Cisco IP-Konferenztelefon – Sicherheit

Übersicht der Sicherheit des Cisco IP Phone

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.

Das Cisco IP-Konferenztelefon 8832 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 in den Statusmeldungen des Telefons 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

Einrichten eines LSC (Locally Significant Certificate), auf Seite 5
Dokumentation Cisco Unified Communications Manager

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)

- *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.

Unterstützte Sicherheitsfunktionen

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.

Die Implementierung von Sicherheitsfunktionen in das Cisco Unified Communications Manager-System verhindert den Identitätsdiebstahl hinsichtlich Telefon und Cisco Unified Communications Manager-Server und schützt vor unbefugtem Zugriff auf Daten, Anrufsignale und Medien-Datenströme.

Zur Abwehr von Bedrohungen dieser Art erstellt das Cisco IP-Telefonienetzwerk zwischen Telefon und Server sichere (verschlüsselte) Kommunikationsdatenströme und erhält diese aufrecht, signiert Dateien digital, bevor diese auf ein Telefon übertragen werden, und verschlüsselt alle Mediendatenströme und Signale, die zwischen Cisco IP-Telefons übertragen werden.

Nachdem Sie die für die CAPF (Certificate Authority Proxy Function) erforderlichen Aufgaben ausgeführt haben, wird auf den Telefonen ein LSC (Locally Significant Certificate) installiert. Zum Konfigurieren eines LSC können Sie die Cisco Unified Communications Manager-Verwaltung verwenden. Die Vorgehensweise hierfür ist im Sicherheitshandbuch für Cisco Unified Communications Manager beschrieben. 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.

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

Im Telefonsicherheitsprofil ist definiert, ob das Gerät sicher oder nicht sicher ist. Weitere Informationen zum Anwenden des Sicherheitsprofils auf das Telefon finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Wenn Sie in der Cisco Unified Communications Manager-Verwaltung sicherheitsrelevante Einstellungen konfigurieren, sind in der Telefonkonfigurationsdatei auch vertrauliche Informationen enthalten. Damit die Konfigurationsdatei entsprechend ihrer Vertraulichkeit geschützt ist, müssen Sie die Datei so konfigurieren, dass eine Verschlüsselung erfolgt. Ausführliche Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.

Die Implementierung von Sicherheitsfunktionen in das Cisco Unified Communications Manager-System verhindert den Identitätsdiebstahl hinsichtlich Telefon und Cisco Unified Communications Manager-Server und schützt vor unbefugtem Zugriff auf Daten, Anrufsignale und Medien-Datenströme.

Die folgende Tabelle enthält eine Übersicht der Sicherheitsfunktionen, die von Cisco IP-Konferenztelefon 8832 unterstützt werden. Weitere Informationen zu diesen Funktionen und zur Sicherheit von Cisco Unified Communications Manager und Cisco IP-Telefon finden Sie in der Dokumentation zu Ihrer Version von Cisco Unified Communications Manager.

Tabelle 1: Überblick der Sicherheitsfunktionen

Funktion	Beschreibung
Imageauthentifizierung	Signierte Binärdateien (mit der Erweiterung SBN) verhindern Wenn das Image manipuliert wurde, kann das Telefon nicht au
Installation des Zertifikats am Kundenstandort	Für jedes Telefon ist zur Geräteauthentifizierung ein eindeutig Installed Certificate), aber für zusätzliche Sicherheit können S ein Zertifikat über die CAPF (Certificate Authority Proxy Functi auch über das Menü Sicherheitskonfiguration auf dem Telefon
Geräteauthentifizierung	Die Geräteauthentifizierung erfolgt zwischen dem Cisco Unifi Zertifikat der anderen Entität akzeptiert. Bestimmt, ob eine sic Manager hergestellt wird, und erstellt, falls erforderlich, mit d Unified Communications Manager registriert Telefone nur, we können.
Dateiauthentifizierung	Überprüft digital signierte Dateien, die das Telefon herunterlä nachdem sie erstellt wurde, nicht manipuliert wurde. Dateien, d dem Telefon geschrieben. Das Telefon weist diese Dateien ohr
Signalisierungsauthentifizierung	Verwendet das TLS-Protokoll, um sicherzustellen, dass die Sig
MIC (Manufacturing Installed Certificate)	Auf jedem Telefon ist ein eindeutiges, vom Hersteller installie die Geräteauthentifizierung verwendet wird. Das MIC ist ein p Communications Manager, das Telefon zu authentifizieren.
Sichere SRST-Referenz	Nachdem Sie eine SRST-Referenz für die Sicherheit konfiguri Manager-Verwaltung zurückgesetzt haben, fügt der TFTP-Serv Telefon. Ein sicheres Telefon verwendet eine TLS-Verbindung

Funktion	Beschreibung
Medienverschlüsselung	Verwendet SRTP, um sicherzustellen, dass die Medienstrea vorgesehenen Geräten empfangen und gelesen werden könn an die Geräte und schützt die Schlüssel, während diese übe
CAPF (Certificate Authority Proxy Function)	Implementiert Teile des Prozesses für die Zertifikatsgeneri Telefon bei der Schlüsselgenerierung und Zertifikatsinstalla kundenspezifischen Zertifizierungsstellen anzufordern ode
Sicherheitsprofile	Definiert, ob das Telefon nicht sicher, authentifiziert oder v
Verschlüsselte Konfigurationsdateien	Ermöglicht Ihnen, den Datenschutz für Telefonkonfiguratio
Die Webserverfunktionalität für ein Telefon deaktivieren	Sie können den Zugriff auf eine Telefon-Webseite verhinde
Telefonhärtung	Weitere Sicherheitsoptionen, die in der Cisco Unified Com • Zugriff auf die Webseiten für ein Telefon deaktivieren **Hinweis** Sie können die aktuellen Einstellungen für die Telefonkonfigurationsmenü anzeigen.
802.1X-Authentifizierung	Das Telefon kann die 802.1X-Authentifizierung verwende
AES 256-Verschlüsselung	Telefone, die mit Cisco Unified Communications Manager V für TLS und SIP für die Signalisierung und Medienverschl Schlüsseln, die mit SHA-2 (Secure Hash Algorithm) und F unterstützen. Die neuen Schlüssel: • Für TLS-Verbindungen: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • Für sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Weitere Informationen finden Sie in der Dokumentation zu
Elliptic Curve Digital Signature Algorithm (ECDSA)-Zertifikate	Als Teil der Common Criteria(CC-)Zertifizierung hat Cisco Dies betrifft alle VOS-Produkte (Voice Operating System)

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

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 Wählen Sie auf dem Telefon **Einstellungen** aus.

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** aus.
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 `Sicherheit nicht erfüllt, Anruf abgelehnt.`

Sicherheitsstufe des Telefons des Initiators	Verwendete Funktion	Sicherheitsstufe der Teilnehmer	Ergebnisse der Aktion
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.

Verschlüsselung für Aufschaltung bereitstellen

Cisco Unified Communications Manager überprüft den Sicherheitsstatus des Telefons, wenn Konferenzen erstellt werden, und ändert die Sicherheitsanzeige für die Konferenz oder blockiert die Durchführung des Anrufs, um Integrität und Sicherheit im System aufrechtzuerhalten.

Ein Benutzer kann sich nicht auf einen verschlüsselten Anruf aufschalten, wenn das für die Aufschaltung verwendete Telefon nicht für die Verschlüsselung konfiguriert ist. Wenn in einem solchen Fall die Aufschaltung fehlschlägt, wird auf dem Telefon, auf dem die Aufschaltung initiiert wurde, ein „Verbindung nicht möglich“-Ton (schneller Besetztton) ausgegeben.

Wenn das Telefon des Initiators für die Verschlüsselung konfiguriert ist, kann sich der Initiator der Aufschaltung über das verschlüsselte Telefon auf einen nicht sicheren Anruf aufschalten. Nach der Aufschaltung klassifiziert Cisco Unified Communications Manager den Anruf als nicht sicher.

Wenn das Telefon des Initiators für die Verschlüsselung konfiguriert ist, kann der Initiator der Aufschaltung sich auf einen verschlüsselten Anruf aufschalten. Auf dem Telefon wird dann angezeigt, dass der Anruf verschlüsselt ist.

WLAN-Sicherheit

Da alle WLAN-Geräte, die sich innerhalb der Reichweite befinden, den gesamten anderen WLAN-Datenverkehr empfangen können, ist die Sicherung der Sprachkommunikation in einem WLAN besonders wichtig. Um zu verhindern, dass der Sprachdatenverkehr von Angreifern manipuliert oder abgefangen wird, unterstützt die Cisco SAFE-Sicherheitsarchitektur das Cisco IP-Telefon und Cisco Aironet Access Points. Weitere Informationen zur Sicherheit in Netzwerken finden Sie unter http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

Die Cisco Wireless IP-Telefonielösung bietet Sicherheit für Wireless-Netzwerke, die nicht autorisierte Anmeldungen und kompromittierte Kommunikation mithilfe der folgenden, durch das Cisco Wireless IP-Telefon unterstützten Authentifizierungsmethoden verhindert:

- Offene Authentifizierung: In einem offenen System kann jedes kabellose Gerät die Authentifizierung anfordern. Der Access Point, der die Anforderung empfängt, kann die Authentifizierung entweder jedem Anforderer oder nur denjenigen Anforderern gewähren, die in einer Benutzerliste aufgeführt sind. Die Kommunikation zwischen dem kabellosen Gerät und dem Access Point kann entweder unverschlüsselt sein, oder die Geräte können zur Gewährleistung der Sicherheit WEP-Schlüssel (Wired Equivalent Privacy) verwenden. Geräte, die WEP verwenden, versuchen sich nur bei einem Access Point zu authentifizieren, der ebenfalls WEP verwendet.
- EAP-FAST-Authentifizierung (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling): Diese Client-Server-Sicherheitsarchitektur verschlüsselt EAP-Transaktionen innerhalb eines TLS-Tunnels (Transport Layer Security) zwischen dem Access Point und dem RADIUS-Server, z. B. dem Cisco ACS (Access Control Server).

  Der TLS-Tunnel verwendet PACs (Protected Access Credentials) für die Authentifizierung zwischen dem Client (Telefon) und dem RADIUS-Server. Der Server sendet eine Autoritäts-ID (Authority ID, AID) an den Client (Telefon), der wiederum die richtige PAC auswählt. Der Client (Telefon) gibt einen PAC-Opaque-Wert an den RADIUS-Server zurück. Der Server entschlüsselt die PAC mit dem primären Schlüssel. Beide Endpunkte verfügen nun über den PAC-Schlüssel, und ein TLS-Tunnel wird erstellt. EAP-FAST unterstützt die automatische PAC-Bereitstellung, muss jedoch auf dem RADIUS-Server aktiviert werden.

Hinweis Auf dem Cisco ACS läuft die PAC standardmäßig nach einer Woche ab. Wenn auf dem Telefon eine abgelaufene PAC vorhanden ist, dauert die Authentifizierung beim RADIUS-Server länger, da das Telefon eine neue PAC abrufen muss. Um Verzögerungen bei der PAC-Bereitstellung zu vermeiden, sollten Sie den Ablaufzeitraum für die PAC auf dem ACS oder RADIUS-Server auf mindestens 90 Tage festlegen.

- Extensible Authentication Protocol-Transport Layer Security-(EAP-TLS-)-Authentifizierung: EAP-TLS erfordert ein Client-Zertifikat für Authentifizierung und Netzwerkzugriff. Bei einem kabelgebundenen EAP-TLS kann es sich beim Client-Zertifikat entweder um das MIC oder das LSC des Telefons handeln. LSC ist das empfohlene Client-Authentifizierungszertifikat für kabelgebundenes EAP-TLS.
- PEAP (Protected Extensible Authentication Protocol): ein von Cisco entwickeltes, kennwortbasiertes Schema zur gegenseitigen Authentifizierung zwischen Client (Telefon) und RADIUS-Server. Das Cisco IP-Telefon kann PEAP für die Authentifizierung beim Wireless-Netzwerk verwenden. Es wird nur PEAP-MSCHAPV2 unterstützt. PEAP-GTC wird nicht unterstützt.

Folgende Authentifizierungsschemata verwenden den RADIUS-Server, um Authentifizierungsschlüssel zu verwalten:

- WPA/WPA2: Verwendet RADIUS-Serverinformationen, um eindeutige Authentifizierungsschlüssel zu generieren. Da diese Schlüssel auf dem zentralen RADIUS-Server generiert werden, bietet WPA/WPA2 eine höhere Sicherheit als die vorinstallierten WPA-Schlüssel, die am Access Point und auf dem Telefon gespeichert sind.
- Fast Secure Roaming: Verwendet RADIUS-Serverinformationen und WDS-Informationen (Wireless Domain Server), um Schlüssel zu verwalten und zu authentifizieren. Der WDS erstellt einen Cache mit Sicherheitsanmeldedaten für CCKM-fähige Client-Geräte, um eine schnelle und sichere erneute Authentifizierung zu gewährleisten. Die Cisco IP-Telefon 8800-Serie unterstützt 802.11r (FT). Sowohl 11r (FT) als auch CCKM werden unterstützt, um ein schnelles, sicheres Roaming zu ermöglichen. Jedoch Cisco empfiehlt dringend die 802.11r (links) über Air Methode nutzen.

Bei WPA/WPA2 und CCKM werden die Verschlüsselungsschlüssel nicht auf dem Telefon eingegeben, sondern zwischen dem Access Point und dem Telefon automatisch abgeleitet. Der EAP-Benutzername und das Kennwort, die zur Authentifizierung verwendet werden, müssen jedoch auf jedem Telefon eingegeben werden.

Um die Sicherheit des Sprachdatenverkehrs zu gewährleisten, unterstützt das Cisco IP-Telefon die Verschlüsselung mit WEP, TKIP und AES (Advanced Encryption Standard). Bei diesen Verschlüsselungsmechanismen werden sowohl die SIP-Signalpakete als auch die RTP-Pakete (Real-Time Transport Protocol) zwischen dem Access Point und dem Cisco IP-Telefon verschlüsselt.

WEP

Bei Verwendung von WEP in einem Wireless-Netzwerk erfolgt die Authentifizierung am Access Point mit offener Authentifizierung oder Authentifizierung über einen gemeinsamen Schlüssel. Der auf dem Telefon eingerichtete WEP-Schlüssel muss mit dem am Access Point konfigurierten WEP-Schlüssel übereinstimmen, um erfolgreiche Verbindungen zu ermöglichen. Das Cisco IP-Telefon unterstützt WEP-Schlüssel, die 40- oder 128-Bit-Verschlüsselung verwenden und auf dem Telefon und am Access Point statisch bleiben.

Bei der EAP- und der CCKM-Authentifizierung können zur Verschlüsselung WEP-Schlüssel verwendet werden. Der RADIUS-Server verwaltet den WEP-Schlüssel und übergibt nach der Authentifizierung einen eindeutigen Schlüssel zur Verschlüsselung aller Sprachpakete an den Access Point. Daher können sich diese WEP-Schlüssel mit jeder Authentifizierung ändern.

TKIP

WPA und CCKM verwenden die TKIP-Verschlüsselung. Dabei handelt es sich um eine Methode, die im Vergleich zu WEP mehrere Verbesserungen aufweist. TKIP ermöglicht die Verschlüsselung einzelner Paket und bietet längere Initialisierungsvektoren (IVs), um die Sicherheit der Verschlüsselung zu erhöhen. Darüber hinaus gewährleistet eine Nachrichtenintegritätsprüfung, dass die verschlüsselten Pakete nicht geändert werden. TKIP besitzt nicht die Vorhersehbarkeit von WEP, die es Angreifern ermöglicht, den WEP-Schlüssel zu entschlüsseln.

AES

Eine Verschlüsselungsmethode, die für die WPA2-Authentifizierung verwendet wird. Dieser nationale Verschlüsselungsstandard verwendet einen symmetrischen Algorithmus, bei dem die Schlüssel für Ver- und Entschlüsselung identisch sind. AES verwendet CBC-Verschlüsselung (Cipher Blocking Chain) mit einer Größe von 128 Bit, wodurch Schlüssellängen von mindestens 128 Bit, 192 Bit und 256 Bit unterstützt werden. Das Cisco IP-Telefon unterstützt eine Schlüssellänge von 256 Bit.

Hinweis Das Cisco IP-Telefon bietet keine Unterstützung für CKIP (Cisco Key Integrity Protocol) mit CMIC.

Authentifizierungs- und Verschlüsselungsschemata werden innerhalb des Wireless LAN eingerichtet. VLANs werden im Netzwerk und an den Access Points konfiguriert und geben verschiedene Kombinationen von Authentifizierung und Verschlüsselung an. Eine SSID wird einem VLAN und dem spezifischen Authentifizierungs- und Verschlüsselungsschema zugeordnet. Damit kabellose Client-Geräte erfolgreich authentifiziert werden können, müssen Sie an den Access Points und auf dem Cisco IP-Telefon die gleichen SSIDs mit ihren Authentifizierungs- und Verschlüsselungsschemata konfigurieren.

Einige Authentifizierungsschemata erfordern bestimmte Arten von Verschlüsselung. Mit der offenen Authentifizierung können Sie für zusätzliche Sicherheit die statische WEP-Verschlüsselung verwenden. Wenn Sie jedoch die Authentifizierung über einen gemeinsamen Schlüssel verwenden, müssen Sie statisches WEP als Verschlüsselung festlegen und einen WEP-Schlüssel auf dem Telefon konfigurieren.

Hinweis

- Wenn Sie WPA Pre-shared Key oder WPA2 Pre-shared Key verwenden, muss der vorinstallierte Schlüssel auf dem Telefon statisch festgelegt werden. Diese Schlüssel müssen mit den Schlüsseln am Access Point übereinstimmen.
- Das Cisco IP-Telefon unterstützt die automatische EAP-Aushandlung nicht. Wenn der EAP-FAST-Modus verwendet werden soll, müssen Sie diesen festlegen.

Die folgende Tabelle enthält eine Liste der Authentifizierungs- und Verschlüsselungsschemata, die auf den vom Cisco IP-Telefon unterstützten Cisco Aironet Access Points konfiguriert werden können. Die Tabelle zeigt die Netzwerkkonfigurationsoption für das Telefon, die der Konfiguration des Access Points entspricht.

Tabelle 3: Authentifizierungs- und Verschlüsselungsschemata

Konfiguration des Cisco IP-Telefon	Konfiguration des Access Points			
Sicherheitsmodus	Sicherheit	Schlüsselverwaltung	Verschlüsselung	Schnelles Roaming
Keine	Keine	Keine	Keine	–
WEP	Statisches WEP	Statisch	WEP	–
PSK	PSK	WPA	TKIP	Kein
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Weitere Informationen zum Konfigurieren von Authentifizierungs- und Verschlüsselungsschemata auf Access Points finden Sie im *Cisco Aironet Configuration Guide* (Konfigurationshandbuch für Cisco Aironet) zu Ihrem Modell und Ihrer Version unter folgender URL:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

Wireless LAN-Sicherheit

Cisco Telefone, die Wi-Fi unterstützen, besitzen mehr Sicherheitsanforderungen und benötigen eine zusätzliche Konfiguration. Diese zusätzlichen Schritte umfassen die Installation von Zertifikaten und die Einrichtung der Sicherheit auf den Telefonen und auf dem Cisco Unified Communications Manager.

Weitere Informationen finden Sie im *Sicherheitshandbuch für Cisco Unified Communications Manager*.

Verwaltungsseite für das Cisco IP-Telefon

Für Cisco Telefone, die Wi-Fi unterstützen, sind spezielle Webseiten verfügbar, die sich von den Webseiten für andere Telefone unterscheiden. Sie verwenden diese speziellen Webseiten für die Sicherheitskonfiguration der Telefone, wenn SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist. Auf diesen Webseiten können Sie Sicherheitszertifikate auf einem Telefon installieren, ein Sicherheitszertifikat herunterladen oder das Datum und die Uhrzeit des Telefons manuell konfigurieren.

Die Webseiten zeigen die gleichen Informationen wie die Webseiten für andere Telefone an, einschließlich die Geräteinformationen, Protokolle und Statistiken.

Konfigurieren der Verwaltungsseite für das Telefon

Die Verwaltungswebseite ist bei Auslieferung des Telefons aktiviert, und das Kennwort ist auf „Cisco“ festgelegt. Wenn ein Telefon jedoch beim Cisco Unified Communications Manager registriert wird, muss die Verwaltungswebseite aktiviert und ein neues Kennwort konfiguriert werden.

Aktivieren Sie diese Webseite, und legen Sie vor der erstmaligen Verwendung der Webseite, nachdem das Telefon registriert wurde, die Anmeldeinformationen fest.

Nach der Aktivierung können Sie über HTTPS-Port 8443 auf die Verwaltungswebseite zugreifen (**`https://x.x.x.x:8443`**, wobei x.x.x.x die IP-Adresse eines Telefons ist).

Vorbereitungen

Legen Sie vor der Aktivierung der Verwaltungswebseite ein Kennwort fest. Das Kennwort kann eine beliebige Kombination aus Buchstaben oder Ziffern sein, muss aber zwischen 8 und 127 Zeichen umfassen.

Ihr Benutzername ist dauerhaft auf „Admin“ festgelegt.

Prozedur

Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

Schritt 2 Navigieren Sie zu Ihrem Telefon.

Schritt 3 Legen Sie im Abschnitt **Produktspezifische Konfiguration** den Parameter **Webadministrator** auf **Aktiviert** fest.

Schritt 4 Geben Sie im Feld **Administrator-Kennwort** ein Kennwort ein.

Schritt 5 Wählen Sie **Speichern** aus, und klicken Sie auf **OK**.

Schritt 6 Wählen Sie **Konfiguration übernehmen** aus, und klicken Sie auf **OK**.

Schritt 7 Starten Sie das Telefon neu.

Auf die Administrations-Webseite des Telefons zugreifen

Wenn Sie auf die Verwaltungswebseiten zugreifen möchten, müssen Sie den Verwaltungsport angeben.

Prozedur

Schritt 1 Rufen Sie die IP-Adresse des Telefons ab:

- Wählen Sie in Cisco Unified Communications Manager Administration **Gerät** > **Telefon** aus, und navigieren Sie zum Telefon. Für Telefone, die sich beim Cisco Unified Communications Manager registrieren, wird die IP-Adresse im Fenster **Telefone suchen und auflisten** sowie oben im Fenster **Telefonkonfiguration** angezeigt.

Schritt 2 Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein, wobei *IP-Adresse* für die jeweilige IP-Adresse des Cisco IP-Telefon steht:

`https://<IP_address>:8443`

Schritt 3 Geben Sie im Feld „Kennwort“ das Kennwort ein.

Schritt 4 Klicken Sie auf **Senden**.

Installieren eines Benutzerzertifikats über die Webseite zur Telefonverwaltung

Sie können ein Benutzerzertifikat manuell auf dem Telefon installieren, wenn das SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist.

Das vom Hersteller installierte Zertifikat (MIC) kann als das Benutzerzertifikat für EAP-TLS verwendet werden.

Nachdem das Benutzerzertifikat installiert wurde, müssen Sie es der Vertrauensliste des RADIUS-Servers hinzufügen.

Vorbereitungen

Bevor Sie ein Benutzerzertifikat für ein Telefon installieren können, benötigen Sie Folgendes:

- Ein Benutzerzertifikat muss auf Ihrem PC gespeichert sein. Das Zertifikat muss im PKCS #12-Format vorliegen.
- Das genaue Kennwort des Zertifikats.

Prozedur

Schritt 1 Wählen Sie auf der Webseite für die Telefonverwaltung **Zertifikate** aus.

Schritt 2 Navigieren Sie zum Zertifikat auf Ihren PC.

Schritt 3 Geben Sie im Feld **Kennwort extrahieren** das Extraktionskennwort des Zertifikats an.

Schritt 4 Klicken Sie auf **Hochladen**.

Schritt 5 Starten Sie das Telefon neu, nachdem der Upload abgeschlossen ist.

Installieren eines Authentifizierungsserver-Zertifikats über die Webseite zur Telefonverwaltung

Sie können ein Authentifizierungsserver-Zertifikat manuell auf dem Telefon installieren, wenn das SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist.

Das CA-Stammzertifikat, über das das RADIUS-Serverzertifikat ausgestellt wurde, muss für EAP-TLS installiert sein.

Vorbereitungen

Bevor Sie ein Zertifikat auf einem Telefon installieren können, müssen Sie ein Authentifizierungsserver-Zertifikat auf Ihrem PC gespeichert haben. Das Zertifikat muss in PEM (Base-64) oder DER codiert sein.

Prozedur

Schritt 1 Wählen Sie auf der Webseite für die Telefonverwaltung **Zertifikate** aus.

Schritt 2 Navigieren Sie zum Feld **Authentifizierungsserver-Zertifikat (Administrator-Webseite)** und klicken Sie auf **Installieren**.

Schritt 3 Navigieren Sie zum Zertifikat auf Ihren PC.

Schritt 4 Klicken Sie auf **Hochladen**.

Schritt 5 Starten Sie das Telefon neu, nachdem der Upload abgeschlossen ist.

Wenn Sie mehr als ein Zertifikat installieren, installieren Sie alle Zertifikate vor dem Neustart des Telefons.

Manuelles Entfernen eines Sicherheitszertifikats von der Webseite zur Telefonverwaltung

Sie können ein Sicherheitszertifikat manuell von einem Telefon entfernen, wenn das SCEP (Simple Certificate Enrollment Protocol) nicht verfügbar ist.

Prozedur

Schritt 1 Wählen Sie auf der Webseite für die Telefonverwaltung **Zertifikate** aus.

Schritt 2 Navigieren Sie auf der Seite **Zertifikate** zum Zertifikat.

Schritt 3 Klicken Sie auf **Löschen**.

Schritt 4 Starten Sie das Telefon nach Abschluss des Löschvorgangs neu.

Manuelles Festlegen des Datums und der Uhrzeit des Telefons

Bei einer auf Zertifikaten basierenden Authentifizierung müssen auf dem Telefon das richtige Datum und die richtige Uhrzeit angezeigt werden. Ein Authentifizierungsserver vergleicht das Datum und die Uhrzeit des Telefons mit dem Ablaufdatum des Zertifikats. Wenn Datum und Uhrzeit auf dem Telefon und dem Server nicht übereinstimmen, funktioniert das Telefon nicht mehr.

Verwenden Sie dieses Verfahren, um das Datum und die Uhrzeit auf dem Telefon manuell einzustellen, wenn das Telefon die richtige Informationen nicht über das Netzwerk abrufen kann.

Prozedur

Schritt 1 Führen Sie auf der Webseite zu Telefonverwaltung einen Bildlauf zu **Datum und Uhrzeit** durch.

Schritt 2 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Telefon auf lokales Datum und lokale Zeit festlegen**, um das Telefon mit einem lokalen Server zu synchronisieren.
- Wählen Sie im Feld **Datum und Uhrzeit angeben** in den Menüs den Monat, den Tag, das Jahr, die Stunde, die Minute und die Sekunde aus, und klicken Sie auf **Telefon auf bestimmtes Datum und bestimmte Zeit festlegen**.

SCEP-Konfiguration

SCEP (Simple Certificate Enrollment Protocol) ist der Standard für die automatische Bereitstellung und Erneuerung von Zertifikaten. Mit SCEP müssen Zertifikate nicht manuell auf Ihrem Telefon installiert werden.

Konfigurieren der produktspezifischen SCEP-Konfigurationsparameter

Sie müssen die folgenden SCEP-Parameter auf der Telefon-Webseite konfigurieren.

- RA-IP-Adresse
- SHA-1- oder SHA-256-Fingerabdruck des CA-Stammzertifikats für den SCEP-Server

Die Cisco IOS-Registrierungsstelle (RA) dient als Proxy für den SCEP-Server. Der SCEP-Client auf dem Telefon verwendet die Parameter, die von Cisco Unified Communication Manager heruntergeladen werden. Nachdem Sie die Parameter konfiguriert haben, sendet das Telefon eine `SCEP getcs`-Anforderung an die RA, und das CA-Stammzertifikat wird mithilfe des definierten Fingerabdrucks validiert.

Prozedur

Schritt 1 Wählen Sie **Gerät** > **Telefon** in der Cisco Unified Communications Manager-Verwaltung aus.

Schritt 2 Suchen Sie das Telefon.

Schritt 3 Navigieren Sie zum Bereich **Produktspezifische Konfiguration – Layout**.

Schritt 4 Aktivieren Sie das Kontrollkästchen **WLAN SCEP-Server**, um den SCEP-Parameter zu aktivieren.

Schritt 5 Aktivieren Sie das Kontrollkästchen **WLAN-Stammzertifizierungsstellen-Fingerabdruck (SHA256 oder SHA1)**, um den SCEP-QED-Parameter zu aktivieren.

SCEP-Serverunterstützung

Wenn Sie einen SCEP-Server (Simple Certificate Enrollment Protocol) verwenden, kann der Server die Benutzer- und Server-Zertifikate automatisch beibehalten. Konfigurieren Sie auf dem SCEP-Server den SCEP-Registrierungs-Agent (RA) so, dass:

- er als vertrauenswürdiger PKI-Punkt fungiert.
- er als PKI-RA fungiert.
- die Geräteauthentifizierung mit einem RADIUS-Server durchgeführt wird.

Weitere Informationen finden Sie in der Dokumentation zum SCEP-Server.

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.

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.
- 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

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.