der Benutzer keinen Signalton.

Hinweis Sichere Anrufe werden zwischen zwei Telefonen unterstützt. Für geschützte Telefone sind einige Funktionen, beispielsweise Konferenzanrufe, gemeinsam genutzte Leitungen und die Anschlussmobilität, nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

Ein Sicherheitssignal wird nur auf einem geschützten Telefon ausgegeben. Auf einem nicht geschützten Telefon wird kein Signalton ausgegeben. Wenn sich der Gesamtstatus des Anrufs während des Anrufs ändert, gibt das geschützte Telefon den geänderten Signalton wieder.

Geschützte Telefone spielen unter folgenden Umständen einen Signalton ab:

- Wenn die Option Sicherheitssignalton aktiviert ist:
  - Wenn auf beiden Seiten sichere Medien eingerichtet sind und der Anrufstatus „Sicher“ lautet, gibt das Telefon das Signal für eine sichere Verbindung wieder (drei lange Signaltöne mit Pausen).
  - Wenn auf beiden Seiten nicht sichere Medien eingerichtet sind und der Anrufstatus „Nicht sicher“ lautet, wird das Signal für eine nicht sichere Verbindung abgespielt (sechs kurze Signaltöne mit kurzen Pausen).

Wenn die Option Sicherheitssignalton wiedergeben deaktiviert ist, erklingt kein Signalton.

802.1x-Authentifizierung

Cisco IP-Telefons unterstützen die 802.1X-Authentifizierung.

Cisco IP-Telefons und Cisco Catalyst-Switches verwenden normalerweise CDP (Cisco Discovery Protocol), um sich gegenseitig zu identifizieren und Paramater zu bestimmen, beispielsweise die VLAN-Zuweisung und Inline-Energieanforderungen. 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. Die Telefone enthalten einen 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 Catalyst-Switch (oder Switch eines Drittanbieters): Der Switch muss 802.1X unterstützen, damit er als Authentifikator agieren und Meldungen zwischen dem Telefon und dem Authentifizierungsserver übermitteln kann. 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: Im 802.1X-Standard werden VLANs nicht berücksichtigt und daher wird empfohlen, dass nur ein einzelnes Gerät gegenüber einem bestimmten Switch-Port authentifiziert wird.

Einige Switches (einschließlich Cisco Catalyst-Switches) unterstützen jedoch die Authentifizierung in mehreren Domänen. Die Switch-Konfiguration bestimmt. ob Sie einen PC in einem PC-Port des Telefon anschließen können.

- Aktiviert: Wenn Sie einen Switch verwenden, der die Authentifizierung in mehreren Domänen unterstützt, können Sie den PC-Port aktivieren und einen PC daran anschließen. In diesem Fall unterstützen Cisco IP-Telefons Proxy-EAPOL-Logoff, um die Authentifizierung zwischen dem Switch und dem angeschlossenen PC zu überwachen. Weitere Informationen zur Unterstützung von IEEE 802.1X auf Cisco Catalyst-Switches finden Sie in den Konfigurationshandbüchern für die Cisco Catalyst-Switches:

  http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

- Deaktiviert: Wenn der Switch nicht mehrere 802.1X-kompatible Geräte am selben Port unterstützt, sollten Sie den PC-Port deaktivieren, wenn die 802.1X-Authentifizierung aktiviert wird. 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 in der 802.1X-Standardkonfiguration keine VLANs vorgesehen sind, sollten Sie diese Einstellung je nach 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 den Port dem systemeigenen VLAN zu.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager