



Sicherheit von Cisco IP-Telefonen

- [Sicherheitsverbesserungen für Ihr Telefonnetzwerk, auf Seite 1](#)
- [Unterstützte Sicherheitsfunktionen, auf Seite 2](#)

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 Manager Version 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>)

**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 Cisco IP-Telefon 8800-Serie entspricht dem FIPS (Federal Information Processing Standard). Um ordnungsgemäß zu funktionieren, ist für den FIPS-Modus eine Schlüssellänge von 2048 Bit oder mehr erforderlich. Wenn das Zertifikat 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.

Wenn das Telefon über ein LSC verfügt, müssen Sie die LSC-Schlüssellänge auf 2048 Bit oder mehr aktualisieren, bevor Sie FIPS aktivieren.

Die folgende Tabelle enthält eine Übersicht der von den Telefonen unterstützten Sicherheitsfunktionen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.


Um die aktuellen Sicherheitseinstellungen auf einem Telefon anzuzeigen, einschließlich Sicherheitsmodus, Vertrauensliste und 802.1X-Authentifizierung, drücken Sie auf **Anwendungen**  und wählen **Verwaltereinstellungen > Sicherheits-Setup**.

Tabelle 1: Überblick der Sicherheitsfunktionen

Funktion	Beschreibung
Imageauthentifizierung	<p>Signierte Binärdateien (mit Dateierweiterung „.sbn“) verhindern das Manipulieren des Firmware-Images vor dem Laden auf das Telefon.</p> <p>Wenn das Image manipuliert wurde, kann das Telefon nicht authentifiziert werden und das Image wird abgelehnt.</p>
Image-Verschlüsselung	<p>Verschlüsselte Binärdateien (mit Dateierweiterung „.sebn“) verhindern das Manipulieren des Firmware-Images vor dem Laden auf das Telefon.</p> <p>Wenn das Image manipuliert wurde, kann das Telefon nicht authentifiziert werden und das Image wird abgelehnt.</p>
Kundenseitiges Installieren von Zertifikaten	<p>Jedes Cisco IP Phone erfordert ein eindeutiges Zertifikat für die Geräteauthentifizierung. Auf den Telefonen ist bereits ein vom Hersteller installiertes Zertifikat (MIC) vorhanden, zusätzliche Sicherheit bietet jedoch die Möglichkeit, die Zertifikatinstallation in der Cisco Unified Communications Manager-Verwaltung mithilfe von CAPF (Certificate Authority Proxy Function) festzulegen. Sie können ein LSC (Locally Significant Certificate) auch über das Menü Sicherheitskonfiguration auf dem Telefon installieren.</p>

Funktion	Beschreibung
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. Der Cisco Unified Communications Manager registriert Telefone nur dann, wenn sie authentifiziert werden können.
Dateiauthentifizierung	Überprüft digital signierte Dateien, die das Telefon herunterlädt. Das Telefon validiert die Signatur, um sicherzustellen, dass die Datei nach der Erstellung 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.
Dateiverschlüsselung	Durch Verschlüsselung wird verhindert, dass bei der Übertragung einer Datei auf das Telefon vertrauliche Informationen preisgegeben werden. Außerdem validiert das Telefon die Signatur, um sicherzustellen, dass die Datei nach der Erstellung 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.
Signalauthentifizierung	Bei dieser Authentifizierung wird anhand des TLS-Protokolls überprüft, dass die Signalkomponenten während der Übertragung 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 dient für das Telefon dauerhaft als eindeutiger Identitätsnachweis und ermöglicht dem Cisco Unified Communications Manager das Authentifizieren des Telefons.
Medienverschlüsselung	Diese stellt mithilfe von SRTP sicher, dass Mediendatenströme zwischen unterstützten Geräten geschützt sind und nur der beabsichtigte Empfänger die Daten erhalten und lesen kann. 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.
Sicherheitsprofil	Definiert, ob das Telefon nicht sicher, authentifiziert, verschlüsselt oder geschützt ist. Die weiteren Einträge in dieser Tabelle erläutern Sicherheitsfunktionen.
Verschlüsselte Konfigurationsdateien	Ermöglicht Ihnen, den Datenschutz für Telefonkonfigurationsdateien sicherzustellen.
Optionale Webserver-Deaktivierung für Telefone	Aus Sicherheitsgründen können Sie für ein Telefon den Zugriff auf die Webseiten (diese zeigen verschiedenste Betriebsstatistiken des Telefons an) und das Selbsthilfe-Portal verhindern.

Funktion	Beschreibung
Telefonhärtung	<p>Weitere Sicherheitsoptionen, die in der Cisco Unified Communications Manager-Verwaltung festgelegt werden:</p> <ul style="list-style-type: none"> • Deaktivierung des PC-Ports • Deaktivierung von Gratuitous ARP-Paketen • Deaktivierung des PC-Sprach-VLAN-Zugriffs • Deaktivierung des Zugriff auf die Einstellungs-menüs oder Beschränkung des Zugriffs auf ausschließlich das Voreinstellungs-menü und die Speichermöglichkeit für Lautstärkeänderungen • Deaktivierung des Zugriffs des Telefons auf Webseiten • Deaktivierung des Bluetooth-Zubehör-Ports • Einschränkung der TLS-Schlüssel
802.1X-Authentifizierung	<p>Cisco IP-Telefon kann die 802.1X-Authentifizierung zur Anfrage und Ausführung des Netzwerkzugriffs verwenden. Weitere Informationen finden Sie unter 802.1X-Authentifizierung, auf Seite 28.</p>
Sicheres SIP-Failover für SRST	<p>Nachdem Sie eine SRST-Sicherheitsreferenz konfiguriert und anschließend die abhängigen Geräte in der Cisco Unified Communications Manager-Verwaltung zurückgesetzt haben, fügt der TFTP-Server das Zertifikat des SRST-fähigen Gateways zur Datei „cnf.xml“ hinzu und sendet diese an das Telefon. Ein sicheres Telefon verwendet eine TLS-Verbindung, um mit dem SRST-fähigen Router zu kommunizieren.</p>
Verschlüsselung des Signalisierungsverkehrs	<p>Durch diese Verschlüsselung wird gewährleistet, dass alle zwischen dem Gerät und dem Cisco Unified Communications Manager-Server ausgetauschten SIP-Signalisierungsnachrichten verschlüsselt werden.</p>
Warnung bei Aktualisierung der Vertrauensliste	<p>Wenn die auf dem Telefon vorhandene Vertrauensliste aktualisiert wird, erhält der Cisco Unified Communications Manager eine Warnmeldung, die angibt, ob die Aktualisierung erfolgreich war oder nicht. Weitere Informationen finden Sie in der nachstehenden Tabelle.</p>
AES 256-Verschlüsselung	<p>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 Schlüssel enthalten:</p> <ul style="list-style-type: none"> • Für TLS-Verbindungen: <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Für sRTP: <ul style="list-style-type: none"> • AEAD_AES_256_GCM • AEAD_AES_128_GCM <p>Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.</p>

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.

In der folgenden Tabelle sind die bei Aktualisierung der Vertrauensliste ausgegebenen Warnmeldungen sowie deren Bedeutung aufgeführt. Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.

Tabelle 2: Warnmeldungen bei Aktualisierung der Vertrauensliste

Code und Meldung	Beschreibung
1 – TL_SUCCESS	Neue CTL bzw. ITL erhalten
2 – CTL_INITIAL_SUCCESS	Neue CTL erhalten, keine TL vorhanden
3 – ITL_INITIAL_SUCCESS	Neue ITL erhalten, keine TL vorhanden
4 – TL_INITIAL_SUCCESS	Neue CTL und ITL erhalten, keine TL vorhanden
5 – TL_FAILED_OLD_CTL	Aktualisierung auf neue CTL fehlgeschlagen, aber vorherige TL vorhanden
6 – TL_FAILED_NO_TL	Aktualisierung auf neue TL fehlgeschlagen, und keine frühere TL vorhanden
7 – TL_FAILED	Allgemeiner Fehler
8 – TL_FAILED_OLD_ITL	Aktualisierung auf neue ITL fehlgeschlagen, aber vorherige TL vorhanden
9 – TL_FAILED_OLD_TL	Aktualisierung auf neue TL fehlgeschlagen, aber vorherige TL vorhanden

Im Menü „Sicherheits-Setup“ sind Informationen zu verschiedenen Sicherheitseinstellungen verfügbar. Von dort aus kann auch auf das Menü „Vertrauensliste“ zugegriffen werden, und es ist angegeben, ob die CTL- bzw. ITL-Datei auf dem Telefon installiert ist.

In der folgenden Tabelle sind die im Menü „Sicherheits-Setup“ verfügbaren Optionen aufgeführt.

Tabelle 3: Menü „Sicherheits-Setup“

Option	Beschreibung	Änderung
Sicherheitsmodus	Zeigt den für das Telefon konfigurierten Sicherheitsmodus an.	Wählen Sie in der Cisco Unified Communications Manager-Verwaltung Gerät > Telefon . Die Einstellung wird im Bereich „Protokollspezifische Informationen“ des Fensters zur Telefonkonfiguration angezeigt.

Option	Beschreibung	Änderung
LSC	Gibt an, ob auf dem Telefon ein für Sicherheitseinstellungen genutztes LSC (Locally Significant Certificate) installiert ist („Ja“) oder nicht („Nein“).	Informationen zum Verwalten des LSCs für das Telefon finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
Vertrauensliste	<p>Das Menü „Vertrauensliste“ beinhaltet Untermenüs für die CTL, die ITL und für signierte Konfigurationsdateien.</p> <p>Im Untermenü „CTL-Datei“ wird der Inhalt der CTL-Datei angezeigt. Im Untermenü „ITL-Datei“ wird der Inhalt der ITL-Datei angezeigt.</p> <p>Außerdem werden im Menü „Vertrauensliste“ folgende Informationen angezeigt:</p> <ul style="list-style-type: none"> • CTL-Signatur: der SHA-1-Hash-Wert der CTL-Datei • Unified CM-/TFTP-Server: der Namen des Cisco Unified Communications Manager- und TFTP-Servers, der vom Telefon verwendet wird. Wenn für diesen Server ein Zertifikat installiert ist, wird ein Zertifikatssymbol angezeigt. • CAPF-Server: der Name des CAPF-Servers, den das Telefon verwendet. Wenn für diesen Server ein Zertifikat installiert ist, wird ein Zertifikatssymbol angezeigt. • SRST-Router: die IP-Adresse des vertrauenswürdigen SRST-Routers, den das Telefon verwenden kann. Wenn für diesen Server ein Zertifikat installiert ist, wird ein Zertifikatssymbol angezeigt. 	Weitere Informationen hierzu finden Sie unter Einrichten eines LSC (Locally Significant Certificate) , auf Seite 7.
802.1X-Authentifizierung	Hier kann die 802.1X-Authentifizierung für das Telefon aktiviert werden.	Siehe 802.1X-Authentifizierung , auf Seite 28.

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 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.

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 nur auf Verbindungen zwischen zwei Telefonen unterstützt. Einige Funktionen, beispielsweise Konferenzerufe und gemeinsam genutzte Leitungen, sind nicht verfügbar, wenn sichere Anrufe konfiguriert sind.

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 4: 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 <code>Sicherheit nicht erfüllt</code> , 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.

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. Als Authentifizierungsmethoden werden sowohl PEAP-MSCHAPV2 als auch PEAP-GTC 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-Signalkpakete 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 5: Authentifizierungs- und Verschlüsselungsschemata

Konfiguration des Cisco IP-Telefon	Konfiguration des Access Points			
	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

Konfiguration des Cisco IP-Telefon	Konfiguration des Access Points			
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
PEAP-GTC	PEAP-GTC	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>

Authentifizierung einrichten

Führen Sie die folgenden Schritte aus, um den Authentifizierungsmodus für dieses Profil auszuwählen:

Prozedur

Schritt 1 Wählen Sie das zu konfigurierende Netzwerkprofil.

Schritt 2 Wählen Sie den Authentifizierungsmodus.

Hinweis Je nach Auswahl müssen Sie für die Wireless-Sicherheit oder die Wireless-Verschlüsselung zusätzliche Optionen konfigurieren. Weitere Informationen finden Sie unter [WLAN-Sicherheit, auf Seite 12](#).

Schritt 3 Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.

Wireless-Sicherheit-Anmeldeinformationen

Wenn in Ihrem Netzwerk EAP-FAST und PEAP für die Benutzerauthentifizierung verwendet werden, müssen Sie ggf. sowohl den Benutzernamen als auch das Kennwort auf dem Remote Authentication Dial-In User Service (RADIUS) und auf dem Telefon konfigurieren.



Hinweis Wenn im Netzwerk Domänen genutzt werden, müssen Sie den Benutzernamen mit dem Domänennamen im Format *Domäne\Benutzername* eingeben.

Die folgenden Aktionen können dazu führen, dass das vorhandene Wi-Fi-Kennwort gelöscht wird:

- Eingeben einer ungültigen Benutzer-ID oder einem ungültigen Kennwort
- Installieren einer ungültigen oder abgelaufenen Stammzertifizierungsstelle, wenn der EAP-Typ auf PEAP-MSCHAPV2 oder PEAP-GTC festgelegt ist
- Deaktivieren des EAP-Typs auf dem RADIUS-Server, der vom Telefon verwendet wird, bevor ein Telefon auf den neuen EAP-Typ geändert wurde

Um EAP-Typen zu ändern, führen Sie in der angegebenen Reihenfolge folgende Schritte durch:

- Aktivieren Sie die neuen EAP-Typen auf dem RADIUS-Server.
- Ändern Sie den EAP-Typ auf einem Telefon in den neuen EAP-Typ.

Behalten Sie die aktuelle EAP-Typ-Konfiguration auf dem Telefon, bis der neue EAP-Typ auf dem RADIUS-Server aktiviert ist. Nachdem der neue EAP-Typ auf dem RADIUS-Server aktiviert ist, können Sie den EAP-Typ des Telefons ändern. Sobald alle Telefone in den neuen EAP-Typ geändert wurden, können Sie den vorherigen EAP-Typ ggf. deaktivieren.

Benutzername und Kennwort einrichten

Bei der Eingabe bzw. Änderung des Benutzernamens oder des Kennworts für das Netzwerkprofil müssen Sie denselben Benutzernamen und dieselbe Kennwortzeichenfolge eingeben, die auf dem RADIUS-Server konfiguriert sind. Die maximale Länge des Benutzernamens bzw. des Kennworts beträgt 64 Zeichen.

Führen Sie die folgenden Schritte aus, um den Benutzernamen und das Kennwort in den Wireless-Sicherheit-Anmeldeinformationen einzurichten:

Prozedur

-
- Schritt 1** Wählen Sie das Netzwerkprofil aus.
 - Schritt 2** Geben Sie im Feld „Benutzername“ den Netzwerkbenutzernamen für dieses Profil ein.
 - Schritt 3** Geben Sie im Feld „Kennwort“ die Zeichenfolge für das Netzwerkkenwort für dieses Profil ein.
 - Schritt 4** Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.
-

Pre-shared Key – Setup

Verwenden Sie die folgenden Abschnitte, um Anweisungen zum Einrichten der vorinstallierten Schlüssel zu erhalten.

Formate für Pre-shared Keys

Das Cisco IP-Telefon unterstützt das ASCII-Format und das Hexadezimalformat. Beim Einrichten eines WPA Pre-shared Keys müssen Sie eines dieser Formate verwenden:

Hexadezimal

Geben Sie für Hexadezimalschlüssel 64 Hexadezimalziffern (0–9 und A–F) ein; beispielsweise AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C.

ASCII

Geben Sie für ASCII-Schlüssel eine Zeichenfolge ein, in der die Ziffern 0–9, die Buchstaben A–Z (Groß- und Kleinbuchstaben) sowie Symbole enthalten sein können, wobei die Länge zwischen 8 und 63 Zeichen betragen muss; beispielsweise GREG12356789ZXYW.

PSK einrichten

Führen Sie die folgenden Schritte aus, um ein PSK im Bereich für Wireless-Anmeldedaten einzurichten:

Prozedur

-
- | | |
|------------------|---|
| Schritt 1 | Wählen Sie das Netzwerkprofil aus, das den WPA Pre-shared Key oder den WPA2 Pre-shared Key aktiviert. |
| Schritt 2 | Geben Sie im Bereich "Schlüsseltyp" den entsprechenden Schlüssel ein. |
| Schritt 3 | Geben Sie im Feld „Passphrase“ bzw. „Pre-shared Key“ eine ASCII-Zeichenfolge bzw. Hexadezimalziffern ein. |
| Schritt 4 | Klicken Sie auf Speichern , um die Änderung zu übernehmen. |
-

Wireless-Verschlüsselung

Wenn in Ihrem Wireless-Netzwerk WEP-Verschlüsselung verwendet wird und Sie den Authentifizierungsmodus auf Offen + WEP festlegen, müssen Sie einen WEP-Schlüssel im ASCII- oder Hexadezimalformat eingeben.

Die WEP-Schlüssel für das Telefon müssen mit den WEP-Schlüsseln übereinstimmen, die dem Access Point zugewiesen sind. Das Cisco IP-Telefon und die Cisco Aironet Access Points unterstützen sowohl 40-Bit- als auch 128-Bit-Verschlüsselungsschlüssel.

WEP-Schlüsselformate

Beim Einrichten eines WEP-Schlüssels müssen Sie eines dieser Formate verwenden:

Hexadezimal

Verwenden Sie für Hexadezimalschlüssel eine der folgenden Schlüssellängen:

40 Bit

Sie geben eine zehnstellige Zeichenfolge für den Verschlüsselungsschlüssel ein, der aus Hexadezimalzeichen (0–9 und A–F) besteht, beispielsweise ABCD123456.

128 Bit

Sie geben eine 26-stellige Zeichenfolge für den Verschlüsselungsschlüssel ein, der aus Hexadezimalzeichen (0–9 und A–F) besteht, beispielsweise AB123456789CD01234567890EF.

ASCII

Geben Sie für ASCII-Schlüssel eine Zeichenfolge ein, in der die Ziffern 0–9, die Buchstaben A–Z (Groß- und Kleinbuchstaben) sowie alle Symbole enthalten sein können; die Schlüsselzeichenfolge muss eine der folgenden Längen aufweisen:

40 Bit

Sie geben eine fünfstellige Zeichenfolge ein, beispielsweise GREG5.

128 Bit

Sie geben eine 13-stellige Zeichenfolge ein, beispielsweise GREGSSECRET13.

WEP-Schlüssel einrichten

Führen Sie die folgenden Schritte aus, um WEP-Schlüssel einzurichten.

Prozedur

-
- Schritt 1** Wählen Sie das Netzwerkprofil aus, das Offen + WEP oder Gemeinsam genutzt + WEP verwendet.
- Schritt 2** Geben Sie im Bereich "Schlüsseltyp" den entsprechenden Schlüssel ein.
- Schritt 3** Wählen Sie im Bereich für die Schlüssellänge eine der folgenden Zeichenfolgelängen aus:
- 40
 - 128
- Schritt 4** Geben Sie im Feld „Verschlüsselungsschlüssel“ die entsprechende Zeichenfolge basierend auf dem ausgewählten Schlüsseltyp und der ausgewählten Schlüssellänge ein. Siehe [WEP-Schlüsselformate](#), auf Seite 17.
- Schritt 5** Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.
-

CA-Zertifikat von ACS mithilfe der Microsoft-Zertifikatdienste exportieren

Exportieren Sie das Stammzertifikat der Zertifizierungsstelle aus dem ACS-Server. Weitere Informationen hierzu finden Sie in der Dokumentation zur Zertifizierungsstelle oder zu RADIUS.

Vom Hersteller installiertes Zertifikat

Im Telefon wurde durch Cisco werksseitig ein MIC (Manufacturing Installed Certificate, vom Hersteller installiertes Zertifikat) integriert.

Während der EAP-TLS-Authentifizierung muss der ACS-Server die Vertrauenswürdigkeit des Telefons überprüfen, während das Telefon die Vertrauenswürdigkeit des ACS-Servers prüfen muss.

Zum Überprüfen des MIC müssen das Manufacturing Root Certificate (Herstellerstammzertifikat) und Manufacturing Certificate Authority Certificate (Hersteller-CA-Zertifikat) von einem Cisco IP-Telefon exportiert und auf dem Cisco ACS-Server installiert werden. Diese beiden Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, anhand der das MIC vom Cisco ACS-Server überprüft wird.

Zum Überprüfen des Cisco ACS-Zertifikats müssen ein vertrauenswürdiges untergeordnetes Zertifikat (sofern vorhanden) sowie ein Stammzertifikat (erstellt von einer Zertifizierungsstelle) auf dem Cisco ACS-Server exportiert und auf dem Telefon installiert werden. Diese Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, anhand derer die Vertrauenswürdigkeit des Zertifikats vom ACS-Server überprüft wird.

Vom Benutzer installiertes Zertifikat

Zur Verwendung eines vom Benutzer installierten Zertifikats wird eine Anforderung zum Signieren des Zertifikats (Certificate Signing Request, CSR) generiert und zur Genehmigung an die Zertifizierungsstelle (Certificate Authority, CA) gesendet. Ein Benutzerzertifikat kann auch von der Zertifizierungsstelle ohne eine CSR generiert werden.

Im Rahmen der EAP-TLS-Authentifizierung überprüft der ACS-Server die Vertrauenswürdigkeit des Telefons, und das Telefon überprüft die Vertrauenswürdigkeit des ACS-Servers.

Zur Überprüfung der Authentizität des vom Benutzer installierten Zertifikats müssen Sie ein vertrauenswürdigen untergeordnetes Zertifikat (falls vorhanden) und ein Stammzertifikat der Zertifizierungsstelle installieren, durch die das Benutzerzertifikat auf dem Cisco ACS-Server genehmigt wurde. Diese Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, die zur Überprüfung der Vertrauenswürdigkeit des vom Benutzer installierten Zertifikats verwendet wird.

Zur Überprüfung des Cisco ACS-Zertifikats exportieren Sie ein vertrauenswürdigen untergeordnetes Zertifikat (falls vorhanden) und das Stammzertifikat (von einer Zertifizierungsstelle) auf dem Cisco ACS-Server. Die exportierten Zertifikate werden auf dem Telefon installiert. Diese Zertifikate sind Teil der vertrauenswürdigen Zertifikatskette, anhand derer die Vertrauenswürdigkeit des Zertifikats vom ACS-Server überprüft wird.

EAP-TLS-Authentifizierungszertifikate installieren

Führen Sie zum Installieren von Authentifizierungszertifikaten für EAP-TLS die folgenden Schritte aus.

Prozedur

Schritt 1 Legen Sie auf der Telefon-Webseite Datum und Uhrzeit des Cisco Unified Communications Manager für das Telefon fest.

Schritt 2 Wenn Sie das MIC (Manufacturing Installed Certificate, vom Hersteller installiertes Zertifikat) verwenden:

- Exportieren Sie das CA-Stammzertifikat und das Hersteller-CA-Zertifikat von der Telefon-Webseite.
- Installieren Sie in Internet Explorer Zertifikate auf dem Cisco ACS-Server, und bearbeiten Sie die Vertrauensliste.
- Importieren Sie das CA-Stammzertifikat in das Telefon.

Weitere Informationen finden Sie hier:

- [Zertifikate im ACS exportieren und installieren, auf Seite 20](#)
- [CA-Zertifikat von ISE mithilfe der Microsoft-Zertifikatdienste exportieren, auf Seite 21](#)

Schritt 3 Richten Sie mit dem ACS-Konfigurationstool das Benutzerkonto ein.

Weitere Informationen finden Sie hier:

- [ACS-Benutzerkonto einrichten und Zertifikat installieren, auf Seite 22](#)
 - [Benutzerhandbuch für Cisco Secure ACS für Windows](http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html)(<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)
-

Datum und Uhrzeit einstellen

Bei EAP-TLS wird die auf Zertifikaten basierende Authentifizierung verwendet, wobei der interne Zeitgeber im Cisco IP-Telefon ordnungsgemäß eingestellt sein muss. Datum und Uhrzeit auf dem Telefon können sich ändern, wenn das Gerät bei Cisco Unified Communications Manager registriert wird.



Hinweis Wenn ein neues Server-Authentifizierungszertifikat angefordert wird und die lokale Zeit hinter der GMT (Greenwich Mean Time) zurückliegt, schlägt die Überprüfung des Authentifizierungszertifikats möglicherweise fehl. Cisco empfiehlt, das lokale Datum und die lokale Uhrzeit so festzulegen, dass sie vor der GMT liegen.

Führen Sie die folgenden Schritte aus, um das lokale Datum und die lokale Uhrzeit korrekt festzulegen.

Prozedur

-
- Schritt 1** Wählen Sie im linken Navigationsbereich **Datum und Uhrzeit**.
 - Schritt 2** Wenn sich die Einstellung im Feld „Aktuelles Datum und Uhrzeit des Telefons“ von der im Feld „Lokales Datum und Uhrzeit“ unterscheidet, klicken Sie auf **Telefon auf lokales Datum und lokale Zeit festlegen**.
 - Schritt 3** Klicken Sie auf **Telefon neu starten** und anschließend auf **OK**.
-

Zertifikate im ACS exportieren und installieren

Zur Verwendung des MIC müssen Sie das Manufacturing Root Certificate (Stammzertifikat des Herstellers) und das Manufacturing CA Certificate (CA-Zertifikat des Herstellers) exportieren und auf dem Cisco ACS-Server installieren.

Führen Sie zum Exportieren des Manufacturing Root Certificate und des Manufacturing CA Certificate auf den ACS-Server die folgenden Schritte aus.

Prozedur

-
- Schritt 1** Wählen Sie auf der Telefon-Webseite **Zertifikate**.
 - Schritt 2** Klicken Sie neben dem Manufacturing Root Certificate auf **Exportieren**.
 - Schritt 3** Speichern Sie das Zertifikat, und kopieren Sie es auf den ACS-Server.
 - Schritt 4** Wiederholen Sie die Schritte 1 und 2 für das Manufacturing CA Certificate.
 - Schritt 5** Geben Sie auf der Seite „ACS-Server – Systemkonfiguration“ den Dateipfad für jedes Zertifikat ein, und installieren Sie die Zertifikate.

Hinweis Weitere Informationen zur Verwendung des ACS-Konfigurationstools finden Sie in der Online-Hilfe zu ACS oder im *Benutzerhandbuch für Cisco Secure ACS für Windows* (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>).

- Schritt 6** Fügen Sie auf der Seite „CTL (Certificate Trust List) bearbeiten“ die Zertifikate hinzu, denen der ACS vertrauen soll.
-

Methoden zum Exportieren von Zertifikaten aus dem ACS

Je nach Typ des aus dem ACS zu exportierenden Zertifikats ist eine der folgenden Methoden anzuwenden:

- Wenn Sie das CA-Zertifikat vom ACS-Server exportieren möchten, der das vom Benutzer installierte Zertifikat oder das ACS-Zertifikat signiert hat, siehe [CA-Zertifikat von ISE mithilfe der Microsoft-Zertifikatdienste exportieren, auf Seite 21](#).
- Wenn Sie das CA-Zertifikat vom ACS-Server exportieren möchten, der ein selbst signiertes Zertifikat verwendet, siehe [CA-Zertifikat von ACS mit Internet Explorer exportieren, auf Seite 21](#).

CA-Zertifikat von ISE mithilfe der Microsoft-Zertifikatdienste exportieren

Mit dieser Methode können Sie das CA-Zertifikat vom ISE-Server exportieren, der das vom Benutzer installierte Zertifikat oder das ISE-Zertifikat signiert hat.

Führen Sie, wie auf der Webseite der Microsoft-Zertifikatdienste beschrieben, die folgenden Schritte aus, um das CA-Zertifikat zu exportieren.

Prozedur

-
- | | |
|------------------|--|
| Schritt 1 | Wählen Sie Zertifizierungsstellenzertifikat, Zertifikatkette oder Zertifikatsperrliste herunterladen . |
| Schritt 2 | Markieren Sie auf der nächsten Seite das aktuelle CA-Zertifikat im Textfeld, wählen Sie unter „Codierungsmethode“ die Option „DER“, und klicken Sie anschließend auf Zertifizierungsstellenzertifikat herunterladen . |
| Schritt 3 | Speichern Sie das CA-Zertifikat. |
-

CA-Zertifikat von ACS mit Internet Explorer exportieren

Verwenden Sie diese Methode, um das CA-Zertifikat vom ACS-Server zu exportieren, der ein selbst signiertes Zertifikat verwendet.

Führen Sie die folgenden Schritte aus, um Zertifikate vom ACS-Server mit dem Internet Explorer zu exportieren.

Prozedur

-
- | | |
|------------------|--|
| Schritt 1 | Wählen Sie im Internet Explorer Extras > Internetoptionen , und klicken Sie dann auf die Registerkarte „Inhalte“. |
| Schritt 2 | Klicken Sie unter „Zertifikate“ auf Zertifikate , und klicken Sie anschließend auf die Registerkarte „Vertrauenswürdige Stammzertifizierungsstellen“. |
| Schritt 3 | Markieren Sie das Stammzertifikat, und klicken Sie auf Exportieren . Der Zertifikatexport-Assistent wird angezeigt. |
| Schritt 4 | Klicken Sie auf Weiter . |
| Schritt 5 | Wählen Sie im nächsten Fenster DER-codiert-binär X.509 (.CER) , und klicken Sie dann auf Weiter . |
| Schritt 6 | Geben Sie einen Namen für das Zertifikat an, und klicken Sie auf Weiter . |
| Schritt 7 | Speichern Sie das CA-Zertifikat, damit es auf dem Telefon installiert werden kann. |
-

Vom Benutzer installiertes Zertifikat anfordern und importieren

Mithilfe der folgenden Schritte können Sie ein Zertifikat abrufen und auf dem Telefon installieren.

Prozedur

-
- Schritt 1** Wählen Sie auf der Telefon-Webseite erst das Netzwerkprofil, das EAP-TLS nutzt, und anschließend im Feld für das EAP-TLS-Zertifikat **Installiert vom Benutzer**.
- Schritt 2** Klicken Sie auf **Zertifikate**.
- Auf der Seite zum Installieren des Benutzerzertifikats sollte der Name im Feld „Allgemeiner Name“ mit dem Benutzernamen für den ACS-Server übereinstimmen.
- Hinweis** Bei Bedarf können Sie das Feld „Allgemeiner Name“ auch bearbeiten. Es muss jedoch sichergestellt sein, dass dessen Inhalt mit dem Benutzernamen für den ACS-Server identisch ist. Siehe [ACS-Benutzerkonto einrichten und Zertifikat installieren, auf Seite 22](#).
- Schritt 3** Geben Sie die Informationen ein, die das Zertifikat enthalten soll, und klicken Sie anschließend auf **Senden**, um die CSR-Datei (Zertifikatssignierungsanforderung) zu generieren.
-

Stammzertifikat des Authentifizierungsservers installieren

Führen Sie die folgenden Schritte aus, um das Stammzertifikat des Authentifizierungsservers auf dem Telefon zu installieren.

Prozedur

-
- Schritt 1** Exportieren Sie das Stammzertifikat des Authentifizierungsservers aus dem ACS. Siehe [Methoden zum Exportieren von Zertifikaten aus dem ACS, auf Seite 21](#).
- Schritt 2** Navigieren Sie zur Telefon-Webseite, und wählen Sie **Zertifikate**.
- Schritt 3** Klicken Sie neben dem Stammzertifikat des Authentifizierungsservers auf **Importieren**.
- Schritt 4** Starten Sie das Telefon neu.
-

ACS-Benutzerkonto einrichten und Zertifikat installieren

Führen Sie die folgenden Schritte aus, um den Namen des Benutzerkontos einzurichten und das MIC-Stammzertifikat für das Telefon im ACS zu installieren.



-
- Hinweis** Weitere Informationen zur Verwendung des ACS-Konfigurationstools finden Sie in der Online-Hilfe zu ACS oder im *Benutzerhandbuch für Cisco Secure ACS für Windows*.
-

Prozedur

- Schritt 1** Erstellen Sie auf der Benutzer-Setup-Seite des ACS-Konfigurationstools einen Benutzerkontonamen für das Telefon, sofern ein solcher nicht bereits eingerichtet ist.
- In der Regel enthält der Benutzername am Ende die MAC-Adresse des Telefons. Für EAP-TLS ist kein Kennwort erforderlich.
- Hinweis** Vergewissern Sie sich, dass der Benutzername mit dem Eintrag im Feld „Allgemeiner Name“ auf der Seite zum Installieren des Benutzerzertifikats übereinstimmt. Siehe [Vom Benutzer installiertes Zertifikat anfordern und importieren, auf Seite 22](#).
- Schritt 2** Aktivieren Sie auf der Seite „Systemkonfiguration“ im Abschnitt „EAP-TLS“ die folgenden Felder:
- **Allow EAP-TLS (EAP-TLS zulassen)**
 - **Certificate CN comparison (CN-Vergleich für Zertifikate)**
- Schritt 3** Fügen Sie auf der Seite „ACS Certification Authority Setup“ (Einrichtung der ACS-Zertifizierungsstelle) dem ACS-Server das Manufacturing Root Certificate (Herstellerstammzertifikat) und das Manufacturing Certificate Authority Certificate (Hersteller-CA-Zertifikat) hinzu.
- Schritt 4** Aktivieren Sie in der ACS-Zertifikate-Vertrauensliste sowohl das Herstellerstammzertifikat als auch das Hersteller-CA-Zertifikat.
-

PEAP-Setup

Protected Extensible Authentication Protocol (PEAP) authentifiziert Clients mit serverseitigen Zertifikaten für öffentliche Schlüssel, indem ein verschlüsselter SSL/TLS-Tunnel zwischen dem Client und dem Authentifizierungsserver hergestellt wird.

Das Cisco IP-Telefon 8865 unterstützt nur ein Serverzertifikat, das entweder über SCEP oder die manuelle Installationsmethode, jedoch nicht über beide, installiert werden kann. Das Telefon unterstützt nicht die TFTP-Methode zur Zertifikatsinstallation.



Hinweis Die Validierung des Authentifizierungsservers kann durch Importieren des Zertifikats für den Authentifizierungsserver aktiviert werden.

Vorbereitungen

Vergewissern Sie sich vor dem Konfigurieren der PEAP-Authentifizierung für das Telefon, dass die folgenden Cisco Secure ACS-Anforderungen erfüllt sind:

- Das ACS-Stammzertifikat muss installiert sein.
- Ein Zertifikat kann auch installiert werden, um die Servervalidierung für PEAP zu aktivieren. Wenn jedoch ein Serverzertifikat installiert wird, wird auch die Servervalidierung aktiviert.
- Die Einstellung „Allow EAP-MSCHAPv2“ (EAP-MSCHAPv2 zulassen) muss aktiviert sein.
- Benutzerkonto und Kennwort müssen konfiguriert sein.

- Für die Kennwortauthentifizierung können Sie die lokale ACS-Datenbank oder eine externe Datenbank (wie Windows oder LDAP) verwenden.

PEAP-Authentifizierung aktivieren

Prozedur

-
- Schritt 1** Wählen Sie auf der Webseite für die Telefonkonfiguration PEAP als Authentifizierungsmodus aus.
- Schritt 2** Geben Sie einen Benutzernamen und ein Kennwort ein.
-

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.

Verwandte Themen

[Webseite für Cisco IP-Telefon](#)

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.
 - Drücken Sie auf dem Telefon auf **Anwendungen** , wählen Sie **Telefoninformationen**, und blättern Sie zum Feld „IPv4-Adresse“.
- 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:

Installieren eines Authentifizierungsserver-Zertifikats über die Webseite zur Telefonverwaltung

- 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 Feld „Benutzerinstallation“, und klicken Sie auf **Installieren**.
- Schritt 3** Navigieren Sie zum Zertifikat auf Ihren PC.
- Schritt 4** Geben Sie im Feld **Kennwort extrahieren** das Extraktionskennwort des Zertifikats an.
- Schritt 5** Klicken Sie auf **Hochladen**.
- Schritt 6** 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 Parameter 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. 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.
- 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 Meldungs austausch 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. 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 anschließen. In diesem Fall unterstützen Cisco IP-Telefon 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 mehrere 802.1X-konforme Geräte am gleichen Port nicht unterstützt, deaktivieren Sie den PC-Port, 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.

Auf die 802.1X-Authentifizierung zugreifen

Führen Sie die folgenden Schritte aus, um auf die Einstellungen für die 802.1X-Authentifizierung zuzugreifen:

Prozedur

Schritt 1

Drücken Sie **Anwendungen** .

Schritt 2

Wählen Sie **Verwaltereinstellungen > Sicherheits-Setup > 802.1X -Authentifizierung**.

Schritt 3

Konfigurieren Sie die Optionen entsprechend der Beschreibung in [802.1X-Authentifizierungsoptionen](#), auf [Seite 30](#).

Schritt 4 Drücken Sie zum Schließen dieses Menüs **Beenden**.

802.1X-Authentifizierungsoptionen


In folgender Tabelle sind die Optionen der 802.1X-Authentifizierung beschrieben.

Tabelle 6: 802.1X-Authentifizierung – Einstellungen

Option	Beschreibung	Änderung
Geräteauthentifizierung	Diese Option gibt an, ob die 802.1X-Authentifizierung aktiviert ist: <ul style="list-style-type: none"> • Aktiviert: Telefon verwendet die 802.1X-Authentifizierung, um Netzwerkzugriff anzufordern. • Deaktiviert: Standardeinstellung. Das Telefon verwendet CDP zur Anforderung des VLAN- und Netzwerkzugriffs. 	Siehe Feld „Geräteauthentifizierung“ auf Seite 30.
Transaktionsstatus	Status: Zeigt den Status der 802.1X-Authentifizierung an: <ul style="list-style-type: none"> • Verbindung getrennt: Zeigt an, dass die 802.1X-Authentifizierung auf dem Telefon nicht konfiguriert ist. • Authentifiziert: Zeigt an, dass das Telefon authentifiziert ist. • Gehalten: Zeigt an, dass die Authentifizierung gerade durchgeführt wird. Protokoll: Zeigt die EAP-Methode an, die für die 802.1X-Authentifizierung verwendet wird (EAP-FAST oder EAP-TLS).	Wird nur angezeigt. Der Wert kann nicht konfiguriert werden.

Feld „Geräteauthentifizierung“ festlegen

Prozedur

- Schritt 1** Drücken Sie **Anwendungen** .
- Schritt 2** Wählen Sie **Verwaltereinstellungen** > **Sicherheits-Setup** > **802.1X-Authentifizierung**.
- Schritt 3** Legen Sie die Option „Geräteauthentifizierung“ fest:
- **Ja**
 - **Nein**
- Schritt 4** Drücken Sie **Übernehmen**.
-

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.