

Häufig gestellte Fragen zu Unified PhoneProxy

Inhalt

[Einführung](#)

[Verwendung](#)

[Konfiguration](#)

[Benutzerverwaltung](#)

[Sicherheit und Verschlüsselung](#)

[Updates, Backup und Wartung](#)

[CallManager-Konfiguration](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beantwortet häufig gestellte Fragen zum Cisco Unified PhoneProxy.

Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps von Cisco zu Konventionen).

Verwendung

F. Können Sie einen PC an die Rückseite eines IP-Telefons anschließen, das für Cisco Unified PhoneProxy aktiviert und registriert ist und Unternehmensdaten abrufen?

Antwort: Nein. Cisco Unified PhoneProxy ermöglicht über eine Firewall eine SCCP-Verbindung (Signaling Connection Control Part) (und zugehörigen RTP-, TFTP- und HTTP-Datenverkehr) von einem Telefon zu einem Cisco Unified CallManager. Sie hat keine Auswirkungen auf Datenverbindungen zum Unternehmensnetzwerk für andere Zwecke als IP-Telefone. Der Benutzer, der an der Rückseite eines Telefons angeschlossen ist, hat nur Zugriff auf das lokale LAN. Sie müssen eine VPN-Verbindung erstellen, um auf Unternehmensdaten zugreifen zu können.

F. Funktioniert Cisco IP Communicator im Anwendungsfall Voice and Data VLAN Bridge auf einem Mobilgerät wie einem PDA? Kann sie sich beim Cisco Unified PhoneProxy registrieren und Anrufe tätigen?

Antwort: Das Anwendungsbeispiel für die Sprach- und Daten-VLAN-Bridge beinhaltet eine Trennung zwischen dem Sprach-VLAN und dem Daten-VLAN, unterstützt jedoch weiterhin IP Communicator-Bereitstellungen für mobile Mitarbeiter. Weitere Informationen zu Anwendungsfällen finden Sie im [Cisco Unified PhoneProxy Administration Guide](#).

Im Anwendungsfall der Sprach- und Daten-VLAN-Bridge hat der Cisco Unified PhoneProxy keinen Einfluss darauf, wie gut der Cisco IP Communicator auf einem Mobilgerät funktioniert. Er proximiert nur die SCCP-Verbindung (und den zugehörigen RTP-, TFTP- und HTTP-Verkehr).

Cisco Unified PhoneProxy behindert oder erleichtert den Zugriff auf Unternehmensnetzwerke nicht, es sei denn, das Telefon kann ordnungsgemäß funktionieren. Wenn Ihr Unternehmensnetzwerk dies erfordert, müssen Sie VPN vor dem Cisco Unified PhoneProxy verwenden. Die VPN-Verbindung muss jedoch nicht eingeschaltet werden, damit das Telefon funktioniert. IP Communicator ist jedoch die Ausnahme. Der IP Communicator-Telefondienst kann unterbrochen werden, wenn VPN ein- und ausgeschaltet wird.

Darüber hinaus können bei der Verbindung eines Telefons mit dem VPN mittelschwere bis schwerwiegende Probleme mit der Audioqualität auftreten, da das VPN keine spezifischen QoS-Stufen implementieren kann, die vom RTP-Stream benötigt werden. Weitere Informationen zu Audioproblemen finden Sie im [Cisco Unified PhoneProxy Administration Guide](#).

F. Wozu dienen die SFTP-Update-Dateien?

Antwort: Wenn Sie manuell eine Aktualisierungsdatei auf dem Cisco Unified PhoneProxy platzieren müssen, stellen Sie eine sichere FTP (SFTP)-Verbindung zur Süd-IP-Adresse (oder, falls aktiviert, zur Management-IP-Adresse) her, und legen Sie die Datei dann im eingehenden Ordner ab.

Hinweis: Mit dem folgenden Befehl können Sie Aktualisierungen aus dem Internet abrufen: erhalten Sie `update <url>`.

F. Lässt sich der RTP-Datenverkehr direkt von einem Remote-IP-Telefon zu einem anderen Remote-IP-Telefon übertragen?

Antwort: Nein. RTP-Datenverkehr wird immer über den Cisco Unified PhoneProxy geleitet. Cisco Unified PhoneProxy verfolgt jedoch nicht die Statusinformationen der einzelnen Telefone. Es ist daher nicht bekannt, dass es sich bei den beiden Anrufen von zwei verschiedenen Telefonen tatsächlich um einen Anruf zwischen zwei Telefonen handelt.

F. Welche Codecs werden von Remote-Telefonen unterstützt, die mit dem Cisco Unified PhoneProxy kommunizieren?

Antwort: Da Cisco Unified PhoneProxy keine Medientransformationen unterstützt, wird jeder Codec unterstützt. Bei verschlüsselten Medien tritt jedoch ein Problem auf, wenn der Modus 64 (RTP-Payload + RTP-Header) 43, 44, 45 oder 46 nicht entspricht. 20 ms g.711 sind daher zulässig. 30 ms g.711 ist nicht zulässig.

Um diesen Wert zu berechnen, verwenden Sie den modulo (mod) Vorgang. Der Modus gibt den Rest zurück, wenn eine Nummer durch eine andere geteilt wird. Beispiel: 13 Modus 5 gibt 3 zurück.

Für g.711 mit einer RTP-Payload von 160 und einem RTP-Header von 12 verwenden Sie die folgenden Berechnungen:

$$160+12=172$$

$172 \text{ Mod } 64 = 44$

44 ist ein akzeptabler Wert.

Hinweis: Eine andere Möglichkeit, diesen Vorgang zu interpretieren, besteht darin, die Nummer zu finden, die 172 am nächsten liegt und durch 64 dividierbar ist, d. h. 128. Der Rest von 172-128 ist 44. Daher sind $172 \text{ Mod } 64 = 44$.

Hinweis: Sie können auch Google Calculator verwenden, um die Ergebnisse einer Mod-Operation zu ermitteln. Geben Sie den Mod Vorgang in das Suchfeld unter [Google.com](https://www.google.com) ein.

Konfiguration

F. Was muss ich in einem Telefon programmieren, bevor ich es dem Endbenutzer gebe?

Antwort: Neben einer alternativen TFTP-Serveradresse, die auf den Proxy verweist, müssen Sie keine zusätzlichen Einstellungen am Telefon programmieren. Wenn die automatische Registrierung deaktiviert ist, sollte das Telefon jedoch in Cisco Unified CallManager bereitgestellt werden.

Hinweis: Möglicherweise müssen Sie das Endbenutzerkabel oder den DSL-Router konfigurieren. Wenn der Router keine Stateful Packet Inspection unterstützt, müssen Sie möglicherweise die UDP-Port-Weiterleitung (User Datagram Protocol) konfigurieren oder das Telefon in der Demilitarized Zone (DMZ) platzieren, insbesondere für Warteschleifenmusik.

F. Speichert der Cisco Unified PhoneProxy geografische Einstellungen?

Antwort: Nein. Der Cisco Unified PhoneProxy speichert keine geografischen Voreinstellungen. Wenn ein Benutzer eine Verbindung zu einem Cisco Unified PhoneProxy-Cluster herstellt, wird die Verbindung anhand der Anzahl der Benutzer hergestellt. Wenn Sie beispielsweise einen Cluster mit Knoten an der Ostküste und der Westküste konfigurieren, werden die Benutzer gleichmäßig auf die Knoten verteilt. Wenn Sie 1.500 Benutzer haben, sind 750 Benutzer an jeden Knoten angeschlossen. Einige Benutzer an der Westküste werden möglicherweise dem Knoten Ostküste zugewiesen, und einige Benutzer an der Ostküste werden möglicherweise dem Knoten Westküste zugewiesen.

F. Bedeutet "Keine Lizenzdurchsetzung", dass im Cisco Unified CallManager (wo die Anzahl nachverfolgt wird) alle Telefone, die über einen Proxy geleitet werden, als 1 angezeigt werden?

Antwort: Nein. Jedes Telefon muss im Cisco Unified CallManager bereitgestellt werden und benötigt dieselbe Anzahl von Lizenzeinheiten wie ohne Cisco Unified PhoneProxy. Weitere Informationen finden Sie im [Cisco Unified PhoneProxy Administration Guide](#).

Benutzerverwaltung

F. Können Sie eine Benutzerliste aus Cisco Unified CallManager oder einer anderen LDAP-Quelle importieren?

Antwort: Derzeit ist Cisco Unified PhoneProxy nicht direkt in diese Quellen integrierbar. Sie können jedoch eine CSV-Datei (Comma-Separated Value) in die Management Console importieren, um mehrere Benutzer hinzuzufügen.

F. Was bedeutet es, einen Anruf aus Benutzersicht zu *aktivieren*?

Antwort: Sie können die folgenden Methoden verwenden, um einen Anruf zu aktivieren:

- Der Endbenutzer aktiviert den Anruf über eine Webseite. Der Benutzer muss einen Benutzernamen, ein Kennwort und eine WAN-IP-Adresse angeben. (Die WAN-IP-Adresse ist nicht die interne 192.168.x.x-Adresse, die der Router bereitstellt.) **Hinweis:** Die Webseite erkennt die externe IP-Adresse und füllt die richtige Adresse aus. Abhängig vom Netzwerk müssen Sie diese IP-Adresse jedoch möglicherweise ändern.
- Der Administrator aktiviert den Anruf über die Befehlszeilenschnittstelle. Der Administrator muss einen Benutzernamen und eine IP-Adresse angeben.
- Die Anwendung aktiviert das Konto und stellt den Benutzernamen, das Kennwort und die IP-Adresse bereit. Sie müssen den Aktivierungs-Webdienst aktivieren, um diese Methode verwenden zu können.

F. Muss ich die Aktivierung vor jedem Anruf, täglich oder nur einmal durchführen?

Antwort: Die Aktivierung bleibt aktiviert, solange eine SCCP-Verbindung zwischen dem IP-Telefon und dem Cisco Unified PhoneProxy besteht. Da bei einer SCCP-Verbindung ein Großteil des Keep-Alive-Verkehrs vorhanden ist, sollte die Aktivierung nicht zeitlich unterbrochen werden.

Die Standardeinstellung für die Leerlaufzeitüberschreitung bei der Aktivierung ist 300 Sekunden (5 Minuten). Diese Leerlaufzeit tritt nur dann auf, wenn das IP-Telefon nach Aktivierung des Kontos nie registriert wird. Beispielsweise wird das Konto aktiviert, aber das Telefon wird nicht innerhalb von 5 Minuten an das Netzwerk angeschlossen, oder das Telefon verliert die Netzwerkverbindung (aufgrund eines Internet- oder Stromausfalls, der länger als 5 Minuten dauert) oder die IP-Adresse ändert sich (weil der IP-Lease abläuft oder DHCP eine andere Adresse zuweist).

Der Cisco Unified PhoneProxy erwartet, dass er eine Verbindung zu diesem Konto und zu dieser IP-Adresse unterhält. Wenn diese Verbindung länger als die konfigurierte Leerlaufzeit unterbrochen wird, ist das Konto inaktiv.

Hinweis: Administratoren können ein vom Leerlauf-Timeout unabhängiges Autorisierungs-Timeout konfigurieren. Das Autorisierungs-Timeout bewirkt, dass ein aktives Konto nach einer festgelegten Anzahl von Sekunden inaktiv wird. Dies erfordert, dass sich die Benutzer erneut authentifizieren, sobald der Timeout-Wert abläuft. Dieser Wert ist standardmäßig 0 Sekunden, d. h. das Konto wird nicht automatisch inaktiv.

Sicherheit und Verschlüsselung

F. Funktioniert Sicherheit und Verschlüsselung mit Cisco Unified CallManager 5.0?

Antwort: Ja. Sicherheit und Verschlüsselung wurden getestet und funktionieren mit Cisco Unified CallManager 5.0.4 und 5.1.

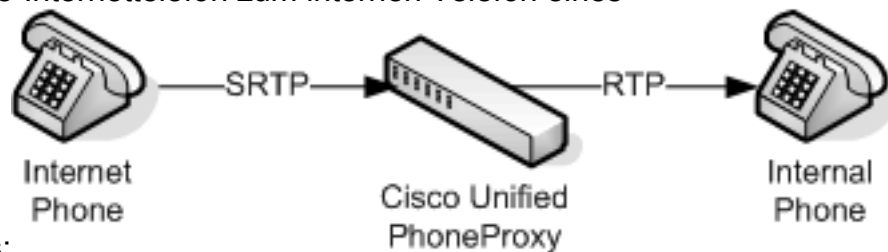
Hinweis: Cisco Unified CallManager 5.0 behandelt Zertifikate anders als Version 4.x.

F. Kann der Cisco Unified PhoneProxy sicher mit Telefonen im nicht vertrauenswürdigen Internet kommunizieren, während er im vertrauenswürdigen internen Netzwerk unverschlüsselt bleibt? Kann der Cisco Unified PhoneProxy sicher mit zwei Telefonen im nicht vertrauenswürdigen Internet kommunizieren?

Antwort: Wenn die Sicherheit aktiviert ist, müssen alle Telefone im nicht vertrauenswürdigen Internet sicher mit dem Cisco Unified PhoneProxy kommunizieren, oder sie dürfen nicht kommunizieren. Das Anrufsegment zwischen dem Cisco Unified PhoneProxy und einem Remote-IP-Telefon wird verschlüsselt. Das Anrufsegment zwischen zwei Remote-IP-Telefonen ist verschlüsselt, aber das Anrufsegment zwischen dem Cisco Unified PhoneProxy oder den internen Cisco Unified CallManager- und IP-Telefonen bleibt unverschlüsselt.

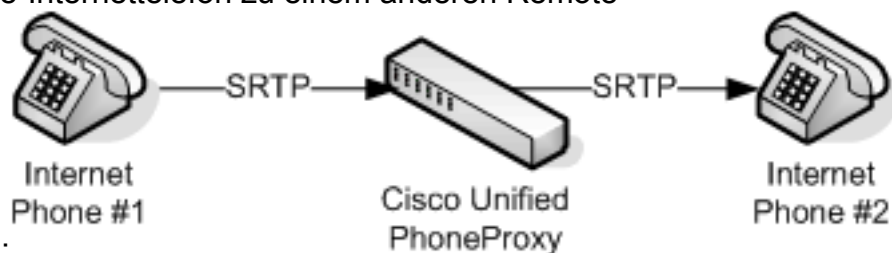
Diese Bilder veranschaulichen die Verschlüsselung von Anrufsegmenten.

- Für ein Remote-Internettelefon zum internen Telefon eines



Unternehmens:

- Für ein Remote-Internettelefon zu einem anderen Remote-



Internettelefon:

F. Wie konfiguriere ich die Adaptive Security Appliance (ASA) für Cisco Phone Proxy?

Antwort: Informationen zum Konfigurieren der ASA für Cisco Phone Proxy-Funktion finden Sie unter [Konfigurieren der Cisco Phone Proxy-Funktion](#).

F. Welche Funktionen werden von ASA Phone Proxy unterstützt?

Antwort: ASA-Telefon-Proxy unterstützt folgende Funktionen:

- Warteschleifenmusik
- XML-Dienste

F. Ist es möglich, einen HTTP-Proxy hinzuzufügen und mit Phone Proxy zu verwenden?

Antwort: Ein umgekehrter HTTP-Proxy zu Cisco Unified Communications Manager kann

verwendet werden, um die IP-Telefone auf die ASA zu verweisen. Diese Lösung ist sicherer als das Öffnen eines HTTP-Servers in Cisco Unified Communications Manager und erfordert einen HTTP Reverse Proxy-Server.

F. Welche Version von PhoneProxy unterstützt die SCCP-Version?

Antwort: Die ASA Version 8.0(4) enthält Unified Communications-Funktionen, wie *Phone Proxy* und *Mobile Proxy*, die SCCPv17 unterstützen.

F. Welche Sprachfunktionen (z. B. Warteschleifenmusik, Anrufweiterleitung, Konferenz) werden von Phone Proxy unterstützt?

Antwort: Warteschleifenmusik wird vom ASA Phone Proxy unterstützt, aber einige Telefone, die über einen Cisco ASA Phone Proxy (Codebase 8.2(1)) verbunden sind, können die lokalen Warteschleifenmusik-Audioquellen vom CUCM nicht hören. Dieses Problem wird durch die Cisco Bug ID [CSCso81816](#) dokumentiert ([nur registrierte](#) Kunden). Anrufe können mithilfe von ASA Phone Proxy gehalten oder weitergeleitet werden. Unternehmensfunktionen wie Konferenzgespräche werden auch auf Remote-Telefonen unterstützt, die über einen ASA-Telefonproxy verbunden sind.

Updates, Backup und Wartung

F. Kann ich das Administrator Kennwort für den Cisco Unified PhoneProxy wiederherstellen?

Antwort: Die Verwaltungseinstellungen in der Management Console sind kennwortgeschützt. Dieses Kennwort kann nicht wiederhergestellt werden. Sie müssen eine neue Konfiguration und ein neues Kennwort erstellen.

Sie können die folgenden Bereiche der Cisco Unified PhoneProxy-CLI auch mit einem Kennwort schützen:

- *Mainpartition* - Sie können die Wartungspartition mit einem Kennwort schützen. Es ist jedoch nicht standardmäßig kennwortgeschützt. Um ein Kennwort zu erstellen, müssen Sie sich in der Wartungspartition befinden. Wenn das Wartungskennwort verloren geht, können Sie es nicht wiederherstellen.
- *image0* und *image1* partitions - Die *image0*- und *image1*-Partitionen sind durch ein Kennwort geschützt, das vom *Partitions*kennwort getrennt ist. Sie können das Kennwort für die Image-Partition innerhalb der Image-Partition oder innerhalb der Wartungspartition festlegen.

F. Gibt es eine Möglichkeit, die *Mainline*-Bootimage zu aktualisieren?

Antwort: Nein. Die Mainbootimage kann nicht aktualisiert werden. Es sollte keinen Grund geben, dieses Bootimage zu aktualisieren.

F. Wenn der Knoten eines Cisco Unified PhoneProxy-Clusters ausfällt, sendet der nächste Unified PhoneProxy Telefonregistrierungen an den Cisco Unified CallManager? Führt diese Situation zu Leistungsproblemen?

Antwort: Der Cisco Unified PhoneProxy überträgt nur Daten, die von den Telefonen gesendet werden. Wenn beispielsweise eines der Mitglieder des Clusters in einem Cisco Unified CallManager-Cluster ausfällt, werden alle Telefone in einen anderen CallManager umgeleitet und registriert. Die Telefone verfügen über eine offene Verbindung zum Standby-Unified CallManager, sodass sie eine Registrierungsanfrage senden. Zwischen dem Telefon und dem Unified CallManager werden weitere Nachrichten gesendet. Dem Telefon ist jedoch nicht bewusst, dass der primäre CallManager ausfällt, bis er einen Takt verpasst hat. Da die Heartbeat-Funktion für die Telefone nicht synchronisiert wird, werden die Registrierungsversuche in einem Intervall von 30 Sekunden verteilt, und die Leistung wird nicht beeinträchtigt.

F. Woher weiß ein Telefon, dass es sich beim sekundären Cisco Unified PhoneProxy-Knoten registrieren lässt, wenn der primäre Knoten ausgefallen ist?

Antwort: Die Heartbeat-Funktion für jedes Telefon wird alle 30 Sekunden aufgerufen. Wenn ein Beat nicht erreicht wird, registriert sich das Telefon beim sekundären Knoten und versucht dann, sich erneut beim primären Knoten zu registrieren.

CallManager-Konfiguration

F. Wird der Cisco Unified PhoneProxy in Cisco Unified CallManager angezeigt?

Antwort: Nein. Die Telefone, die weitergeleitet werden, werden in Cisco Unified CallManager angezeigt, der Cisco Unified PhoneProxy wird jedoch nicht angezeigt.

Hinweis: Im Cisco Unified CallManager zeigen alle registrierten und proxitierten Telefone dieselbe IP-Adresse an. Diese IP-Adresse ist die IP-Adresse der Süd-Schnittstelle des Cisco Unified PhoneProxy, der sich im gleichen Subnetz wie das Sprach-VLAN für CallManager befindet.

F. Muss ich jedes Telefon im Proxy und im Cisco Unified CallManager konfigurieren?

Antwort: Ja. Wenn die automatische Registrierung deaktiviert wurde, sollte das Telefon im Cisco Unified CallManager rechtzeitig bereitgestellt werden. Außerdem sollte ein Konto für das Telefon erstellt und über die Management Console für den Cisco Unified PhoneProxy veröffentlicht werden. Um das Konto zu erstellen, müssen Sie einen Benutzernamen, ein Kennwort, eine Station-ID des Telefons (z. B. SEP112233445566) und den CallManager angeben, auf den die Registrierung angewiesen ist. Wenn der Benutzer das Konto aktiviert, muss er den Benutzernamen, das Kennwort und die IP-Adresse angeben.

Hinweis: Im Cisco Unified CallManager zeigen alle registrierten und proxitierten Telefone dieselbe IP-Adresse an. Diese IP-Adresse ist die IP-Adresse der Süd-Schnittstelle des Cisco Unified PhoneProxy, der sich im gleichen Subnetz wie das Sprach-VLAN für CallManager befindet.

F. Werden Partitionen, Anruffunktionen und gewählte Nummern von Cisco Unified CallManager gesteuert?

Antwort: Ja. Telefon, gewählte Nummer, Calling Search Spaces und Partitionen sollten in Cisco Unified CallManager bereitgestellt werden. Cisco Unified CallManager behält die Kontrolle über Wählpläne.

Dem Cisco Unified PhoneProxy sind Leitungsnummern, Weiterleitungsmuster, Calling Search Spaces oder Partitionen nicht bekannt. Der Cisco Unified PhoneProxy leitet nur die Telefonregistrierung (und RTP) weiter.

Zugehörige Informationen

- [Cisco Unified PhoneProxy-Dokumentation](#)
- [Administrationsleitfaden für Cisco Unified PhoneProxy](#)
- [Unterstützung von Sprachtechnologie](#)
- [Produkt-Support für Sprach- und Unified Communications](#)
- [Empfohlene Lektüre: Fehlerbehebung bei Cisco IP-Telefonie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)