Multiplattform-Telefone der Cisco IP Phone 6800-Serie – Bereitstellungshandbuch

Erste Veröffentlichung: 22 November 2017

Letzte Änderung: 5 August 2019

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

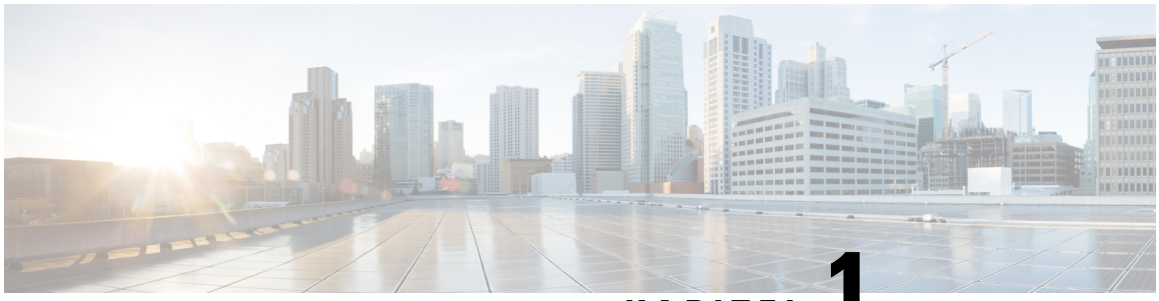
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

INHALTSVERZEICHNIS



KAPITEL 1

Bereitstellung

Neue und geänderte Informationen

Neu und geändert in Firmware-Version 11.2(4)

Revisionen	Neue und geänderte Abschnitte
Parameter für Wi-Fi-Einstellungen hinzugefügt	Beispiel für XML-Open-Format, auf Seite 83

Neu und geändert in Firmware-Version 11.2(3)SR1

Die Funktionen in den folgenden Abschnitten wurden neu hinzugefügt oder aktualisiert, um das Multiplattform-Telefone der Cisco IP Phone 6800-Serie zu unterstützen.

Revisionen	Neue und geänderte Abschnitte
Ein neues Thema zur Einführung des Aktivierungscodes wurde hinzugefügt.	Auf Ihrem Telefon mit dem Aktivierungscode , auf Seite 11

Neu und geändert in Firmware-Version 11.2(3)

Die Funktionen in den folgenden Abschnitten wurden neu hinzugefügt oder aktualisiert, um das Multiplattform-Telefone der Cisco IP Phone 6800-Serie zu unterstützen.

Revisionen	Neue und geänderte Abschnitte
Ein Konzeptthema für die Verschlüsselung des Open-Format-Profils hinzugefügt.	Open-Format-Profil – Verschlüsselung, auf Seite 21
Ein neues Thema zur RFC 8188-basierten HTTP-Inhaltsverschlüsselung hinzugefügt.	RFC-8188-basierte HTTP-Inhaltsverschlüsselung, auf Seite 25
Mit Details zur RFC 8188-basierten Verschlüsselung aktualisiert.	Konfigurationsprofil-Formate, auf Seite 15 HTTP-Bereitstellung, auf Seite 45
Einführungsdetails für die Verschlüsselung des Open-Format-Profils aktualisiert.	AES-256-CBC-Verschlüsselung, auf Seite 21
Beschreibung der **`--Schlüssel`**-Option aktualisiert und einen Hinweis zur RFC 8188-basierten Verschlüsselung hinzugefügt.	Schlüssel, auf Seite 25 Konfigurationsprofilparameter, auf Seite 71
Beispiele für XML-Open-Format mit neuen Parametern und verfügbaren Optionen aktualisiert	Beispiel für XML-Open-Format, auf Seite 83

Neu und geändert in Firmware-Version 11.2(1)

Revisionen	Neue oder geänderte Abschnitte
Thema mit einem Verweis auf den Vergleich der XML- und TR69-Parameter aktualisiert	TR69-Bereitstellung, auf Seite 4
Neues Thema zur Unterstützung des Privatfunktion-Headers hinzugefügt	Privatfunktion-Header für Telefon einrichten, auf Seite 68
Neues Thema zur Unterstützung von Peer-Firmware-Freigabe hinzugefügt	Peer-Firmware-Freigabe, auf Seite 12
Thema mit den Verschlüsselungsmethoden aktualisiert	Anfordern eines signierten Serverzertifikats, auf Seite 48
Thema aktualisiert, um Unterstützung der Funktion zum Umgehen des Bildschirms **Kennwort festlegen** hinzuzufügen	Konfigurationszugriffssteuerung, auf Seite 9
Neues Thema hinzugefügt, um das Umgehen des Bildschirms **Kennwort festlegen** zu unterstützen	Umgehen des Bildschirms „Kennwort festlegen“, auf Seite 13

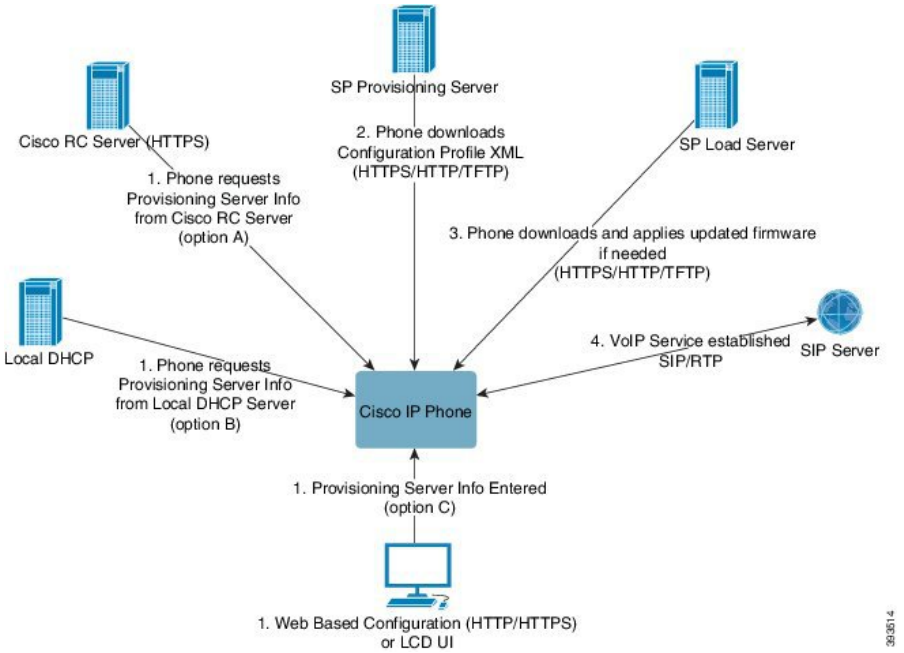
Übersicht über die Bereitstellung

Cisco IP Phones sind für Massenbereitstellungen von Voice-over-IP-(VoIP-)Serviceanbietern für Kunden in Home-, Business- oder Enterprise-Umgebungen vorgesehen. Daher stellt die Bereitstellung des Telefons über Remoteverwaltung und -konfiguration den ordnungsgemäßen Betrieb des Telefons am Kundenstandort sicher.

Cisco unterstützt die angepasste kontinuierliche Funktionskonfiguration des Telefons durch:

- Zuverlässige Remotesteuerung des Telefons
- Verschlüsselung der Kommunikation, mit der das Telefon gesteuert wird
- Optimierte Bindung von Telefon und Konto

Telefone können so bereitgestellt werden, dass sie Konfigurationsprofile oder aktualisierte Firmware von einem Remoteserver herunterladen. Die Downloads können in festgelegten Intervallen durchgeführt werden oder immer dann, wenn die Telefone mit einem Netzwerk verbunden oder eingeschaltet werden. Die Bereitstellung erfolgt normalerweise im Rahmen von VoIP-Massenbereitstellungen, die von Serviceanbietern durchgeführt werden. Konfigurationsprofile oder aktualisierte Firmware werden über TFTP, HTTP oder HTTPS an das Gerät übertragen.



Auf einer hohen Ebene verläuft der Telefonbereitstellungsprozess wie folgt:

1. Wenn das Telefon noch nicht konfiguriert ist, werden die Bereitstellungsserverinformationen an das Telefon über eine der folgenden Optionen übertragen:
   - **A** – Vom Remote Customization-(RC-)Server des Cisco Enablement Data Orchestration System (EDOS) über HTTPS heruntergeladen.
   - **B** – Vom lokalen DHCP-Server abgefragt.
   - **C** – Manuell über das webbasierte Konfigurationsprogramm oder die Telefon-UI des Cisco Telefons eingegeben.
2. Das Telefon lädt die Informationen des Bereitstellungsservers herunter und wendet die Konfigurations-XML über das HTTPS-, HTTP- oder TFTP-Protokoll an.
3. Das Telefon lädt die aktualisierte Firmware bei Bedarf über HTTPS, HTTP oder TFTP herunter und wendet sie an.

4. Der VoIP-Dienst wird mithilfe der angegebenen Konfiguration und Firmware eingerichtet.

VoIP-Serviceanbieter beabsichtigen, viele Telefone für Privatkunden und kleine Unternehmen bereitzustellen. In Unternehmens- oder Enterprise-Umgebungen können Telefone als Endknoten fungieren. Die Anbieter verbreiten diese Geräte weit über das Internet. Sie werden über Router und Firewalls an den Kundenstandorten verbunden.

Das Telefon kann als Remote-Erweiterung der Back-End-Geräte des Serviceanbieters verwendet werden. Remoteverwaltung und -konfiguration ermöglichen den ordnungsgemäßen Betrieb des Telefons an den Kundenstandorten.

TR69-Bereitstellung

Das Cisco IP Phone ermöglicht es dem Administrator, die TR69-Parameter über die Webbenutzeroberfläche zu konfigurieren. Informationen zu den Parametern, einschließlich einem Vergleich der XML- und TR69-Parameter, finden Sie im Administratorhandbuch für die entsprechende Telefonserie.

Das Telefon unterstützt die Auto Configuration Server-(ACS-)Erkennung über die DHCP-Option 43, 60 und 125.

- Option 43 – Herstellerspezifische Informationen für die ACS-URL.
- Option 60 – VCI (Vendor Class Identifier, Herstellerklassenbezeichner) für das Telefon, um sich selbst mit `dslforum.org` beim ACS zu identifizieren.
- Option 125 – Herstellerspezifische Informationen zur Gateway-Zuordnung.

RPC-Methoden

Unterstützte RPC-Methoden

Die Telefone unterstützen nur eine begrenzte Auswahl an Remote Procedure Call-(RPC-)Methoden, wie die folgenden:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform

- Download: Die RPC-Methode Download unterstützt die folgenden Dateitypen:
  - Firmware-Upgrade-Image
  - Anbieterspezifische Konfigurationsdatei
  - Benutzerdefinierte Certificate Authority-(CA-)Datei
- Transfer Complete

Unterstützte Ereignistypen

Die Telefone unterstützen Ereignistypen basierend auf den unterstützten Funktionen und Methoden. Nur die folgenden Ereignistypen werden unterstützt:

- Bootstrap
- Boot
- value change
- connection request
- Periodic
- Transfer Complete
- M Download
- M Reboot

Verschlüsselung der Kommunikation

Die Konfigurationsparameter, die an das Gerät übermittelt werden, enthalten Autorisierungscodes oder andere Informationen, die das System vor unbefugtem Zugriff schützen. Es liegt im Interesse des Serviceanbieters, unbefugte Kundenaktivitäten zu verhindern. Im Interesse des Kunden ist es, eine unbefugte Nutzung seines Kontos zu verhindern. Der Serviceanbieter kann den Austausch der Konfigurationsprofildaten zwischen dem Bereitstellungsserver und dem Gerät verschlüsseln und zusätzlich den Zugriff auf den Verwaltungswebserver einschränken.

Verhalten des Telefons bei Netzwerküberlastung

Alle Aktivitäten, die die Netzwerkleistung beeinträchtigen, können sich auf die Audio- und Videoqualität des Telefons auswirken und verursachen, dass ein Anruf getrennt wird. Eine Netzwerküberlastung kann unter anderem von folgenden Aktivitäten verursacht werden:

- Verwaltungsaufgaben, beispielsweise die Überprüfung von internen Anschlüssen oder der Sicherheit
- Netzwerkangriffe, beispielsweise ein Denial-of-Service-Angriff

Bereitstellung

Cisco IP Phones bieten bequeme Mechanismen für die Bereitstellung, die auf diesen Bereitstellungsmodellen basieren:

- Massenverteilung: Der Serviceanbieter erwirbt Cisco IP Phones in großen Stückzahlen und stellt sie entweder vorab intern bereit oder erwirbt RC-Einheiten für die Remote-Personalisierung von Cisco. Die Geräte werden dann im Rahmen eines VoIP-Servicevertrags an die Kunden ausgegeben.
- Verteilung über den Einzelhandel: Der Kunde erwirbt das Cisco IP Phone in einem Einzelhandelsgeschäft und fordert vom Serviceanbieter den VoIP-Service an. Der Serviceanbieter muss dann die sichere Remotekonfiguration des Geräts unterstützen.

Massenverteilung

Bei diesem Modell gibt der Serviceanbieter Telefone im Rahmen eines VoIP-Servicevertrags an seine Kunden weiter. Die Geräte sind entweder für die Remote-Personalisierung vorgesehen oder werden intern vorab bereitgestellt.

Cisco stellt die für die Remote-Personalisierung vorgesehenen Geräte vorab bereit, sodass sie sich mit einem Cisco Server resynchronisieren, der das Geräteprofil und Firmware-Updates herunterlädt.

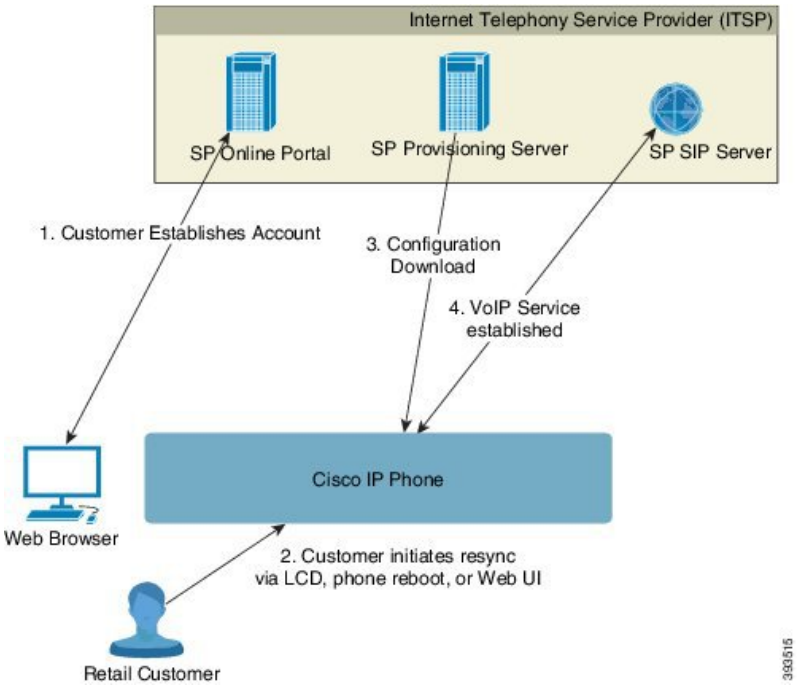
Ein Serviceanbieter kann Telefone mit den gewünschten Parametern vorab bereitstellen, einschließlich der Parameter, welche die Resynchronisierung steuern. Hierfür sind verschiedene Methoden verfügbar:

- Intern mit DHCP und TFTP
- Remote mit TFTP, HTTP oder HTTPS
- Eine Kombination aus interner und Remotebereitstellung

Verteilung über den Einzelhandel

Bei dem Modell der Verteilung über den Einzelhandel erwirbt der Kunde ein Telefon und abonniert einen bestimmten Dienst. Der ITSP (Internet Telephony Service Provider, Internet-Telefonie-Serviceanbieter) richtet einen Bereitstellungsserver ein und verwaltet ihn, und er stellt das Telefon so vorab bereit, dass es sich mit dem Server des Serviceanbieters resynchronisiert.

Abbildung 1: Verteilung über den Einzelhandel



Das Telefon enthält ein webbasiertes Configuration Utility, das die interne Konfiguration anzeigt und neue Konfigurationsparameterwerte akzeptiert. Der Server akzeptiert auch eine spezielle URL-Befehlssyntax für die Resynchronisierung des Profils und Firmware-Updates von Remotestandorten.

Der Kunde meldet sich beim Service an, richtet ein VoIP-Benutzerkonto möglicherweise über ein Online-Portal ein und verknüpft das Gerät mit dem zugewiesenen Servicekonto. Das nicht vorbereitete Telefon wird angewiesen, sich mit einem bestimmten Bereitstellungsserver über einen URL-Befehl zur Resynchronisierung zu resynchronisieren. Der URL-Befehl umfasst in der Regel eine Kontonummer mit Kunden-ID oder einen alphanumerischen Code, um das Gerät dem neuen Konto zuzuordnen.

Im folgenden Beispiel wird ein Gerät mit der von DHCP zugewiesenen IP-Adresse 192.168.1.102 angewiesen, sich selbst hier für den SuperVoIP-Service bereitzustellen:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

In diesem Beispiel ist 1234abcd die Kunden-ID-Nummer des neuen Kontos. Der Remote-Bereitstellungsserver ordnet das Telefon, das die Resynchronisierung anfordert, anhand der URL und der bereitgestellten Kunden-ID dem neuen Konto zu. Durch diese erste Resynchronisierung wird das Telefon in einem Schritt konfiguriert. Das Telefon wird automatisch angewiesen, sich danach mit einer permanenten URL auf dem Server erneut zu synchronisieren. Beispiel:

```
https://prov.supervoip.com/cisco-init
```

Sowohl beim ersten als auch beim permanenten Zugriff stützt sich der Bereitstellungsserver bei der Authentifizierung auf das Clientzertifikat des Telefons. Der Bereitstellungsserver stellt anhand des zugehörigen Servicekontos die richtigen Konfigurationsparameterwerte bereit.

Wenn das Gerät eingeschaltet wird oder eine angegebene Zeitspanne verstrichen ist, führt das Telefon die Resynchronisierung durch und lädt die neuesten Parameter herunter. Diese Parameter können zu verschiedenen Zwecken verwendet werden, z. B. zum Einrichten einer Sammelanschlussgruppe, Festlegen von Kurzwahlnummern und Beschränken der Funktionen, die ein Benutzer ändern kann.

Verwandte Themen

Interne Vorabbereitstellung von Geräten, auf Seite 43

Resynchronisierungsvorgang

Die Firmware eines jeden Telefons enthält einen Verwaltungswebserver, der neue Konfigurationsparameterwerte akzeptiert. Das Telefon kann über einen URL-Befehl im Geräteprofil angewiesen werden, die Konfiguration nach dem Neustart oder in geplanten Intervallen mit einem angegebenen Bereitstellungsserver erneut zu synchronisieren.

Der Webserver ist standardmäßig aktiviert. Um den Webserver zu deaktivieren oder zu aktivieren, verwenden Sie den URL-Befehl „resync“.

Falls nötig, kann eine sofortige Resynchronisierung über eine Aktions-URL mit dem Befehl „resync“ angefordert werden. Der URL-Befehl „resync“ kann eine Kontonummer mit Kunden-ID oder einen alphanumerischen Code enthalten, um das Gerät eindeutig dem Konto des Benutzers zuzuordnen.

Beispiel

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

In diesem Beispiel wird ein Gerät mit der von DHCP zugewiesenen IP-Adresse 192.168.1.102 angewiesen, sich selbst für den SuperVoIP-Service auf prov.supervoip.com bereitzustellen. Die Kunden-ID-Nummer für das neue Konto lautet 1234abcd. Der Remote-Bereitstellungsserver ordnet das Telefon, das die Resynchronisierung anfordert, anhand der URL und Kunden-ID dem Konto zu.

Durch diese erste Resynchronisierung wird das Telefon in einem Schritt konfiguriert. Das Telefon wird automatisch angewiesen, sich danach mit einer permanenten URL auf dem Server erneut zu synchronisieren.

Sowohl beim ersten als auch beim permanenten Zugriff stützt sich der Bereitstellungsserver bei der Authentifizierung auf das Clientzertifikat. Der Server stellt anhand des zugehörigen Servicekontos die richtigen Konfigurationsparameterwerte bereit.

Bereitstellung

Ein Telefon kann so konfiguriert werden, dass sein interner Konfigurationszustand in regelmäßigen Abständen und beim Einschalten mit einem Remoteprofil resynchronisiert wird. Das Telefon kontaktiert einen NPS (Normal Provisioning Server, normaler Bereitstellungsserver) oder einen ACS (Access Control Server, Zugriffssteuerungsserver).

Standardmäßig wird eine erneute Profilsynchronisierung nur dann versucht, wenn das Telefon inaktiv ist. Auf diese Weise wird verhindert, dass durch eine Aktualisierung ein Neustart der Software ausgelöst und ein Gespräch unterbrochen wird. Wenn zwischenzeitliche Upgrades erforderlich sind, um eine ältere Version auf einen aktuellen Upgrade-Status zu aktualisieren, kann die Upgrade-Logik mehrstufige Upgrades automatisieren.

Normaler Bereitstellungsserver

Bei einem NPS kann es sich um einen TFTP-, HTTP- oder HTTPS-Server handeln. Da die Firmware keine vertraulichen Informationen enthält, wird für ein Remote-Upgrade der Firmware TFTP, HTTP oder HTTPS verwendet.

Obwohl HTTPS empfohlen wird, ist für die Kommunikation mit dem NPS kein sicheres Protokoll erforderlich, da das aktualisierte Profil mit einem Shared-Secret-Schlüssel verschlüsselt werden kann. Weitere Informationen zur Nutzung von HTTPS finden Sie unter Verschlüsselung der Kommunikation, auf Seite 5. Eine sichere erstmalige Bereitstellung erfolgt über einen Mechanismus, der SSL-Funktionen nutzt. Ein nicht konfiguriertes Telefon erhält ein mit einem symmetrischen 256-Bit-Schlüssel verschlüsseltes Profil, das für dieses Gerät vorgesehen ist.

Konfigurationszugriffssteuerung

Die Firmware des Telefons stellt Mechanismen zum Einschränken des Endbenutzerzugriffs auf einige Parameter bereit. Die Firmware sieht bestimmte Berechtigungen für die Anmeldung bei einem **Administratorkonto** oder einem **Benutzerkonto** vor. Beide können unabhängig voneinander mit einem Kennwort geschützt werden.

- Administratorkonto – Bietet dem Serviceanbieter vollständigen Zugriff auf alle Verwaltungswebserverparameter.
- Benutzerkonto – Ermöglicht dem Benutzer, eine Teilmenge der Verwaltungswebserverparameter zu konfigurieren.

Der Serviceanbieter kann das Benutzerkonto im Bereitstellungsprofil wie folgt einschränken:

- Beim Erstellen der Konfiguration angeben, welche Konfigurationsparameter für das Benutzerkonto verfügbar sind.
- Den Zugriff von Benutzern auf den Verwaltungswebserver deaktivieren.
- Den Benutzerzugriff auf die LCD-Benutzeroberfläche deaktivieren.
- Umgehen des Bildschirms **Kennwort festlegen** für den Benutzer.
- Die Internet-Domänen beschränken, auf die das Gerät zugreift, um eine Resynchronisierung, Upgrades oder die SIP-Registrierung für Leitung 1 durchzuführen.

Verwandte Themen

Eigenschaften der Element-Tags, auf Seite 16
Zugriffskontrolle, auf Seite 18

Auf die Webseite des Telefons zugreifen

Wenn Ihr Serviceanbieter den Zugriff auf das Konfigurationsprogramm deaktiviert hat, wenden Sie sich an den Serviceanbieter, bevor Sie fortfahren.

Prozedur

Schritt 1 Stellen Sie sicher, dass der Computer mit dem Telefon kommunizieren kann. Es wird kein VPN verwendet.

Schritt 2 Starten Sie einen Webbrowser.

Schritt 3 Geben Sie die IP-Adresse des Telefons in die Adressleiste des Browsers ein.

- Benutzerzugriff: **`http://<IP-Adresse>`**
- Administratorzugriff: **`http://<IP-Adresse>/admin/advanced`**
- Administratorzugriff: **`http://<IP-Adresse>`**. Klicken Sie auf **Administratoranmeldung** und **advanced**.

For example, `http://10.64.84.147/admin`

Schritt 4 Geben Sie bei entsprechender Aufforderung das Kennwort ein.

Den Webzugriff auf das Cisco IP Phone gewähren

Um die Telefonparameter anzuzeigen, aktivieren Sie das Konfigurationsprofil. Um einen Parameter zu ändern, müssen Sie das Konfigurationsprofil bearbeiten können. Der Systemadministrator hat die Telefonoption möglicherweise deaktiviert, damit die Webbenutzeroberfläche des Telefons angezeigt und bearbeitet werden kann.

Weitere Informationen finden Sie unter *Multiplattform-Telefone der Cisco IP Phone 6800-Serie – Bereitstellungshandbuch*.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Prozedur

Schritt 1 Klicken Sie auf **Sprache** > **System**.

Schritt 2 Legen Sie im Bereich **Systemkonfiguration** die Option **Webserver aktivieren** auf **Ja** fest.

Schritt 3 Um das Konfigurationsprofil zu aktualisieren, klicken Sie auf **Alle Änderungen übernehmen**, nachdem Sie die Felder auf der Webbenutzeroberfläche des Telefons geändert haben.

Das Telefon wird neu gestartet und die Änderungen werden übernommen.

Schritt 4 Um alle Änderungen zu verwerfen, die Sie während der aktuellen Sitzung (oder nachdem Sie auf **Alle Änderungen übernehmen** geklickt haben) vorgenommen haben, klicken Sie auf **Alle Änderungen rückgängig machen**. Die Werte werden auf die vorherigen Einstellungen zurückgesetzt.

Telefonbereitstellungsverfahren

In der Regel wird das Cisco IP Phone so konfiguriert, dass die Bereitstellung beim Herstellen der ersten Verbindung mit dem Netzwerk erfolgt. Das Telefon wird auch in den geplanten Intervallen bereitgestellt, die vom Serviceanbieter oder VAR bei der Vorabbereitstellung (Konfiguration) des Telefons festgelegt werden. Serviceanbieter können VARs oder erfahrene Benutzer autorisieren, das Telefon manuell mithilfe des Tastenfelds bereitzustellen. Die Bereitstellung kann auch mit der Webbenutzeroberfläche des Telefons konfiguriert werden.

Aktivieren Sie **Status** > **Telefonstatus** > **Bereitstellung** in der LCD-Benutzeroberfläche des Telefons oder die Option „Bereitstellungsstatus“ auf der Registerkarte **Status** des webbasierten Konfigurationsprogramms.

Verwandte Themen

Manuelle Bereitstellung eines Telefons über das Tastenfeld, auf Seite 11

Auf Ihrem Telefon mit dem Aktivierungscode

Diese Funktion ist in der Firmware-Version 11-2-3MSR1, BroadWorks Application Server Version 22.0 (Patch AP.as. 22.0.1123. ap368163 und deren Abhängigkeiten) verfügbar. Sie können jedoch Telefone mit älterer Firmware ändern, um diese Funktion zu verwenden. Sie teilen dem Telefon mit, auf die neue Firmware zu aktualisieren und die `GDS://` Profilregel zu verwenden, um den Aktivierungscode-Bildschirm auszulösen. Ein Benutzer gibt einen 16-stelligen Code im bereitgestellten Feld automatisch auf dem Telefon ein.

Hinweis Multiplattform-Telefone der Cisco IP Phone 6861-Serie unterstützt den Onboard-Aktivierungscode nicht.

Vorbereitungen

Stellen Sie sicher, dass der activation.webex.com-Dienst über die Firewall die Onboarding-Aktivierung über den Aktivierungscode unterstützt.

Prozedur

Schritt 1 Bearbeiten Sie die Telefondatei config.xml in einem Text- oder XML-Editor.

Schritt 2 Befolgen Sie das folgende Beispiel in Ihrer Datei config.xml, um die Profilregel für das Aktivierungscode-Onboarding festzulegen.

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

Schritt 3 Speichern Sie die Änderungen an der Datei config.xml.

Manuelle Bereitstellung eines Telefons über das Tastenfeld

Prozedur

Schritt 1 Drücken Sie **Anwendungen** .

Schritt 2 Wählen Sie **Geräteadministration** > **Profilregel** aus.

Schritt 3 Geben Sie die Profilregel im folgenden Format ein:

```
protocol://server[:port]/profile_pathname
```

Zum Beispiel:

```
tftp://192.168.1.5/CP_x8xx_MPP.cfg
```

Wenn kein Protokoll angegeben ist, wird TFTP verwendet. Wenn kein Servername angegeben ist, wird der Host, der die URL anfordert, als Servername verwendet. Wenn kein Port angegeben ist, wird der Standardport verwendet (69 für TFTP, 80 für HTTP oder 443 für HTTPS).

Schritt 4 Drücken Sie **NeuSync**.

Verwandte Themen

Telefonbereitstellungsverfahren, auf Seite 10

Peer-Firmware-Freigabe

Peer-Firmware-Freigabe (PFS) ist ein Firmware-Verteilungsmodell, bei dem ein Cisco IP Phone andere Telefone gleichen Modells oder gleicher Serie im Subnetz finden und aktualisierte Firmware-Dateien für diese freigeben kann, wenn Sie mehrere Telefone gleichzeitig aktualisieren möchten. PFS verwendet das Cisco-eigene Protokoll Cisco Peer-to-Peer-Distribution Protocol (CPPDP). Mit CPPDP bilden alle Geräte im Subnetz eine Peer-zu-Peer-Hierarchie und kopieren dann die Firmware oder andere Dateien von Peer-Geräten an die benachbarten Geräte. Um Firmware-Upgrades zu optimieren, lädt ein Stamm-Telefon das Firmware-Image vom Softwarespeicherserver herunter und übergibt dann die Firmware über TCP-Verbindungen an andere Telefone im Subnetz.

Peer-Firmware-Freigabe:

- Beschränkt Überlastungen bei TFTP-Übertragungen an zentrale Remote-Softwarespeicherserver.
- Firmware-Updates müssen nicht mehr manuell gesteuert werden.
- Reduziert die Ausfallzeiten der Telefone während Updates, wenn zahlreiche Telefone gleichzeitig zurückgesetzt werden.

Hinweis

- Peer-Firmware-Freigabe ist nur funktionsfähig, wenn mehrere Telefone auf zeitgleiches Aktualisieren festgelegt sind. Wenn ein NOTIFY mit Event:resync gesendet wird, wird eine Resynchronisierung auf dem Telefon ausgelöst. Beispiel einer XML-Datei, die die Konfigurationen zum Initiieren eines Updates enthalten kann:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Beim Festlegen der Peer-Firmware-Freigabe-Log-Server auf-IP-Adresse und einen Port werden PFS-spezifische Protokolle als UDP-Nachrichten an diesen Server gesendet. Diese Einstellung muss auf jedem Telefon vorgenommen werden. Sie können dann die Protokollnachrichten bei der Behebung von Problemen im Zusammenhang mit PFS verwenden.

Peer_Firmware_Sharing_Log_Server gibt den Host-Namen und den Port des UDP-Remote-Syslog-Servers an. Der Port ist standardmäßig auf den Standard-Syslog 514 festgelegt.

Zum Beispiel:

```
<Peer_Firmware_Sharing_Log_Server>192.168.5.5</ Peer_Firmware_Sharing_Log_Server>
```

Um diese Funktion zu verwenden, aktivieren Sie PFS auf den Telefonen.

Umgehen des Bildschirms „Kennwort festlegen“

Sie können den Bildschirm **Kennwort festlegen** des Telefons beim ersten Start oder nach dem Zurücksetzen auf die Werkseinstellungen umgehen, basierend auf diesen Bereitstellungsaktionen:

- DHCP-Konfiguration
- EDOS-Konfiguration
- Benutzerkennwort-Konfiguration mithilfe der XML-Konfigurationsdatei des Telefons.

Tabelle 1: Bereitstellungsaktionen, die die Anzeige des Bildschirms „Kennwort festlegen“ bestimmen

Konfigurierte DHCP	Konfigurierte EDOS	Konfiguriertes Benutzerkennwort	Bildschirm „Kennwort festlegen“ umgehen
Ja	n/z	Ja	Ja
Ja	n/z	Nein	**Nein**
Nein	Ja	Ja	Ja
Nein	Ja	Nein	**Nein**
Nein	Nein	n/z	**Nein**

Prozedur

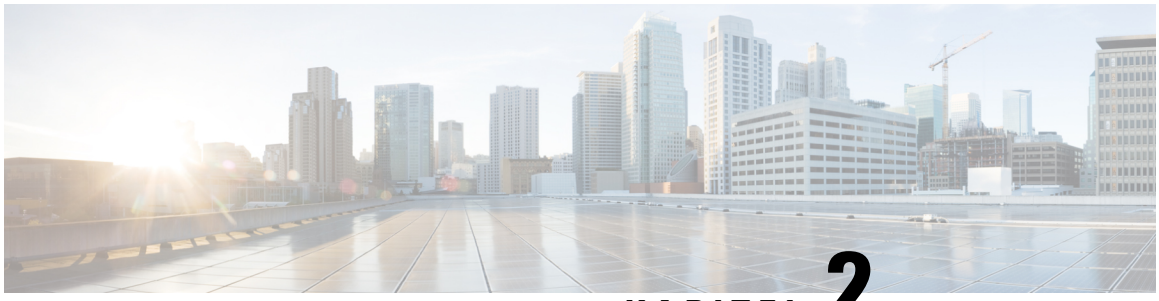
Schritt 1 Bearbeiten Sie die `cfg.xml`-Datei des Telefons in einem Text- oder XML-Editor.

Schritt 2 Fügen Sie das Tag **<User_Password>** mit einer der folgenden Optionen ein.

- **Kein Kennwort (Start- und End-Tag)** – **<User_Password></User_Password>**
- **Kennwortwert (4 bis 127 Zeichen)**–**<User_Password ua="rw">Abc123</User_Password>**
- **Kein Kennwort (nur Start-Tag)**–**<User_Password />**

Schritt 3 Speichern Sie die Änderungen in der Datei `cfg.xml`.

Der Bildschirm **Kennwort festlegen** wird beim ersten Start oder nach dem Zurücksetzen auf die Werkseinstellungen nicht angezeigt. Wenn ein Kennwort angegeben ist, wird der Benutzer zur Eingabe des Kennworts aufgefordert, wenn er auf die Telefon-Webseite oder auf die Menüs des Telefonbildschirms zugreift.



KAPITEL 2

Bereitstellungsformate

Bereitstellungsskripts

Das Telefon kann im XML-Format konfiguriert werden.

Detaillierte Informationen zu Ihrem Telefon finden Sie im Administratorhandbuch für Ihr Gerät. In allen Handbüchern werden die Parameter beschrieben, die über den Verwaltungswebserver konfiguriert werden können.

Konfigurationsprofil-Formate

Im Konfigurationsprofil werden die Parameterwerte für das Telefon definiert.

Für das XML-Format des Konfigurationsprofils werden Standard-XML-Entwicklungstools verwendet, um die Parameter und Werte zu kompilieren.

Hinweis Es wird nur der UTF-8-Zeichensatz unterstützt. Wenn Sie das Profil in einem Editor bearbeiten, ändern Sie das Verschlüsselungsformat nicht, ansonsten wird die Datei vom Telefon nicht erkannt.

Jedes Telefon verfügt über einen anderen Funktionssatz und somit auch über einen anderen Parametersatz.

Profil im XML-Format (XML)

Das Open-Format-Profil ist eine Textdatei mit einer XML-ähnlichen Syntax in einer Hierarchie von Elementen mit Elementattributen und Werten. Mit diesem Format können Sie Standardtools verwenden, um die Konfigurationsdatei zu erstellen. Eine Konfigurationsdatei in diesem Format kann während eines

Resynchronisierungsvorgangs vom Bereitstellungsserver an das Telefon gesendet werden. Die Datei kann ohne Kompilierung als binäres Objekt gesendet werden.

Das Telefon unterstützt Konfigurationsformate, die von Standardtools generiert werden. Diese Funktion erleichtert die Entwicklung von Back-End-Bereitstellungsserver-Software, mit der Konfigurationsprofile aus vorhandenen Datenbanken generiert werden.

Um vertrauliche Informationen im Konfigurationsprofil zu schützen, übermittelt der Bereitstellungsserver diese Art von Datei über einen durch TLS geschützten Kanal an das Telefon. Optional kann die Datei mithilfe des gzip-Deflate-Algorithmus (RFC1951) komprimiert werden.

Die Datei kann mit einer der folgenden Verschlüsselungsmethoden verschlüsselt werden:

- AES-256-CBC-Verschlüsselung
- RFC-8188-basierte HTTP-Inhaltsverschlüsselung mit AES-128-GCM-Schlüssel

Beispiel: Open-Format-Profil

```
<flat-profile>
<Resync_On_Reset> Yes </Resync_On_Reset>
<Resync_Periodic> 7200 </Resync_Periodic>
<Profile_Rule> tftp://prov.telco.com:6900/cisco/config/CP_xxxx_MPP.cfg</Profile_Rule>
</flat-profile>
```

Das Element-Tag <flat-profile> umfasst alle Parameterelemente, die vom Telefon erkannt werden.

Verwandte Themen

Open-Format-Profil (XML) – Komprimierung und Verschlüsselung, auf Seite 20

Komponenten der Konfigurationsdatei

Eine Konfigurationsdatei kann die folgenden Komponenten enthalten:

- Element-Tags
- Attribute
- Parameter
- Formatierungsfunktionen
- XML-Kommentare

Eigenschaften der Element-Tags

- Das XML-Bereitstellungsformat und die Webbenutzeroberfläche ermöglichen die Konfiguration der gleichen Einstellungen. Der Name des XML-Tags und die Feldnamen in der Webbenutzeroberfläche ähneln sich, können aber aufgrund der Beschränkungen beim XML-Elementnamen variieren. Beispielsweise werden Unterstriche (_) anstelle von Anführungszeichen („ “) verwendet.
- Das Telefon erkennt Elemente mit ordnungsgemäßen Parameternamen, die im speziellen Element <flat-profile> enthalten sind.

- Elementnamen werden in spitze Klammern gesetzt.
- Die meisten Elementnamen ähneln den Feldnamen auf den Verwaltungswebseiten für das Gerät, wobei die folgenden Modifikationen gelten:
  - Elementnamen dürfen keine Leerzeichen oder Sonderzeichen enthalten. Um den Elementnamen aus dem Verwaltungs-Web-Feldnamen abzuleiten, ersetzen Sie alle Leerzeichen oder Sonderzeichen durch einen Unterstrich `[`, `]`, `(`, `)` oder `/`.

    Beispiel: Das Element <Resync_On_Reset> steht für das Feld **Erneute Synchronisierung nach Neustart**.
  - Jeder Elementname muss eindeutig sein. Auf den Verwaltungswebseiten können die gleichen Felder auf mehreren Webseiten angezeigt werden, z. B. die Seiten „Leitung“, „Benutzer“ und „Durchwahl“. Hängen Sie `[n]` an den Elementnamen an, um die Nummer anzugeben, die auf der Registerkarte „Seite“ angezeigt wird.

    Beispiel: Das Element <Dial_Plan_1_> steht für den **Rufnummernplan** für Leitung 1.
- Jedes öffnende Element-Tag muss über ein entsprechendes schließendes Element-Tag verfügen. Beispiel:

```
<flat-profile>
<Resync_On_Reset> Yes
  </Resync_On_Reset>
<Resync_Periodic> 7200
  </Resync_Periodic>
<Profile_Rule>tftp://prov.telco.com: 6900/cisco/config/CP_xxxx_MPP.cfg
  </Profile_Rule>
</flat-profile>
```

- Bei Element-Tags wird die Groß-/Kleinschreibung beachtet.
- Leere Element-Tags sind zulässig und werden als Wert ohne Konfiguration interpretiert. Geben Sie das öffnende Element-Tag ohne ein entsprechendes Element-Tag ein, und fügen Sie ein Leerzeichen und einen Vorwärtsschrägstrich vor der schließenden spitzen Klammer (>) ein. In diesem Beispiel ist Profilregel B leer:

```
<Profile_Rule_B />
```

- Ein leeres Element-Tag kann verwendet werden, um zu verhindern, dass die während einer Resynchronisierung durch einen Benutzer eingegebenen Werte überschrieben werden. Im folgenden Beispiel bleiben die Kurzwahleinstellungen für Benutzer unverändert:

```
<flat-profile>
<Speed_Dial_2_Name ua="rw"/>
<Speed_Dial_2_Number ua="rw"/>
<Speed_Dial_3_Name ua="rw"/>
<Speed_Dial_3_Number ua="rw"/>
<Speed_Dial_4_Name ua="rw"/>
<Speed_Dial_4_Number ua="rw"/>
<Speed_Dial_5_Name ua="rw"/>
<Speed_Dial_5_Number ua="rw"/>
<Speed_Dial_6_Name ua="rw"/>
<Speed_Dial_6_Number ua="rw"/>
<Speed_Dial_7_Name ua="rw"/>
<Speed_Dial_7_Number ua="rw"/>
<Speed_Dial_8_Name ua="rw"/>
<Speed_Dial_8_Number ua="rw"/>
<Speed_Dial_9_Name ua="rw"/>
```

```
<Speed_Dial_9_Number ua="rw"/>
</flat-profile>
```

- Verwenden Sie einen leeren Wert, um den entsprechenden Parameter auf eine leere Zeichenfolge festzulegen. Geben Sie ein öffnendes und ein schließendes Element ohne Wert ein. Im folgenden Beispiel wird der Parameter GPP_A auf eine leere Zeichenfolge festgelegt.

```
<flat-profile>
<GPP_A>
  </GPP_A>
</flat-profile>
```

- Nicht erkannte Elementnamen werden ignoriert.

Verwandte Themen

Konfigurationszugriffssteuerung, auf Seite 9

Attribut für Benutzerzugriff

Die Steuerelemente für das Benutzerzugriffsattribut (**ua**) können verwendet werden, um den Zugriff durch das Benutzerkonto zu ändern. Wenn das Attribut **ua** nicht festgelegt ist, wird die vorhandene Einstellung für den Benutzerzugriff beibehalten. Dieses Attribut wirkt sich nicht auf den Zugriff durch das Administratorkonto aus.

Das Attribut **ua** muss, sofern es vorhanden ist, einen der folgenden Werte haben:

- na: Kein Zugriff
- ro: Schreibgeschützt
- rw: Lesen/Schreiben

Im folgenden Beispiel wird das Attribut **ua** dargestellt:

```
<flat-profile>
   <SIP_TOS_DiffServ_Value_1_ ua=”na”/>
   <Dial_Plan_1_ ua=”ro”/>
   <Dial_Plan_2_ ua=”rw”/>
</flat-profile>
```

Der Wert der Option **ua** muss von doppelten Anführungszeichen umschlossen sein.

Zugriffskontrolle

Wenn der Parameter <Phone-UI-User-Mode> aktiviert ist, wird in der GUI des Telefons das Attribut für den Benutzerzugriff der relevanten Parameter beachtet, wenn die GUI für ein Menüelement steht.

Für Menüeinträge, die einem einzelnen Konfigurationsparameter zugeordnet sind:

- Die Bereitstellung des Parameters mit dem Attribut „ua=na“ („ua“ steht für „Benutzerzugriff“) führt dazu, dass der Eintrag ausgeblendet wird.
- Bei Bereitstellung des Parameters mit dem Attribut „ua=ro“ wird der Eintrag schreibgeschützt und kann nicht bearbeitet werden.

Für Menüeinträge, die mehreren Konfigurationsparametern zugeordnet sind:

- Die Bereitstellung aller betroffenen Parameter mit dem Attribut „ua=na“ führt dazu, dass die Einträge ausgeblendet werden.

Verwandte Themen

Konfigurationszugriffssteuerung, auf Seite 9

Parametereigenschaften

Diese Eigenschaften gelten für die Parameter:

- Alle Parameter, die von keinem Profil festgelegt sind, bleiben auf dem Telefon unverändert.
- Nicht erkannte Parameter werden ignoriert.
- Wenn das Open-Format-Profil mehrere Vorkommen des gleichen Parameter-Tags enthält, überschreibt das letzte dieser Vorkommen alle früheren Vorkommen. Um ein versehentliches Überschreiben der Konfigurationswerte für einen Parameter zu vermeiden, wird empfohlen, dass in jedem Profil immer nur eine Instanz eines Parameters festgelegt wird.
- Das zuletzt verarbeitete Profil hat Vorrang. Wenn in mehreren Profilen der gleiche Konfigurationsparameter angeben ist, hat der Wert des letzten Profils Vorrang.

Formate der Zeichenfolge

Die folgenden Eigenschaften gelten für die Formatierung von Zeichenfolgen:

- Kommentare sind über die standardmäßige XML-Syntax zulässig.

```
<!-- My comment is typed here -->
```

- Vor- und nachstehende Leerzeichen sind für bessere Lesbarkeit zulässig, werden jedoch aus dem Parameterwert entfernt.
- Neue Zeilen in einem Wert werden in Leerzeichen konvertiert.
- Ein XML-Header in Form von `<? ?>` ist zulässig, wird jedoch vom Telefon ignoriert.
- Verwenden Sie zum Eingeben von Sonderzeichen grundlegende XML-Escape-Zeichen, wie in der folgenden Tabelle dargestellt.

Sonderzeichen	XML-Escape-Sequenz
& (Und-Zeichen)	&
< (kleiner als)	<
> (größer als)	>
' (Apostroph)	'
“ (doppelte Anführungszeichen)	"

Im folgenden Beispiel werden die Escape-Zeichen eingegeben, um die Symbole für Größer als und Kleiner als darzustellen, die in einer Rufnummernplan-Regel erforderlich sind. In diesem Beispiel wird ein Rufnummernplan für eine Informationshotline definiert, bei dem der Parameter <Dial_Plan_1_> (**Administratoranmeldung** > **Erweitert** > **Sprache** > **Nebenstelle (n)**) gleich (S0 <:18005551212>) festgelegt ist.

```
<flat-profile>
 <Dial_Plan_1_>
  (S0 <:18005551212>)
 </Dial_Plan_1_>
</flat-profile>
```

- Numerische Escape-Zeichen, in denen Dezimal- und Hexadezimalwerte verwendet werden (z. B. (und .), sind übersetzt.
- Die Telefon-Firmware unterstützt nur ASCII-Zeichen.

Open-Format-Profil (XML) – Komprimierung und Verschlüsselung

Das Open-Format-Konfigurationsprofil kann komprimiert werden, um die Netzwerkbelastung auf dem Bereitstellungsserver zu reduzieren. Das Profil kann auch zum Schutz von vertraulichen Informationen verschlüsselt werden. Die Komprimierung ist nicht erforderlich, muss jedoch vor der Verschlüsselung erfolgen.

Verwandte Themen

Konfigurationsprofil-Formate, auf Seite 15

Open-Format-Profil – Komprimierung

Die unterstützte Komprimierungsmethode ist der gzip-Deflate-Algorithmus (RFC1951). Das gzip-Utility und die Komprimierungsbibliothek, die den gleichen Algorithmus (zlib) implementiert, stehen im Internet zur Verfügung.

Um die Komprimierung ermitteln zu können, erwartet das Telefon, dass die komprimierte Datei einen gzip-kompatiblen Header enthält. Durch Aufruf des gzip-Utility im ursprünglichen Open-Format-Profil wird der Header generiert. Die heruntergeladene Header-Datei wird vom Telefon überprüft, um das Dateiformat zu bestimmen.

Wenn beispielsweise `profile.xml` ein gültiges Profil ist, wird die Datei `profile.xml.gz` ebenfalls akzeptiert. Dieser Profiltyp kann über einen der folgenden Befehle generiert werden:

- `>gzip profile.xml`

  Ersetzt die Originaldatei durch die komprimierte Datei.

- `>cat profile.xml | gzip > profile.xml.gz`

  Belässt die Originaldatei und erstellt eine neue komprimierte Datei.

Ein Tutorial zur Komprimierung steht im Abschnitt Offenes Profil mit Gzip komprimieren, auf Seite 65 zur Verfügung.

Verwandte Themen

Offenes Profil mit Gzip komprimieren, auf Seite 65

Open-Format-Profil – Verschlüsselung

Die symmetrische Verschlüsselung kann verwendet werden, um ein Open-Format-Konfigurationsprofil zu verschlüsseln, unabhängig davon, ob die Datei komprimiert ist. Die Komprimierung muss, soweit sie angewendet wird, vor der Verschlüsselung durchgeführt werden.

Der Bereitstellungsserver verwendet HTTPS, um die anfängliche Bereitstellung des Telefons nach der Einrichtung abzuwickeln. Die Offline-Vorverschlüsselung von Konfigurationsprofilen ermöglicht die anschließende Verwendung von HTTP für die Resynchronisierung von Profilen. Dadurch wird die Belastung des HTTP-Servers in großen Bereitstellungen reduziert.

Das Telefon unterstützt zwei Methoden zur Verschlüsselung für Konfigurationsdateien:

- AES-256-CBC-Verschlüsselung
- RFC-8188-basierte HTTP-Inhaltsverschlüsselung mit AES-128-GCM-Schlüssel

Der Schlüssel oder das Input Keying Material (IKM) muss zuvor für das Gerät bereitgestellt worden sein. Bootstrapping des Geheimschlüssels kann über HTTPS sicher erfolgen.

Der Konfigurationsdateiname erfordert kein bestimmtes Format, aber ein Dateiname, der mit der Erweiterung `.cfg` endet, gibt normalerweise ein Konfigurationsprofil an.

AES-256-CBC-Verschlüsselung

Das Telefon unterstützt die AES-256-CBC-Verschlüsselung für Konfigurationsdateien.

Das OpenSSL-Verschlüsselungstool kann von verschiedenen Internetseiten heruntergeladen und für die Verschlüsselung verwendet werden. Zur Unterstützung der 256-Bit-AES-Verschlüsselung ist möglicherweise eine erneute Kompilierung des Tools zur Aktivierung des AES-Codes erforderlich. Die Firmware wurde mit Version openssl-0.9.7c getestet.

Ein Profil mit OpenSSL verschlüsseln, auf Seite 66 bietet ein Tutorial zur Verschlüsselung.

Bei einer verschlüsselten Datei erwartet das Profil, dass die Datei dasselbe Format aufweist wie bei der Generierung mit dem folgenden Befehl:

```
# example encryption key = SecretPhrase1234

openssl enc –e –aes-256-cbc –k SecretPhrase1234 –in profile.xml –out profile.cfg

# analogous invocation for a compressed xml file

openssl enc –e –aes-256-cbc –k SecretPhrase1234 –in profile.xml.gz –out profile.cfg
```

Ein kleingeschriebenes -k steht vor dem Geheimschlüssel; dies kann eine beliebige Nur-Text-Phrase sein und wird verwendet, um einen 64-Bit-Zufallssalt zu generieren. Mit dem durch das -k-Argument angegeben Geheimnis leitet das Verschlüsselungstool einen zufälligen 128-Bit-Anfangsvektor und den tatsächlichen 256-Bit-Verschlüsselungscode ab.

Wenn diese Form der Verschlüsselung in einem Konfigurationsprofil verwendet wird, muss das Telefon den geheimen Schlüsselwert erhalten, um die Datei entschlüsseln zu können. Dieser Wert wird als Qualifizierer in der URL für das Profil angegeben. Die Syntax lautet unter Verwendung einer expliziten URL wie folgt:

```
[--key "SecretPhrase1234"] http://prov.telco.com/path/profile.cfg
```

Dieser Wert wird mithilfe eines der Profile_Rule-Parameter programmiert.

Verwandte Themen

Ein Profil mit OpenSSL verschlüsseln, auf Seite 66

Makroerweiterung

Mehrere Bereitstellungsparameter werden intern vor der Auswertung einer Makroerweiterung unterzogen. Dieser Vorbewertungsschritt bietet mehr Flexibilität bei der Steuerung der Resynchronisierung des Telefons und der Upgrade-Aktivitäten.

Die folgenden Parametergruppen werden vor der Auswertung einer Makroerweiterung unterzogen:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

Unter bestimmten Umständen werden einige allgemeine Parameter (GPP_*) auch einer Makroerweiterung unterzogen. Dies wird explizit in Optionale Argumente für die Resynchronisierung, auf Seite 25 angegeben.

Während der Makroerweiterung ersetzen die Inhalte der benannten Variablen die Ausdrücke der Form $NAME und $(NAME). Diese Variablen umfassen allgemeine Parameter, mehrere Produktbezeichner, bestimmte Ereignistimer und Bereitstellungsstatus-Werte. Eine vollständige Liste finden Sie im Makroerweiterungsvariablen, auf Seite 79.

Im folgenden Beispiel wird der Ausdruck $(MAU) verwendet, um die MAC-Adresse 000E08012345 einzufügen.

Der Administrator gibt Folgendes ein: **`$(MAU)config.cfg`**

Die resultierende Makroerweiterung für ein Gerät mit der MAC-Adresse 000E08012345 lautet: `000E08012345config.cfg`

Wenn ein Makroname nicht erkannt wird, wird er nicht erweitert. Der Name STRANGE wird beispielsweise nicht als gültiger Makroname erkannt, während MAU als gültiger Makroname erkannt wird.

Der Administrator gibt Folgendes ein: **`$STRANGE$MAU.cfg`**

Die resultierende Makroerweiterung für ein Gerät mit der MAC-Adresse 000E08012345 lautet: `$STRANGE000E08012345.cfg`

Eine Makroerweiterung wird nicht rekursiv angewendet. $$MAU" wird beispielsweise in $MAU" erweitert ($$ wird erweitert) und nicht in die MAC-Adresse.

Der Inhalt der speziellen Parameter GPP_SA bis GPP_SD wird den Makroausdrücken $SA bis $SD zugeordnet. Für diese Parameter wird die Makroerweiterung nur als Argument der Optionen **--key** , **--uid** und **--pwd** in einer Resynchronisierungs-URL durchgeführt.

Bedingungsausdrücke

Bedingungsausdrücke können Resynchronisierungsereignisse auslösen und alternative URLs für die Resynchronisierung und Upgrade-Vorgänge auswählen.

Bedingungsausdrücke bestehen aus einer Liste von Vergleichen, getrennt durch den Operator **and**. Alle Vergleiche müssen erfüllt werden, damit für die Bedingung „True“ ausgegeben wird.

Jeder Vergleich kann sich auf eine der folgenden drei Arten von Buchstabensymbolen beziehen:

- Ganzzahlige Werte
- Software- oder Hardware-Versionsnummern
- Zeichenfolgen in doppelten Anführungszeichen

Versionsnummern

Die formale Software-Version von Multiplattform-Telefonen verwendet dieses Format, dabei ist BN die Build-Nummer:

- Cisco IP Phone 6800-Serie: `sip68xx.v1-v2-v3MPP-BN`

In der Vergleichszeichenfolge muss dasselbe Format verwendet werden. Andernfalls führt dies zu einem Format-Analysefehler.

In der Software-Version kann v1-v2-v3-v4 unterschiedliche Ziffern und Zeichen angeben, muss aber mit einer Ziffer beginnen. Beim Vergleich der Software-Version wird v1-v2-v3-v4 nacheinander abgeglichen; dabei haben die am weitesten links stehenden Ziffern Vorrang vor den anderen Ziffern.

Wenn v[x] nur Ziffern umfasst, werden die Ziffern miteinander verglichen; wenn v[x] Ziffern und Buchstaben umfasst, werden zuerst die Ziffern und dann die Buchstaben in alphabetischer Reihenfolge verglichen.

Beispiel für eine gültige Versionsnummer

sipyyyy.11-0-0MPP-BN

Im Gegensatz dazu ist 11.0.0 ein ungültiges Format.

Vergleich

sip68xx.11-0-0MPP-BN < sip68xx.11-0-1MPP-BN

Zeichenfolgen in Anführungszeichen können auf Gleichheit oder Ungleichheit verglichen werden. Ganzzahlen und Versionsnummern können auch arithmetisch verglichen werden. Die Vergleichsoperatoren können als Symbole oder als Akronyme angegeben werden. Akronyme eignen sich für die Bedingung in einem Open-Format-Profil.

Operator	Alternative Syntax	Beschreibung	Gilt für Ganzzahl- und Versions-Operanden	Gilt für Operanden von Zeichenfolgen in Anführungszeichen
=	eq	ist gleich	Ja	Ja
!=	ne	ist ungleich	Ja	Ja
<	lt	kleiner als	Ja	Nein
<=	le	kleiner oder gleich	Ja	Nein
>	gt	größer als	Ja	Nein

Operator	Alternative Syntax	Beschreibung	Gilt für Ganzzahl- und Versions-Operanden	Gilt für Operanden von Zeichenfolgen in Anführungszeichen
>=	ge	größer oder gleich	Ja	Nein
UND		und	Ja	Ja

Es ist wichtig, Makrovariablen in doppelte Anführungszeichen zu setzen, wenn ein Buchstabensymbol einer Zeichenfolge erwartet wird. Wenn eine Zahl oder Versionsnummer erwartet wird, sollten Sie nicht so vorgehen.

Bei Verwendung in Zusammenhang mit den Parametern Profile_Rule* und Upgrade_Rule müssen Bedingungsausdrücke in der Syntax „(expr)?“ wie in diesem Beispiel für eine Upgrade-Regel integriert werden. Denken Sie daran, dass BN die Build-Nummer angibt.

```
($SWVER ne sip68xx.11-0-0MPP)? http://ps.tell.com/sw/sip68xx.11-0-0MPP-BN.loads
```

Verwenden Sie die vorstehende Syntax nicht mit Klammern zur Konfiguration der Resync_Trigger_*-Parameter.

URL-Syntax

Verwenden Sie die Standard-URL-Syntax, um anzugeben, wie Konfigurationsdateien und Firmware jeweils in den Parametern Profile_Rule* und Upgrade_Rule abgerufen werden. Die Syntax lautet wie folgt:

[scheme://] [server [:port]] filepath

Wobei **scheme** einer der folgenden Werte ist:

- tftp
- http
- https

Wenn **scheme** nicht angegeben wird, wird TFTP angenommen. Der Server kann ein DNS-anerkannter Host-Name oder eine numerische IP-Adresse sein. Der Port ist die Ziel-UDP- oder -TCP-Portnummer. Der Dateipfad muss mit dem Stammverzeichnis (/) beginnen. Es muss sich um einen absoluten Pfad handeln.

Wenn **server** nicht angegeben wird, wird der über DHCP (Option 66) angegebene TFTP-Server verwendet.

Hinweis Für Upgrade-Regeln muss der Server angegeben werden.

Wenn **port** nicht angegeben wird, wird der Standard-Port für das angegebene Schema verwendet. TFTP verwendet UDP-Port 69, HTTP verwendet TCP-Port 80, HTTPS verwendet TCP-Port 443.

Es muss ein Dateipfad vorhanden sein. Dieser muss nicht unbedingt zu einer statischen Datei verweisen, sondern kann dynamischen Inhalt angeben, der über CGI abgerufen wird.

Die Makroerweiterung gilt innerhalb von URLs. Im Folgenden erhalten Sie Beispiele für gültige URLs:

```
/$MA.cfg
/cisco/cfg.xml
192.168.1.130/profiles/init.cfg
tftp://prov.call.com/cpe/cisco$MA.cfg
http://neptune.speak.net:8080/prov/$D/$E.cfg
https://secure.me.com/profile?Linksys
```

Beim Verwenden der DHCP-Option 66 wird die leere Syntax nicht von der Upgrade-Regel unterstützt. Dies gilt nur für Profile Rule*.

RFC-8188-basierte HTTP-Inhaltsverschlüsselung

Das Telefon unterstützt die RFC 8188-basierte HTTP-Inhaltsverschlüsselung mit AES-128-GCM-Schlüssel für Konfigurationsdateien. Mit dieser Verschlüsselungsmethode kann jede Entität die HTTP-Nachrichten-Header lesen. Nur die Entitäten, die das Input Keying Material (IKM) kennen, können die Nutzlast lesen. Wenn das Telefon mit dem IKM bereitgestellt wird, können das Telefon und der Bereitstellungsserver Konfigurationsdateien sicher austauschen und Netzwerkelementen von Drittanbietern gleichzeitig ermöglichen, die Nachrichten-Header zu Analyse- und Überwachungszwecken zu verwenden.

Der XML-Konfigurationsparameter **IKM_HTTP_Encrypt_Content** enthält das IKM auf dem Telefon. Aus Sicherheitsgründen ist dieser Parameter nicht auf der Webseite der Telefon-Verwaltung zugänglich. Er ist ebenfalls nicht in der Konfigurationsdatei des Telefons sichtbar, auf die Sie über die IP-Adresse des Telefons oder über die Konfigurationsberichte des Telefons zugreifen können, die an den Bereitstellungsserver gesendet werden.

Wenn Sie die RFC 8188-basierte Verschlüsselung verwenden, stellen Sie Folgendes sicher:

- Stellen Sie das Telefon mit dem IKM bereit, indem Sie das IKM mit dem XML-Parameter **IKM_HTTP_Encrypt_Content** in der Konfigurationsdatei angeben, die vom Bereitstellungsserver an das Telefon gesendet wird.
- Wenn diese Verschlüsselung auf die vom Bereitstellungsserver an das Telefon gesendeten Konfigurationsdateien angewendet wird, stellen Sie sicher, dass der HTTP-Header der *Inhalts-Codierung* in der Konfigurationsdatei „aes128gcm“ aufweist.

  Ohne diesen Header erhält die AES-256-CBC-Methode Vorrang. Das Telefon wendet, ungeachtet des IKM, die AES-256-CBC-Entschlüsselung an, wenn ein AES-256-Schlüssel in einer Profilregel vorhanden ist.
- Wenn das Telefon diese Verschlüsselung auf die Konfigurationsberichte anwenden soll, die es an den Bereitstellungsserver sendet, stellen Sie sicher, dass kein AES-256-CBC-Schlüssel in der Berichtsregel angegeben ist.

Optionale Argumente für die Resynchronisierung

Die optionalen Argumente **key**, **uid** und **pwd** können vor den URLs stehen, die in den Profile_Rule*-Parametern eingegeben werden, und müssen insgesamt von eckigen Klammern umschlossen sein.

Schlüssel

Die **--Schlüssel**-Option weist das Telefon darauf hin, dass die Konfigurationsdatei, die es vom Bereitstellungsserver empfängt, mit der AES-256-CBC-Verschlüsselung verschlüsselt ist, es sei denn, der Header *Inhalts-Codierung* in der Datei gibt die Verschlüsselung „aes128gcm“ an. Der Schlüssel selbst wird

als Zeichenfolge angegeben, die auf den Begriff **--key** folgt. Der Schlüssel kann optional in Anführungszeichen (") eingeschlossen werden. Das Telefon verwendet den Schlüssel, um die Konfigurationsdatei zu entschlüsseln.

Beispiele für die Verwendung

```
[--key VerySecretValue]
[--key "my secret phrase"]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

Für die optionalen Argumente in Klammern wird eine Makroerweiterung durchgeführt. Die speziellen Parameter GPP_SA bis GPP_SD werden nur per Makroerweiterung in die Makrovariablen $SA bis $SD umgewandelt, wenn sie als key-Optionsargumente verwendet werden. Siehe folgende Beispiele:

```
[--key $SC]
[--key "$SD"]
```

In Open-Format-Profilen muss das Argument für **--key** dem Argument für die **-k**-Option entsprechen, die **openssl** zugewiesen ist.

uid und pwd

Die Optionen **uid** und **pwd** können verwendet werden, um die Benutzer-ID- und Kennwort-Authentifizierung für die benannte URL anzugeben. Für die optionalen Argumente in Klammern wird eine Makroerweiterung durchgeführt. Die speziellen Parameter GPP_SA bis GPP_SD werden nur per Makroerweiterung in die Makrovariablen $SA bis $SD umgewandelt, wenn sie als key-Optionsargumente verwendet werden. Siehe folgende Beispiele:

```
GPP_SA = MyUserID
GPP_SB = MySecretPassword
```

[--uid $SA --pwd $SB] https://provisioning_server_url/path_to_your_config/your_config.xml

würde dann erweitert in:

[--uid MyUserID --pwdMySecretPassword]
https://provisioning_server_url/path_to_your_config/your_config.xml

Anwenden eines Profils auf das IP-Telefonie-Gerät

Nachdem Sie ein XML-Konfigurationsskript erstellt haben, muss es zur Anwendung an das Telefon übertragen werden. Um die Konfiguration zu übernehmen, können Sie die Konfigurationsdatei von einem TFTP-, HTTP- oder HTTPS-Server entweder mithilfe eines Webbrowsers oder mit dem cURL-Befehlszeilen-Utility auf das Telefon herunterladen.

Die Konfigurationsdatei auf das Telefon von einem TFTP-Server aus herunterladen

Führen Sie die folgenden Schritte aus, um die Konfigurationsdatei für eine TFTP-Serveranwendung auf Ihren PC herunterzuladen.

Prozedur

Schritt 1 Verbinden Sie Ihren PC mit dem Telefon-LAN.

Schritt 2 Führen Sie eine TFTP-Serveranwendung auf dem PC aus, und stellen Sie sicher, dass die Konfigurationsdatei im TFTP-Stammverzeichnis verfügbar ist.

Schritt 3 Geben Sie in einem Webbrowser die LAN-IP-Adresse des Telefons, die IP-Adresse des Computers, den Dateinamen und die Anmeldeinformationen ein. Verwenden Sie das folgende Format:

```
http://<WAN-IP-Adresse>/admin/resync?tftp://<PC-IP-Adresse>/<Dateiname>&xuser=admin&xpassword=<Kennwort>
```

Beispiel:

```
http://192.168.15.1/admin/resync?tftp://192.168.15.100/my_config.xml&xuser=admin&xpassword=admin
```

Die Konfigurationsdatei auf das Telefon mit cURL herunterladen

Führen Sie die folgenden Schritte aus, um die Konfiguration auf das Telefon unter Verwendung von cURL herunterzuladen. Dieses Befehlszeilentool wird verwendet, um Daten mit einer URL-Syntax zu übertragen. Hier können Sie cURL herunterladen:

https://curl.haxx.se/download.html

Hinweis Wir empfehlen, dass Sie cURL nicht verwenden, um die Konfiguration auf dem Telefon zu veröffentlichen, da der Benutzername und das Kennwort während der Verwendung von cURL nicht sicher sind.

Prozedur

Schritt 1 Verbinden Sie Ihren PC mit dem LAN-Port des Telefons.

Schritt 2 Laden Sie die Konfigurationsdatei auf das Telefon herunter, indem Sie den folgenden cURL-Befehl eingeben:

```
curl -d @my_config.xml
"http://192.168.15.1/admin/config.xml&xuser=admin&xpassword=admin"
```

Bereitstellungsparameter

In diesem Abschnitt werden die Bereitstellungsparameter grob nach Funktion sortiert erläutert:

Die folgenden Typen von Bereitstellungsparametern stehen zur Auswahl:

- Allgemeine Dienste
- Wirkung
- Kaufanreize

- Konfigurierbare Zeitpläne
- Profilregeln
- Upgrade Rule

Allgemeine Parameter

Die allgemeinen GPP_*-Parameter (**Administratoranmeldung** > **Erweitert** > **Sprache** > **Bereitstellung**) werden als freie Zeichenfolgen verwendet, die registriert werden, wenn das Telefon für die Interaktion mit einer bestimmten Bereitstellungsserverlösung konfiguriert wird. Die GPP_*-Parameter sind standardmäßig leer. Die Parameter können mit verschiedenen Werten konfiguriert werden:

- Verschlüsselungscodes
- URLs
- Statusinformationen für die mehrstufige Bereitstellung
- Vorlagen für POST-Anforderungen
- Zuordnungen von Parameter-Namensaliasen
- Teilweise Zeichenfolgenwerte, die in vollständige Parameterwerten zusammengefasst werden

Die GPP_*-Parameter stehen für eine Makroerweiterung in anderen Bereitstellungsparametern zur Verfügung. Daher sind Makronamen mit einem Großbuchstaben (A bis P) ausreichend, um den Inhalt der Parameter GPP_A bis GPP_P zu ermitteln. Außerdem werden mit den Makronamen mit zwei Großbuchstaben SA bis SD die Parameter GPP_SA bis GPP_SD als Sonderfall identifiziert, wenn sie als Argumente der folgenden URL Optionen verwendet werden:

key, **uid** und **pwd**

Sie können diese Parameter als Variablen in Bereitstellungs- und Upgrade-Regeln verwenden. Zur Referenzierung wird dem Variablennamen das Zeichen „$“ vorangestellt, z. B. $GPP_A.

Allgemeine Parameter verwenden

Wenn GPP_A beispielsweise die Zeichenfolge ABC und GPP_B die Zeichenfolge 123 enthält, wird für den Ausdruck AB die Makroerweiterung in ABC123 durchgeführt.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Prozedur

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

Schritt 2 Blättern Sie zum Abschnitt **Allgemeine Parameter**.

Schritt 3 Geben Sie gültige Werte in die Felder GPP A bis GPP P ein.

Schritt 4 Klicken Sie auf **Alle Änderungen übernehmen**.

Wirkung

Die Parameter Provision_Enable und Upgrade_Enable steuern alle Profilresynchronisierungs- und Firmware-Upgrade-Vorgänge. Resynchronisierungen und Upgrades werden unabhängig voneinander gesteuert. Außerdem werden mit diesen Parametern Resynchronisierungs- und Upgrade-URL-Befehle gesteuert, die über den Verwaltungswebserver erteilt werden. Diese beiden Parameter sind standardmäßig auf **Ja** festgelegt.

Der Parameter Resync_From_SIP steuert Anforderungen für Resynchronisierungsvorgänge. Ein SIP NOTIFY-Ereignis wird vom Serviceanbieter-Proxyserver an das Telefon gesendet. Wenn aktiviert, kann der Proxy eine Resynchronisierung anfordern. Hierzu sendet der Proxy eine SIP NOTIFY-Nachricht an das Gerät, die das Ereignis zum Resynchronisieren enthält.

Das Gerät gibt auf die Anforderung eine 401-Antwort (Autorisierung für verwendete Anmeldeinformationen abgelehnt) zurück. Das Gerät erwartet eine authentifizierte nachfolgende Anforderung, bevor es die Resynchronisierungsanforderung des Proxy akzeptiert. Mit den Headern Event: reboot_now und Event: restart_now werden kalte bzw. warme Neustarts durchgeführt, die ebenfalls geprüft werden.

Die beiden verbleibenden Enable-Parameter lauten Resync_On_Reset und Resync_After_Upgrade_Attempt. Diese Parameter bestimmen, ob das Gerät nach dem Neustart der Software und nach jedem Upgrade-Versuch einen Resynchronisierungsvorgang ausführt.

Wenn Resync_On_Reset aktiviert ist, führt das Gerät nach dem Startvorgang eine zufällige Verzögerung ein, bevor es zurückgesetzt wird. Die Verzögerung ist eine zufällige Zeitangabe bis zu dem Wert, der für Resync_Random_Delay (in Sekunden) angegeben ist. In einem Pool von Telefonen, die gleichzeitig eingeschaltet werden, werden durch diese Verzögerung die Startzeiten der Resynchronisierungsanforderungen der einzelnen Geräte besser verteilt. Diese Funktion kann bei einer großen lokalen Bereitstellung nützlich sein, wenn ein Stromausfall auftritt.

Kaufanreize

Das Telefon ermöglicht Ihnen die Resynchronisierung in bestimmten Zeitintervallen oder zu einem speziellen Zeitpunkt.

In bestimmten Zeitintervallen resynchronisieren

Das Telefon ist darauf ausgelegt, regelmäßig eine Resynchronisierung mit dem Bereitstellungsserver durchzuführen. Das Intervall für die Resynchronisierung wird im Parameter Resync_Periodic (in Sekunden) konfiguriert. Wenn dieser Wert leer ist, führt das Gerät keine regelmäßigen Resynchronisierungen aus.

Eine erneute Synchronisierung wird normalerweise ausgeführt, wenn die Sprachleitungen inaktiv sind. Wenn eine Sprachleitung aktiv und eine Resynchronisierung fällig ist, verzögert das Telefon die Resynchronisierung, bis die Leitung wieder inaktiv ist. Eine Resynchronisierung kann eine Änderung der Konfigurationsparameter verursachen.

Eine Resynchronisierung kann fehlschlagen, weil das Telefon kein Profil vom Server abrufen kann, die heruntergeladene Datei beschädigt ist oder ein interner Fehler aufgetreten ist. Das Gerät versucht, die Resynchronisierung nach einer Zeitspanne, die in Resync_Error_Retry_Delay (in Sekunden) angegeben ist, zu wiederholen. Wenn Resync_Error_Retry_Delay auf 0 festgelegt ist, führt das Gerät keine neue Resynchronisierung aus, nachdem eine Resynchronisierung fehlgeschlagen ist.

Wenn ein Upgrade fehlschlägt, wird nach den in Upgrade_Error_Retry_Delay angegebenen Sekunden ein erneuter Versuch ausgeführt.

Es stehen zwei konfigurierbare Parameter für die bedingte Auslösung einer Resynchronisierung zur Verfügung: Resync_Trigger_1 und Resync_Trigger_2. Jeder Parameter kann mit einem Bedingungsausdruck programmiert werden, der eine Makroerweiterung durchläuft. Wenn das Intervall für die Resynchronisierung abläuft (Zeit für die nächste Resynchronisierung), verhindern die Auslöser, sofern sie festgelegt sind, die Resynchronisierung, es sei denn, mindestens ein Auslöser wird mit „True“ bewertet.

Die folgende Beispielbedingung löst eine Resynchronisierung aus. Im Beispiel sind seit dem letzten Telefon-Upgrade-Versuch mehr als fünf Minuten (300 Sekunden) und seit dem letzten Resynchronisierungsversuch mindestens 10 Minuten (600 Sekunden) vergangen.

```
$UPGTMR gt 300 and $PRVTMR ge 600
```

Resynchronisierung zu einem speziellen Zeitpunkt

Der Parameter Resync_At ermöglicht es dem Telefon, zu einem bestimmten Zeitpunkt eine Resynchronisierung durchzuführen. Dieser Parameter verwendet das 24-Stunden-Format (hhmm), um die Zeit festzulegen.

Der Parameter Resync_At_Random_Delay ermöglicht es dem Telefon, mit einer nicht spezifizierten Verzögerung zu resynchronisieren. Dieser Parameter verwendet ein positives Ganzzahl-Format, um die Zeit festzulegen.

Es sollte vermieden werden, den Server mit Resynchronisierungsanforderungen von mehreren Telefonen zu belasten, deren Resynchronisierung auf dieselbe Zeit festgelegt ist. Aus diesem Grund löst das Telefon die Resynchronisierung bis zu 10 Minuten nach dem angegebenen Zeitpunkt aus.

Wenn Sie die Resynchronisierungszeit beispielsweise auf 1000 (10:00 Uhr) festlegen, löst das Telefon die Resynchronisierung irgendwann zwischen 10:00 Uhr und 10:10 Uhr aus.

Diese Funktion ist standardmäßig deaktiviert. Wenn der Parameter Resync_At bereitgestellt wurde, wird der Parameter Resync_Periodic ignoriert.

Konfigurierbare Zeitpläne

Mithilfe der folgenden Bereitstellungsparameter können Sie Zeitpläne für regelmäßige Resynchronisierungen konfigurieren und die Wiederholungsintervalle für Resynchronisierungs- und Upgrade-Fehler angeben:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Jeder Parameter akzeptiert einen einzelnen Verzögerungswert (in Sekunden). Die neue erweiterte Syntax ermöglicht eine durch Komma getrennte Liste von aufeinanderfolgenden Verzögerungselementen. Das letzte Element in der Sequenz wird implizit unendlich wiederholt.

Optional können Sie ein Pluszeichen (+) verwenden, um einen anderen numerischen Wert anzugeben, der eine zusätzliche zufällige Verzögerung festlegt.

Beispiel 1

In diesem Beispiel erfolgt die Resynchronisierung des Telefons in regelmäßigen Abständen alle zwei Stunden. Wenn ein Resynchronisierungsfehler auftritt, erfolgen auf dem Gerät Wiederholungsversuche in den folgenden

Intervallen: 30 Minuten, 1 Stunde, 2 Stunden, 4 Stunden. Das Gerät führt weitere Versuche in 4-Stunden-Intervallen durch, bis die Resynchronisierung erfolgreich ist.

```
Resync_Periodic=7200
Resync_Error_Retry_Delay=1800,3600,7200,14400
```

Beispiel 2

In diesem Beispiel erfolgt die Resynchronisierung des Geräts in regelmäßigen Abständen jede Stunde (mit einer zusätzlichen zufälligen Verzögerung von bis zu 10 Minuten). Bei einem Resynchronisierungsfehler erfolgen auf dem Gerät Wiederholungsversuche in den folgenden Intervallen: 30 Minuten (plus bis zu 5 Minuten). 1 Stunde (plus bis zu 10 Minuten), 2 Stunden (plus bis zu 15 Minuten). Das Gerät führt weitere Versuche in 2-Stunden-Intervallen durch (plus bis zu 15 Minuten), bis die Resynchronisierung erfolgreich ist.

```
Resync_Periodic=3600+600
Resync_Error_Retry_Delay=1800+300,3600+600,7200+900
```

Beispiel 3

Wenn in diesem Beispiel ein Remote-Upgrade-Versuch fehlschlägt, wiederholt das Gerät das Upgrade nach 30 Minuten, dann wieder nach einer weiteren Stunde und dann nach zwei Stunden. Wenn das Upgrade weiterhin fehlschlägt, versucht es das Gerät alle vier bis fünf Stunden erneut, bis das Upgrade erfolgreich ist.

```
Upgrade_Error_Retry_Delay  =  1800,3600,7200,14400+3600
```

Profilregeln

Das Telefon bietet mehrere Remote-Konfigurationsprofilparameter (Profile_Rule*). Somit können mit jedem Resynchronisierungsvorgang mehrere Dateien abgerufen werden, die von verschiedenen Servern verwaltet werden.

Im einfachsten Fall erfolgt die Resynchronisierung des Geräts regelmäßig mit einem einzelnen Profil auf einem zentralen Server, der alle relevanten internen Parameter aktualisiert. Alternativ kann das Profil auf verschiedene Dateien aufgeteilt werden. Eine Datei gilt für alle Telefone in einer Bereitstellung. Eine weitere, eindeutige Datei wird für jedes Konto bereitgestellt. Verschlüsselungscodes und Zertifikatinformationen können von einem weiteren Profil bereitgestellt werden, das auf einem separaten Server gespeichert ist.

Wenn eine Resynchronisierung fällig ist, wertet das Telefon die vier Profile_Rule*-Parameter nacheinander aus:

1. Profile_Rule
2. Profile_Rule_B
3. Profile_Rule_C
4. Profile_Rule_D

Jede Auswertung kann dazu führen, dass ein Profil von einem Remote-Bereitstellungsserver abgerufen wird und einige der internen Parameter möglicherweise aktualisiert werden. Wenn eine Auswertung fehlschlägt, wird die Resynchronisierungssequenz unterbrochen und entsprechend den Angaben für den Parameter

Resync_Error_Retry_Delay Parameter (in Sekunden) erneut durchgeführt. Wenn alle Auswertungen erfolgreich sind, wartet das Gerät, bis die im Parameter Resync_Periodic angegebene Zeit erreicht ist, und führt dann eine weitere Resynchronisierung durch.

Der Inhalt der einzelnen Profile_Rule*-Parameter besteht aus einer Reihe von Alternativen. Die Alternativen werden durch einen senkrechten Strich | getrennt. Jede Alternative besteht aus einem Bedingungsausdruck, einem Zuweisungsausdruck, einer Profil-URL und allen zugeordneten URL-Optionen. All diese Komponenten sind innerhalb jeder Alternative optional. Im Folgenden sind die zulässigen Kombinationen und die Reihenfolge, in der sie ggf. erscheinen müssen, aufgeführt:

```
[ conditional-expr ] [ assignment-expr ] [[ options ] URL ]
```

Innerhalb jedes Profile_Rule*-Parameters müssen alle Alternativen mit Ausnahme der letzten einen Bedingungsausdruck enthalten. Dieser Ausdruck wird ausgewertet und wie folgt verarbeitet:

1. Bedingungen werden von links nach rechts ausgewertet, bis eine gefunden wird, deren Auswertung „True“ ergibt (oder bis eine Alternative ohne Bedingungsausdruck gefunden wird).
2. Alle zugehörigen Zuweisungsausdrücke werden ggf. ausgewertet.
3. Wenn eine URL als Teil dieser Alternative angegeben ist, wird versucht, das Profil herunterzuladen, das sich unter der angegebenen URL befindet. Das System versucht, die internen Parameter entsprechend zu aktualisieren.

Wenn alle Alternativen über Bedingungsausdrücke verfügen und keine Auswertung „True“ ergibt (oder wenn die gesamte Profilregel leer ist), wird der gesamte Profile_Rule*-Parameter übersprungen. Der nächste Profilregelparameter in der Sequenz wird ausgewertet.

Beispiel 1

In diesem Beispiel erfolgt eine unbedingte Resynchronisierung mit dem Profil unter der angegebenen URL, und es wird eine HTTP GET-Anforderung an den Remote-Bereitstellungsserver gesendet:

```
http://remote.server.com/cisco/$MA.cfg
```

Beispiel 2

In diesem Beispiel erfolgt die Resynchronisierung des Geräts mit zwei unterschiedlichen URLs, abhängig vom Registrierungsstatus der Leitung 1. Im Falle einer verlorenen Registrierung führt das Gerät eine HTTP POST-Anforderung an ein CGI-Skript durch. Das Gerät sendet den Inhalt des makroerweiterten GPP_A-Parameters, der zusätzliche Informationen zum Gerätestatus enthalten kann:

```
($PRVTMR ge 600)? http://p.tel.com/has-reg.cfg
| [--post a] http://p.tel.com/lost-reg?
```

Beispiel 3

In diesem Beispiel erfolgt die Resynchronisierung des Geräts mit demselben Server. Das Gerät bietet zusätzliche Informationen, wenn kein Zertifikat auf der Einheit installiert ist (für ältere Einheiten vor 2.0):

```
(“$CCERT” eq “Installed”)? https://p.tel.com/config?
```

```
| https://p.tel.com/config?cisco$MAU
```

Beispiel 4

In diesem Beispiel ist Leitung 1 deaktiviert, bis GPP_A über die erste URL auf einen Wert gleich „Provisioned“ gesetzt wird. Anschließend erfolgt die Resynchronisierung mit der zweiten URL:

```
("$A" ne "Provisioned")? (Line_Enable_1_ = "No";)! https://p.tel.com/init-prov
| https://p.tel.com/configs
```

Beispiel 5

In diesem Beispiel wird angenommen, dass das Profil, das vom Server zurückgegeben wird, XML-Element-Tags enthält. Diese Tags müssen mithilfe der Alias-Zuordnung, die in GPP_B gespeichert ist, erneut den entsprechenden Parameternamen zugeordnet werden:

```
[--alias b] https://p.tel.com/account/$PN$MA.xml
```

Eine Resynchronisierung wird normalerweise als fehlgeschlagen betrachtet, wenn ein angefordertes Profil vom Server nicht empfangen wird. Der Parameter Resync_Fails_On_FNF kann dieses Standardverhalten überschreiben. Wenn Resync_Fails_On_FNF auf „No“ festgelegt ist, akzeptiert das Gerät eine Datei-nicht-gefunden-Antwort vom Server als erfolgreiche Resynchronisierung. Der Standardwert für Resync_Fails_On_FNF lautet „Yes“.

Upgrade Rule (Upgrade-Regel)

Mithilfe der Upgrade-Regel wird das Gerät angewiesen, eine neue Software zu aktivieren, und ggf. informiert, wo diese Software abgerufen werden kann. Wenn die Software bereits auf dem Gerät vorhanden ist, versucht es nicht, sie abzurufen. Die Gültigkeit des Software-Speicherorts ist demnach nicht von Bedeutung, wenn sich die gewünschte Software auf der inaktiven Partition befindet.

Mit dem Parameter Upgrade_Rule wird eine Firmware angegeben, die, wenn sie sich von der aktuellen Firmware unterscheidet, heruntergeladen und angewendet wird, sofern dies nicht durch einen Bedingungsausdruck verhindert wird oder Upgrade_Enable auf **No** festgelegt wurde.

Das Telefon umfasst einen konfigurierbaren Remote-Upgrade-Parameter: Upgrade_Rule. Dieser Parameter akzeptiert eine ähnliche Syntax wie die Profilregelparameter. URL-Optionen werden für Upgrades nicht unterstützt, aber Bedingungsausdrücke und Zuweisungsausdrücke können verwendet werden. Wenn Bedingungsausdrücke verwendet werden, können für den Parameter mehrere Alternativen, getrennt durch das |-Zeichen, angegeben werden. Die Syntax für die einzelnen Alternativen lautet wie folgt:

```
[ conditional-expr ] [ assignment-expr ] URL
```

Wie bei den Profile_Rule*-Parametern werden mit dem Parameter Upgrade_Rule alle Alternativen ausgewertet, bis ein Bedingungsausdruck erfüllt ist oder eine Alternative keinen Bedingungsausdruck aufweist. Der zugehörige Zuweisungsausdruck wird ausgewertet, sofern er angegeben wurde. Anschließend wird versucht, ein Upgrade über die angegebene URL durchzuführen.

Wenn Upgrade_Rule eine URL ohne einen Bedingungsausdruck enthält, wird das Gerät auf das Firmware-Image aktualisiert, das mit der URL angegeben wird. Nach der Makroerweiterung und Auswertung der Regel versucht

das Gerät so lange nicht erneut, ein Upgrade durchzuführen, bis die Regel oder die effektive Kombination von scheme + server + port + filepath geändert wurde.

Um zu versuchen, ein Firmware-Upgrade durchzuführen, wird zu Beginn des Vorgangs die Audiofunktion auf dem Gerät deaktiviert, und am Ende des Vorgangs wird das Gerät neu gestartet. Das Gerät führt nur dann automatisch ein Upgrade durch, das durch den Inhalt von Upgrade_Rule gesteuert wird, wenn alle Sprachleitungen derzeit inaktiv sind.

Beispiel:

- Für die Cisco IP Phone 6800-Serie:

```
http://p.tel.com/firmware/sip68xx.11-1-0MPP-BN.loads

where BN==Build Number
```

In diesem Beispiel wird mit Upgrade_Rule die Firmware auf das Image aktualisiert, das unter der angegebenen URL gespeichert ist.

Hier ein weiteres Beispiel für die Cisco IP Phone 6800-Serie:

```
("$F" ne "beta-customer")? http://p.tel.com/firmware/sip68xx.11-0-1MPP-BN.loads
| http://p.tel.com/firmware/sip68xx.11-0-1MPP-BN.loads

where BN==Build Number
```

In diesem Beispiel wird das Gerät angewiesen, basierend auf den Inhalten des allgemeinen Parameters GPP_F eines von zwei Images zu laden.

Das Gerät kann ein Downgrade-Limit bezüglich der Firmware-Versionsnummer erzwingen; dies kann eine nützliche Anpassungsoption sein. Wenn eine gültige Firmware-Versionsnummer im Parameter Downgrade_Rev_Limit konfiguriert ist, weist das Gerät Upgrade-Versuche für Firmware-Versionen vor dem angegebenen Grenzwert zurück.

Datentypen

Folgende Datentypen werden mit Konfigurationsprofilparametern verwendet:

- {a,b,c,…} – Wahlmöglichkeit zwischen a, b, c…
- Bool – Boolescher Wert „Ja“ oder „Nein“
- CadScript – Miniskript, mit dem die Rhythmusparameter eines Signals angegeben werden. Bis zu 127 Zeichen

  Syntax: $S_1[;S_2]$, wobei Folgendes gilt:

  - $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$. Dies wird als Abschnitt (section) bezeichnet.
  - $on_{i,j}$ und $off_{i,j}$ stehen für die Dauer der Aktivität/Inaktivität in Sekunden eines *Segments*. i = 1 oder 2 und j = 1 bis 6.
  - D_i ist die Gesamtdauer des Abschnitts in Sekunden.

Sie können die Zeitintervalle mit jeweils bis zu drei Dezimalstellen angeben, sodass sie bis auf die Millisekunde genau sind. Der Platzhalter „*“ steht für Endlosdauer. Die Segmente innerhalb der einzelnen Abschnitte werden der Reihe nach wiedergegeben und wiederholt, bis die Gesamtdauer erreicht ist.

Beispiel 1:

```
60(2/4)

Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60 s
Number of Segments = 1
Segment 1: On=2s, Off=4s

Total Ring Length = 60s
```

Beispiel 2 – Eindeutiger Rufton (kurz, kurz, kurz, lang):

```
60(.2/.2,.2/.2,.2/.2,1/4)

Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60s
Number of Segments = 4
Segment 1: On=0.2s, Off=0.2s
Segment 2: On=0.2s, Off=0.2s
Segment 3: On=0.2s, Off=0.2s
Segment 4: On=1.0s, Off=4.0s

Total Ring Length = 60s
```

- DialPlanScript – Skripterstellungssyntax, die zum Angeben der Rufnummernpläne für Leitung 1 und Leitung 2 verwendet wird.
- Float<n> – Gleitkommawert mit bis zu n Dezimalstellen.
- FQDN – Vollständiger Domänenname. Kann bis zu 63 Zeichen enthalten. Im Folgenden finden Sie einige Beispiele:
  - sip.Cisco.com:5060 oder 109.12.14.12:12345
  - sip.Cisco.com oder 109.12.14.12
- FreqScript – Miniskript, mit dem die Frequenz- und Pegelparameter eines Tons angegeben werden. Enthält bis zu 127 Zeichen.

  Syntax: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, wobei:
  - F_1– F_6 für die Frequenz in Hz stehen (nur Ganzzahlen ohne Vorzeichen).
  - L_1– L_6 sind entsprechende Pegel in dBm (mit bis zu einer Dezimalstelle).

  Leerzeichen vor und nach dem Komma sind erlaubt, werden jedoch nicht empfohlen.

  Beispiel 1 – Ton für wartenden Anruf:

```
440@-10

Number of Frequencies = 1
```

```
Frequency 1 = 440 Hz at -10 dBm
```

Beispiel 2 – Wählton:

```
350@-19,440@-19

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
```

- IP – Gültige IPv4-Adresse in der Form x.x.x.x, wobei x zwischen 0 und 255 liegt. Beispiel: 10.1.2.100.
- UserID – Benutzer-ID, wie sie in einer URL angezeigt wird; bis zu 63 Zeichen.
- Phone – Eine Zeichenfolge für die Telefonnummer, z. B. 14081234567, *69, *72, 345678; oder eine allgemeine URL, wie z. B. 1234@10.10.10.100:5068 oder jsmith@Cisco.com. Die Zeichenfolge kann bis zu 39 Zeichen enthalten.
- PhTmplt – Telefonnummernvorlage. Jede Vorlage kann eines oder mehrere Muster enthalten, die durch ein Komma (,) voneinander getrennt sind. Leerzeichen zu Beginn jedes Musters werden ignoriert. „?“ und „*“ sind Platzhalter. Verwenden Sie zur tatsächlichen Darstellung dieser Zeichen %xx. Beispiel: %2a steht für *. Die Vorlage kann bis zu 39 Zeichen enthalten. Beispiele: „1408*, 1510*“, „1408123????, 555?1.”.
- Port – TCP-/UDP-Portnummer (0-65535). Kann im Dezimal- oder Hexadezimalformat angegeben werden.
- ProvisioningRuleSyntax – Skripterstellungssyntax, mit der Regeln für die Konfigurationsresynchronisierung und Firmware-Upgrades definiert werden.
- PwrLevel – Leistungspegel in dBm mit einer Dezimalstelle, z. B. –13,5 oder 1,5 (dBm).
- RscTmplt – Vorlage des SIP-Antwort-Statuscodes, z. B. „404, 5*“, „61?“, „407, 408, 487, 481“. Kann bis zu 39 Zeichen enthalten.
- Sig<n> – n-Bit-Wert mit Vorzeichen. Kann im Dezimal- oder Hexadezimalformat angegeben werden. Vor negativen Werten muss ein „-“-Zeichen stehen. Ein „+“-Zeichen vor positiven Werten ist optional.
- Star Codes – Aktivierungscode für einen zusätzlichen Dienst, z. B. *69. Der Code kann bis zu 7 Zeichen enthalten.
- Str<n> – Allgemeine Zeichenfolge mit bis zu n nicht reservierten Zeichen.
- Time<n> – Zeitintervall in Sekunden mit bis zu n Dezimalstellen. Zusätzlich angegebene Dezimalstellen werden ignoriert.
- ToneScript – Miniskript, mit dem die Frequenz-, Pegel- und Rhythmusparameter eines Anrufstatus-Tons angegeben werden. Das Skript darf maximal 127 Zeichen enthalten.

  Syntax: FreqScript;Z_1[;Z_2].

  Der Abschnitt Z_1 ähnelt dem Abschnitt S_1 in einem CadScript, allerdings folgt auf jedes Ein-/Aus-Segment ein Frequenzkomponenten-Parameter: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$. Dabei ist:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ gibt die Frequenzkomponenten im FreqScript an, die in diesem Segment verwendet werden.

Wenn mehr als eine Frequenzkomponente in einem Segment verwendet wird, werden die Komponenten zusammengezählt.

Beispiel 1 – Wählton:

```
350@-19,440@-19;10(*/0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 10 s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 10s
```

Beispiel 2 – Unterbrochener Rufton:

```
350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 2
Cadence Section 1: Section Length = 2s
Number of Segments = 1
Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
Cadence Section 2: Section Length = 10s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 12s
```

- Uns<n> – n-Bit-Wert ohne Vorzeichen, wobei n = 8, 16 oder 32. Kann im Dezimal- oder Hexadezimalformat angegeben werden, z. B. 12 oder 0x18, solange der Wert in die n-Bits passt.

Hinweis Beachten Sie Folgendes:

- <Par Name> steht für den Namen eines Konfigurationsparameters. In einem Profil wird das entsprechende Tag gebildet, indem das Leerzeichen durch einen Unterstrich „_“ ersetzt wird, z. B. **Par_Name**.
- Ein leeres Standardwert-Feld impliziert eine leere Zeichenfolge < „“ >.
- Das Telefon verwendet weiterhin die zuletzt konfigurierten Werte für Tags, die in einem bestimmten Profil nicht vorhanden sind.
- Vorlagen werden in der angegebenen Reihenfolge verglichen. Die erste, *nicht die beste*, Übereinstimmung wird ausgewählt. Der Parametername muss genau übereinstimmen.
- Wenn mehr als eine Definition für einen Parameter in einem Profil angegeben ist, wird die letzte entsprechende Definition in der Datei auf dem Telefon verwendet.
- Durch eine Parameterspezifikation mit einem leeren Parameterwert wird erzwungen, dass der Parameter auf den Standardwert zurückgesetzt wird. Um stattdessen eine leere Zeichenfolge anzugeben, verwenden Sie die leere Zeichenfolge „“ als Parameterwert.

Profil-Updates und Firmware-Upgrades

Das Telefon unterstützt die sichere Remotebereitstellung (Konfiguration) und Firmware-Upgrades. Ein nicht konfiguriertes Telefon kann ein speziell für dieses Gerät entwickeltes, verschlüsseltes Profil empfangen. Aufgrund eines sicheren erstmaligen Bereitstellungsmechanismus, bei dem die SSL-Funktionalität verwendet wird, benötigt das Telefon keinen expliziten Schlüssel.

Ein Benutzereingriff ist nicht erforderlich, um ein Profil-Update oder ein Firmware-Upgrade zu starten oder durchzuführen, oder wenn zwischenzeitliche Upgrades erforderlich sind, um eine ältere Version auf einen aktuellen Upgrade-Status zu aktualisieren. Es wird nur dann versucht, eine Profilresynchronisierung durchzuführen, wenn das Telefon inaktiv ist, da eine Resynchronisierung einen Neustart der Software auslösen und einen Anruf beenden kann.

Der Bereitstellungsprozess wird durch allgemeine Parameter verwaltet. Jedes Telefon kann so konfiguriert werden, dass es regelmäßig einen NPS kontaktiert. Kommunikation mit dem NPS erfordert kein sicheres Protokoll, da das aktualisierte Profil mit einem Shared-Secret-Schlüssel verschlüsselt wird. Der NPS kann ein standardmäßiger TFTP-, HTTP- oder HTTPS-Server mit Client-Zertifikaten sein.

Der Administrator kann Telefone über die Webbenutzeroberfläche des Telefons aktualisieren, neu starten oder resynchronisieren. Diese Aufgaben können auch mithilfe einer SIP NOTIFY-Benachrichtigung ausgeführt werden.

Konfigurationsprofile werden mithilfe von gängigen Open-Source-Tools generiert, die sich in Bereitstellungssysteme von Serviceanbietern integrieren lassen.

Verwandte Themen

Zulassen und Konfigurieren von Profil-Updates, auf Seite 38

Zulassen und Konfigurieren von Profil-Updates

Profil-Updates können in bestimmten Intervallen ermöglicht werden. Aktualisierte Profile werden von einem Server über TFTP, HTTP oder HTTPS an das Telefon gesendet.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Prozedur

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

Schritt 2 Wählen Sie im Abschnitt **Konfigurationsprofil** die Option **Ja** aus dem Dropdown-Listenfeld **Bereitstellung aktivieren**.

Schritt 3 Geben Sie die Parameter ein.

Schritt 4 Klicken Sie auf **Alle Änderungen übernehmen**.

Verwandte Themen

Profil-Updates und Firmware-Upgrades, auf Seite 38

Zulassen und Konfigurieren von Firmware-Upgrades

Firmware-Updates können in bestimmten Intervallen ermöglicht werden. Aktualisierte Firmware wird von einem Server über TFTP oder HTTP an das Telefon gesendet. Die Sicherheit ist bei Firmware-Upgrades ein zu vernachlässigendes Problem, da Firmware keine persönlichen Daten enthält.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Prozedur

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

Schritt 2 Wählen Sie im Abschnitt **Firmware-Upgrade** die Option **Ja** aus dem Dropdown-Listenfeld **Upgrade aktivieren**.

Schritt 3 Geben Sie die Parameter ein.

Schritt 4 Klicken Sie auf **Alle Änderungen übernehmen**.

Firmware mit TFTP, HTTP oder HTTPS aktualisieren

Das Telefon unterstützt ein einzelnes Image-Upgrade über TFTP, HTTP oder HTTPS.

Hinweis Das Zurücksetzen auf frühere Versionen ist möglicherweise nicht für alle Geräte verfügbar. Weitere Informationen finden Sie in den Versionshinweisen für Ihr Telefon und Ihre Firmware-Version.

Vorbereitungen

Die Firmware-Datei muss auf einen verfügbaren Server heruntergeladen werden.

Prozedur

Schritt 1 Benennen Sie das Image wie folgt um:

`cp-x8xx-sip.aa-b-cMPP.cop` bis **`cp-x8xx-sip.aa-b-cMPP.tar.gz`**

Hierbei gilt:

`x8xx` ist die Telefonserie, z. B. 6841.

`aa-b-c` ist die Versionsnummer, z. B. 10-4-1.

Schritt 2 Verwenden Sie den Befehl **`tar -xzvf`**, um den Tarball zu entpacken.

Schritt 3 Kopieren Sie den Ordner in ein TFTP-, HTTP- oder HTTPS-Downloadverzeichnis.

Schritt 4 Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Schritt 5 Wählen Sie **Sprache** > **Bereitstellung** aus.

Schritt 6 Suchen Sie den Dateinamen der Software, der mit **.loads** endet, und fügen Sie diesen der gültigen URL hinzu.

Schritt 7 Klicken Sie auf **Alle Änderungen übernehmen**.

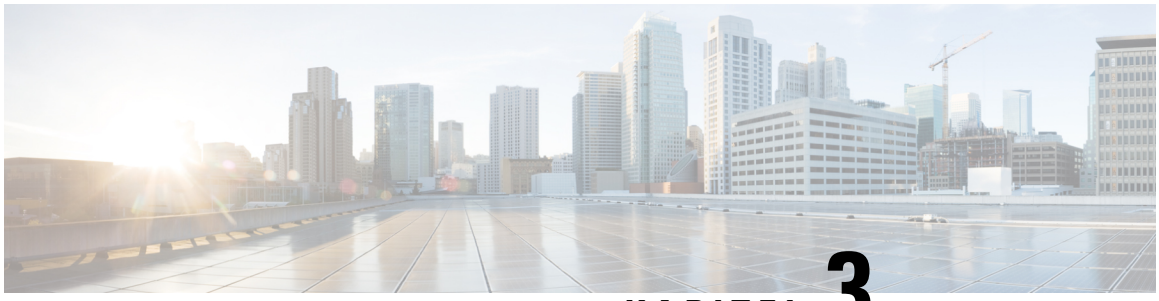
Aktualisieren der Firmware mit einem Browserbefehl

Ein in die Adressleiste des Browsers eingegebener Upgrade-Befehl kann verwendet werden, auf die Firmware auf einem Telefon zu aktualisieren. Das Telefon wird nur aktualisiert, wenn es inaktiv ist. Es wird automatisch versucht, das Update durchzuführen, wenn ein Anruf abgeschlossen ist.

Prozedur

Geben Sie den folgenden Befehl ein, um das Telefon mit einer URL in einem Webbrowser zu aktualisieren:

```
http://<phone_ip>/admin/upgrade?<schema>://<serv_ip[:port]>/filepath
```



KAPITEL 3

Interne Vorabbereitstellung und Bereitstellungsserver

Interne Vorabbereitstellung und Bereitstellungsserver

Mit Ausnahme der für die Remote-Personalisierung vorgesehenen Geräte konfiguriert der Serviceanbieter Telefone vorab mit einem Profil. Dieses Vorabbereitstellungsprofil kann eine begrenzte Anzahl von Parametern umfassen, mit denen das Telefon resynchronisiert wird. Das Profil kann auch einen gesamten Parametersatz enthalten, der vom Remoteserver übertragen wird. Standardmäßig führt das Telefon beim Einschalten und in den Intervallen, die im Profil konfiguriert sind, Resynchronisierungen durch. Wenn der Benutzer das Telefon am Kundenstandort anschließt, lädt das Gerät das aktualisierte Profil und alle eventuell vorhandenen Firmware-Updates herunter.

Dieser Vorgang der Vorabbereitstellung, Bereitstellung und Remotebereitstellung kann auf verschiedene Weise erfolgen.

Servervorbereitung und Softwaretools

Die Beispiele in diesem Kapitel erfordern, dass mindestens ein Server verfügbar ist. Diese Server können auf einem lokalen PC installiert und ausgeführt werden:

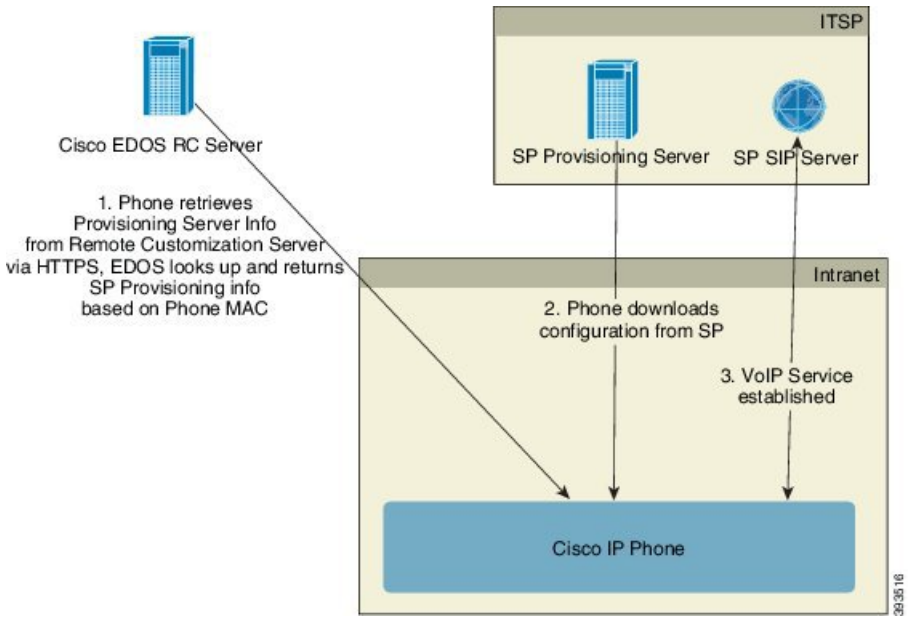
- TFTP (UDP-Port 69)
- Syslog (UDP-Port 514)
- HTTP (TCP-Port 80)
- HTTPS (TCP-Port 443)

Zum Beheben von Problemen mit der Serverkonfiguration ist es hilfreich, Clients für jeden Servertyp auf einem separaten Server zu installieren. Dieses Vorgehen gewährleistet einen ordnungsgemäßen Serverbetrieb, unabhängig von der Interaktion mit den Telefonen.

Außerdem wird empfohlen, die folgenden Softwaretools zu installieren:

- Zum Generieren von Konfigurationsprofilen installieren Sie das Open-Source-Komprimierungs-Utility gzip.
- Für Profilverschlüsselung und HTTPS-Operationen installieren Sie das Open-Source-Softwarepaket OpenSSL.
- Zum Testen der dynamischen Profilgenerierung und zur Remotebereitstellung über HTTPS in einem Schritt wird eine Skriptsprache empfohlen, die CGI-Scripting unterstützt. Die Open-Source-Sprache Perl ist ein Beispiel für eine solche Skriptsprache.
- Um den sicheren Datenaustausch zwischen Bereitstellungsservern und den Telefonen zu überprüfen, installieren Sie einen Ethernet-Packetsniffer (wie den kostenlos herunterladbaren Ethereal/Wireshark). Erfassen Sie eine Ethernet-Paketablaufverfolgung der Interaktionen zwischen dem Telefon und dem Bereitstellungsserver. Führen Sie hierzu den Packetsniffer auf einem PC aus, der mit einem Switch verbunden ist, auf dem die Portspiegelung aktiviert ist. Für HTTPS-Transaktionen können Sie das Utility ssldump verwenden.

Remote-Personalisierungsverteilung



Alle Telefone kontaktieren den Cisco EDOS RC-Server, bis sie zum ersten Mal bereitgestellt werden.

Bei einem Remote-Personalisierungsverteilungsmodell erwirbt der Kunde ein Telefon, das bereits einem bestimmten Serviceanbieter im Cisco EDOS RC-Server zugeordnet wurde. Der ITSP richtet einen Bereitstellungsserver ein und verwaltet ihn und registriert die Bereitstellungsserverinformationen beim Cisco EDOS RC-Server.

Wenn das Telefon eingeschaltet wird und über eine Internetverbindung verfügt, lautet der Personalisierungsstatus für das nicht konfigurierte Telefon **Offen**. Das Telefon fragt zuerst die Bereitstellungsserverinformationen vom lokalen DHCP-Server ab und legt den Personalisierungsstatus des Telefons fest. Wenn die DHCP-Abfrage erfolgreich ist, wird der Personalisierungsstatus auf **Abgebrochen**

festgelegt und es wird keine Remote-Personalisierung durchgeführt, weil DHCP die erforderlichen Bereitstellungsserverinformationen bereitstellt.

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

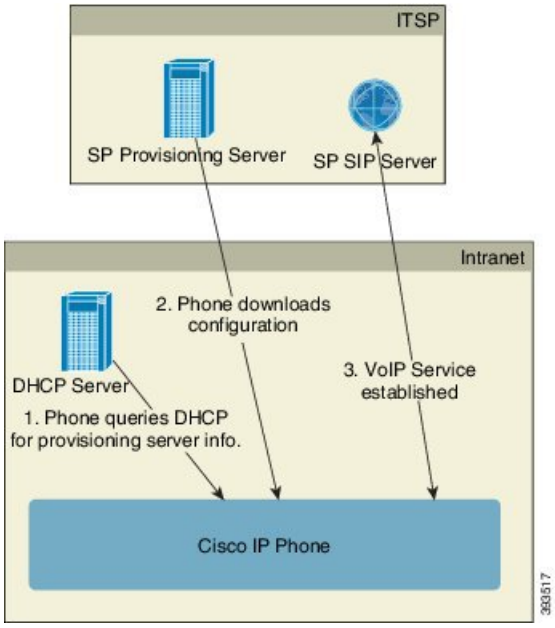
Wenn der DHCP-Server keine Bereitstellungsserverinformationen anbietet, fragt das Telefon den Cisco EDOS RC-Server ab, gibt seine MAC-Adresse und sein Modell an und legt den Personalisierungsstatus auf **Ausstehend** fest. Der Cisco EDOS-Server antwortet mit den Bereitstellungsserverinformationen des zugehörigen Serviceanbieters, einschließlich Bereitstellungsserver-URL, und der Personalisierungsstatus des Telefons wird auf **Anpassung-Ausstehend** festgelegt. Das Telefon führt dann einen URL-Befehl zur Resynchronisierung aus, um die Konfiguration des Serviceanbieters abzurufen. Wenn der Befehl fehlerfrei ausgeführt wird, wird der Personalisierungsstatus auf **Erfasst** festgelegt.

Wenn dem Telefon auf dem Cisco EDOS RC-Server kein Serviceanbieter zugeordnet ist, wird der Personalisierungsstatus des Telefons auf **Nicht verfügbar** festgelegt. Das Telefon kann manuell konfiguriert werden kann, oder dem Cisco EDOS Server kann eine Zuordnung für den Serviceanbieter des Telefons hinzugefügt werden.

Wenn ein Telefon über die LCD-Anzeige oder das Web Configuration Utility bereitgestellt wird, bevor der Personalisierungsstatus auf **Erfasst** festgelegt worden ist, dann wird der Personalisierungsstatus auf **Abgebrochen** festgelegt und der Cisco EDOS Server wird nur dann abgefragt, wenn das Telefon auf die Werkseinstellungen zurückgesetzt wird.

Nachdem das Telefon bereitgestellt worden ist, wird der Cisco EDOS RC-Server nur dann verwendet, wenn das Telefon auf die Werkseinstellungen zurückgesetzt wird.

Interne Vorabbereitstellung von Geräten



Mit der werksseitigen Standardkonfiguration von Cisco versucht das Telefon automatisch, sich mit einem Profil auf einem TFTP-Server zu resynchronisieren. Ein verwalteter DHCP-Server in einem LAN liefert die Informationen über das Profil und den TFTP-Server, der für die Vorabbereitstellung des Geräts konfiguriert ist. Der Serviceanbieter verbindet jedes neue Telefon mit dem LAN. Das Telefon führt automatisch eine Resynchronisierung mit dem lokalen TFTP-Server durch und initialisiert seinen internen Status, um sich auf die Bereitstellung vorzubereiten. Dieses Vorabbereitstellungsprofil enthält in der Regel die URL eines Remote-Bereitstellungsservers. Der Bereitstellungsserver aktualisiert das Gerät laufend, nachdem das Gerät bereitgestellt und mit dem Kundennetzwerk verbunden worden ist.

Der Barcode des vorab bereitgestellten Geräts kann gescannt werden, um die MAC-Adresse oder die Seriennummer aufzuzeichnen, bevor das Telefon an den Kunden geliefert wird. Diese Informationen können zum Erstellen des Profils, mit dem sich das Telefon resynchronisiert, verwendet werden.

Nach dem Empfang des Telefons verbindet der Kunden das Gerät mit den Breitband-Link. Beim Einschalten kontaktiert das Telefon den Bereitstellungsserver über die URL, die über die Vorabbereitstellung konfiguriert wird. Daher kann das Telefon das Profil und die Firmware bei Bedarf resynchronisieren und aktualisieren.

Verwandte Themen

Verteilung über den Einzelhandel, auf Seite 6
TFTP-Bereitstellung, auf Seite 44

Bereitstellungsserver-Setup

In diesem Abschnitt werden die Setup-Anforderungen beschrieben, die für die Bereitstellung eines Telefons mithilfe verschiedener Server und in verschiedenen Szenarien erforderlich sind. Für dieses Dokument und zum Testen werden Bereitstellungsserver auf einem lokalen PC installiert und ausgeführt. Zudem gibt es allgemein verfügbare Softwaretools, die bei der Bereitstellung von Telefonen hilfreich sind.

TFTP-Bereitstellung

Die Telefone unterstützen TFTP bei der Bereitstellung von Resynchronisierung und Firmware-Upgrades. Wenn Geräte remote bereitgestellt werden, wird HTTPS empfohlen, aber HTTP und TFTP kann auch verwendet werden. In diesem Fall muss eine Dateiverschlüsselung verwendet werden, um die Sicherheit und Zuverlässigkeit der gegebenen NAT- und Routerschutzmechanismen zu erhöhen. TFTP eignet sich für die interne Vorabbereitstellung einer großen Anzahl nicht konfigurierter Geräte.

Das Telefon kann die IP-Adresse eines TFTP-Servers über die DHCP-Option 66 direkt vom DHCP-Server abrufen. Wenn ein Profile_Rule-Parameter im Dateipfad dieses TFTP-Servers konfiguriert ist, lädt das Gerät sein Profil vom TFTP-Server herunter. Der Download wird ausgeführt, wenn das mit einem LAN verbundene Gerät eingeschaltet wird.

Der mit der werksseitigen Standardkonfiguration bereitgestellte Profile_Rule-Parameter ist *&PN*.cfg, wobei *&PN* für den Namen des Telefonmodells steht.

Beispielsweise lautet für das Modell CP-6841-3PCC der Dateiname CP-6841-3PCC.cfg.

Ein Gerät mit dem werksseitigen Standardprofil führt nach dem Einschalten eine Resynchronisierung mit dieser Datei durch, die sich auf dem von der DHCP-Option 66 angegebenen lokalen TFTP-Server befindet. Der Dateipfad bezieht sich auf das virtuelle Stammverzeichnis des TFTP-Servers.

Verwandte Themen

Interne Vorabbereitstellung von Geräten, auf Seite 43

Remote-Endpunktsteuerung und NAT

Das Telefon ist mit NAT (Network Address Translation) kompatibel und kann daher über einen Router auf das Internet zugreifen. Zur Erhöhung der Sicherheit kann der Router versuchen, nicht autorisierte eingehende Pakete durch die Implementierung von symmetrischem NAT zu blockieren. Dies ist eine Paketfilterungsstrategie, welche die Pakete beschränkt, die dazu berechtigt sind, vom Internet aus in das geschützte Netzwerk einzudringen. Aus diesem Grund wird die Remotebereitstellung mithilfe von TFTP nicht empfohlen.

VoIP kann nur dann zusammen mit NAT eingesetzt werden, wenn eine Art von NAT-Durchquerung ermöglicht wird. STUN (Configure Simple Traversal of UDP through NAT). Diese Option setzt beim Benutzer Folgendes voraus:

- Eine dynamische externe (öffentliche) IP-Adresse von Ihrem Service
- Einen Computer, der STUN-Serversoftware ausführt
- Ein peripheres Gerät mit einem asymmetrischen NAT-Mechanismus

HTTP-Bereitstellung

Das Telefon verhält sich wie ein Browser, der von einer Remotewebsite im Internet Webseiten anfordert. Dies stellt eine zuverlässige Methode zum Erreichen des Bereitstellungsserver dar, selbst wenn der Router des Kunden symmetrisches NAT oder einen anderen Schutzmechanismen implementiert. HTTP und HTTPS sind in Remotebereitstellungen zuverlässiger als TFTP, insbesondere wenn die bereitgestellten Geräte hinter lokalen Firewalls oder NAT-fähigen Routern vernetzt sind. HTTP und HTTPs sind in den nachstehenden Beschreibungen von Anforderungstypen austauschbar.

Eine einfache HTTP-basierte Bereitstellung stützt sich beim Abrufen der Konfigurationsprofile auf die HTTP-Methode GET. In der Regel wird für jedes bereitgestellte Telefon eine Konfigurationsdatei erstellt, und diese Dateien werden in einem HTTP-Serververzeichnis gespeichert. Wenn der Server die GET-Anforderung erhält, gibt er einfach die Datei zurück, die im GET-Anforderungsheader angegeben ist.

Das Konfigurationsprofil muss nicht statisch sein, sondern kann auch dynamisch generiert werden, indem eine Kundendatenbank abgefragt und das Profil anschließend erzeugt wird.

Wenn das Telefon eine Resynchronisierung anfordert, kann es unter Verwendung der HTTP-Methode POST die Konfigurationsdaten für die Resynchronisierung anfordern. Das Gerät kann so konfiguriert werden, dass bestimmte Status- und Identifikationsinformationen im Hauptteil der HTTP POST-Anforderung an den Server übermittelt werden. Der Server verwendet diese Informationen, um als Antwort das gewünschte Konfigurationsprofil zu generieren oder die Statusinformationen zur späteren Analyse oder Ablaufverfolgung zu speichern.

Als Teil der GET und POST-Anforderungen fügt das Telefon automatisch grundlegende identifizierende Informationen in das Feld „User-Agent“ des Anforderungsheaders ein. Diese Informationen geben den Hersteller, den Produktnamen, die aktuelle Firmware-Version und die Seriennummer des Geräts an.

Im folgenden Beispiel ist das Anforderungsfeld „User-Agent“ von einem CP-6841-3PCC dargestellt:

```
User-Agent: Cisco-CP-6841-3PCC/11.0 (00562b043615)
```

Wenn das Telefon so konfiguriert ist, dass die Resynchronisierung mit einem Konfigurationsprofil über HTTP erfolgt, empfiehlt es sich, zum Schutz der vertraulichen Informationen HTTPS zu verwenden oder das Profil zu verschlüsseln. Wenn das Telefon verschlüsselte Profile unter Verwendung von HTTP herunterlädt, wird

das Risiko vermieden, dass die im Konfigurationsprofil enthaltenen vertraulichen Informationen offen gelegt werden. Diese Art der Resynchronisierung erzeugt eine geringere Rechenlast für den Bereitstellungsserver als die Verwendung von HTTPS.

Das Telefon kann Profile entschlüsseln, die mit einer der folgenden Verschlüsselungsmethoden verschlüsselt sind:

- AES-256-CBC-Verschlüsselung
- RFC-8188-basierte Verschlüsselung mit AES-128-GCM-Schlüssel

Hinweis Die Telefone unterstützen HTTP-Version 1.0, HTTP-Version 1.1 und die Abschnittstransfercodierung, wenn HTTP-Version 1.1 das ausgehandelte Transportprotokoll ist.

HTTP-Statuscodeverarbeitung bei Resynchronisierung und Aktualisierung

Das Telefon unterstützt HTTP-Antworten für die Remotebereitstellung (Resynchronisierung). Das aktuelle Verhalten des Telefons lässt sich in drei Kategorien einteilen:

- A: Erfolg, wobei die Werte für „Resync Periodic“ (Periodische Resynchronisierung) und „Resync Random Delay“ (Zufällige Resynchronisierungsverzögerung) die nachfolgenden Anforderungen bestimmen.
- B: Fehler, wenn die Datei nicht gefunden wird oder das Profil beschädigt ist. Der Wert von „Resync Error Retry Delay“ (Wiederholungsverzögerung bei fehlgeschlagener Resynchronisierung) bestimmt die nachfolgenden Anforderungen.
- C: Anderer Fehler, wenn eine ungültige URL oder IP-Adresse einen Verbindungsfehler verursachen. Der Wert von „Resync Error Retry Delay“ (Wiederholungsverzögerung bei fehlgeschlagener Resynchronisierung) bestimmt die nachfolgenden Anforderungen.

Tabelle 2: Telefonverhalten in Reaktion auf HTTP-Antworten

HTTP-Statuscode	Beschreibung	Verhalten des Telefons
301 Dauerhaft verschoben	Diese und zukünftige Anforderungen sollen an den neue Speicherort gerichtet werden.	Anforderung sofort mit dem neuen Speicherort wiederholen.
302 Gefunden	Auch als „Vorübergehend verschoben“ bezeichnet.	Anforderung sofort mit dem neuen Speicherort wiederholen.
3xx	Andere 3xx-Antworten werden nicht verarbeitet.	C
400 Unzulässige Anforderung	Die Anforderung kann aufgrund einer fehlerhaften Syntax nicht erfüllt werden.	C
401 Nicht autorisiert	Authentifizierungsaufforderung bei einfacher oder Digest-Access-Authentifizierung.	Anforderung mit Authentifizierungsinformationen sofort wiederholen. Maximal 2 Wiederholungen. Bei einem Fehler entspricht das Verhalten des Telefons C.

HTTP-Statuscode	Beschreibung	Verhalten des Telefons
403 Unzulässig	Der Server weigert sich, zu antworten.	C
404 Nicht gefunden	Die angeforderte Ressource wurde nicht gefunden. Nachfolgende Anforderungen des Clients sind zulässig.	B
407 Proxy-Authentifizierung erforderlich	Authentifizierungsaufforderung bei einfacher oder Digest-Access-Authentifizierung.	Anforderung mit Authentifizierungsinformationen sofort wiederholen. Maximal zwei Wiederholungen. Bei einem Fehler entspricht das Verhalten des Telefons C.
4xx	Andere Client-Fehlerstatuscodes werden nicht verarbeitet.	C
500 Interner Serverfehler	Allgemeine Fehlermeldung.	Das Verhalten des Telefons entspricht C.
501 Nicht implementiert	Der Server erkennt die Anforderungsmethode nicht, oder er kann die Anforderung nicht erfüllen.	Das Verhalten des Telefons entspricht C.
502 Ungültiges Gateway	Der Server fungiert als Gateway oder Proxy und erhält vom Upstream-Server eine ungültige Antwort.	Das Verhalten des Telefons entspricht C.
503 Service nicht verfügbar	Der Server ist derzeit nicht verfügbar (überlastet oder zu Wartungszwecken heruntergefahren). Dies ist ein temporärer Zustand.	Das Verhalten des Telefons entspricht C.
504 Gateway-Zeitüberschreitung	Der Server fungiert als Gateway oder Proxy und erhält vom Upstream-Server nicht rechtzeitig eine Antwort.	C
5xx	Andere Serverfehler	C

HTTPS-Bereitstellung

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

Damit ein Serviceanbieter die Bereitstellung über HTTPS verwalten kann, muss für jeden Bereitstellungsserver, mit dem sich ein Telefon über HTTPS resynchronisiert, ein Serverzertifikat generiert werden. Das Serverzertifikat muss mit dem Cisco Server CA-Stammschlüssel signiert sein, dessen Zertifikat auf allen

bereitgestellten Geräten vorhanden ist. Um ein signiertes Serverzertifikat zu erhalten, muss der Serviceanbieter eine Zertifikatsignieranforderung an Cisco senden. Cisco signiert das Serverzertifikat und sendet es zur Installation auf dem Bereitstellungsserver an den Serviceanbieter zurück.

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

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

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

Anfordern eines signierten Serverzertifikats

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

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

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

Prozedur

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

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

Schritt 2 Wählen Sie **Zertifikatverwaltung** aus.

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

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

Hinweis Dieses Produkt umfasst die Multiplattform-Telefone der Cisco IP Phone 6800-Serie.

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

Schritt 5 Wählen Sie die Verschlüsselungsmethode aus:

- MD5
- SHA1
- SHA256

Cisco empfiehlt die SHA256-Verschlüsselung.

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

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

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

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

Schritt 9 Klicken Sie auf **Senden**.

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

CA-Client-Stammzertifikat für Multiplattform-Telefone

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

Das eindeutige Clientzertifikat, das jedes Gerät während einer HTTPS-Sitzung anbietet, enthält identifizierende Informationen, die in das Betrefffeld eingebettet sind. Diese Informationen können vom HTTPS-Server für ein CGI-Skript, das zum Bearbeiten sicherer Anforderungen aufgerufen wird, verfügbar gemacht werden. Der Zertifikatbetreff gibt den Produktnamen des Geräts (OU-Element), die MAC-Adresse (S-Element) und die Seriennummer (L-Element) an.

Das folgende Beispiel aus dem Betrefffeld des Clientzertifikats für Multiplattform-Telefone vom Typ Cisco IP Phone 6841 enthält die folgenden Elemente:

```
OU=CP-6841-3PCC, L=88012BA01234, S=000e08abcdef
```

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

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

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

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

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

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

Redundante Bereitstellungsserver

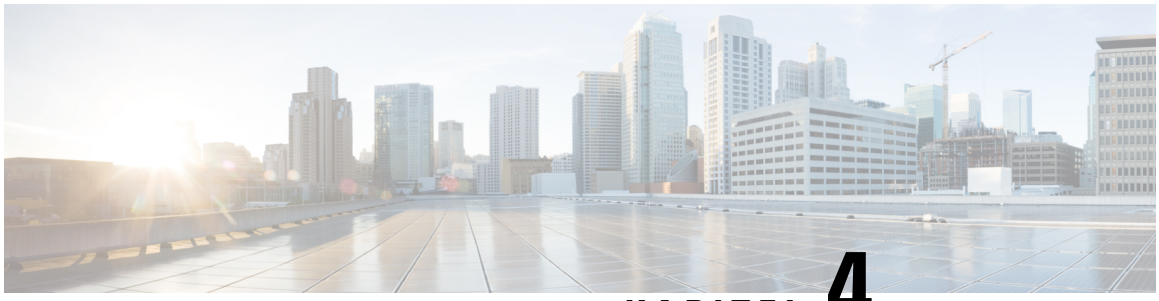
Der Bereitstellungsserver kann als IP-Adresse oder als vollständiger Domänenname (FQDN) angegeben werden. Die Verwendung eines FQDN erleichtert die Bereitstellung redundanter Bereitstellungsserver. Wenn der Bereitstellungsserver durch einen FQDN identifiziert wird, versucht das Telefon, den FQDN über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

Syslog Server (Syslog-Server)

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

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

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



KAPITEL 4

Bereitstellungsbeispiele

Bereitstellungsbeispiele – Übersicht

Dieses Kapitel enthält Beispielverfahren für die Übertragung von Konfigurationsprofilen zwischen dem Telefon und dem Bereitstellungsserver.

Informationen zum Erstellen von Konfigurationsprofilen finden Sie unter Bereitstellungsformate, auf Seite 15.

Grundlagen der Resynchronisierung

In diesem Abschnitt wird die grundlegende Funktionalität der Resynchronisierung der Telefone veranschaulicht.

TFTP-Resynchronisierung

Vom Telefon werden mehrere Netzwerkprotokolle zum Abrufen von Konfigurationsprofilen unterstützt. TFTP (RFC1350) ist das einfachste Profiltransferprotokoll. TFTP wird häufig zur Bereitstellung von Netzwerkgeräten innerhalb privater LANs verwendet. TFTP wird zwar nicht für die Bereitstellung von Remote-Endpunkten über das Internet empfohlen, eignet sich aber für die Bereitstellung in kleinen Organisationen, für die interne Vorabbereitstellung und zum Entwickeln und Testen. Weitere Informationen zur internen Vorabbereitstellung finden Sie im Abschnitt Interne Vorabbereitstellung von Geräten, auf Seite 43. Im folgenden Verfahren wird ein Profil nach dem Herunterladen einer Datei von einem TFTP-Server geändert.

Prozedur

Schritt 1 Innerhalb einer LAN-Umgebung verbinden Sie einen PC und ein Telefon mit einem Hub, Switch oder kleinen Router.

Schritt 2 Installieren und aktivieren Sie auf dem PC einen TFTP-Server.

Schritt 3 Erstellen Sie mit einem Texteditor ein Konfigurationsprofil, in dem, wie im Beispiel gezeigt, der Wert für GPP_A auf 12345678 festgelegt wird.

```
<flat-profile>
  <GPP_A> 12345678
  </GPP_A>
</flat-profile>
```

Schritt 4 Speichern Sie das Profil unter dem Namen `basic.txt` im Stammverzeichnis des TFTP-Servers.

Sie können überprüfen, ob der TFTP-Server ordnungsgemäß konfiguriert ist: Rufen Sie die Datei `basic.txt` mit einem anderen TFTP-Client als dem des Telefons ab. Verwenden Sie vorzugsweise einen TFTP-Client, der auf einem anderen Host als dem Bereitstellungsserver ausgeführt wird.

Schritt 5 Öffnen Sie im PC-Webbrowser die Konfigurationsseite „admin/advanced“. Wenn z. B. die IP-Adresse des Telefons 192.168.1.100 lautet:

```
http://192.168.1.100/admin/advanced
```

Schritt 6 Wählen Sie die Registerkarte **Sprache** > **Bereitstellung** aus, und überprüfen Sie die Werte der allgemeinen Parameter GPP_A bis GPP_P. Sie sollten leer sein.

Schritt 7 Öffnen Sie die Resynchronisierungs-URL in einem Webbrowserfenster, um das Testtelefon mit dem Konfigurationsprofil `basic.txt` neu zu synchronisieren.

Wenn die IP-Adresse des TFTP-Servers 192.168.1.200 lautet, sollte der Befehl dem folgenden Beispiel ähneln:

```
http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt
```

Wenn das Telefon diesen Befehl empfängt, fordert das Gerät mit der Adresse 192.168.1.100 die Datei `basic.txt` vom TFTP-Server mit der IP-Adresse 192.168.1.200 an. Das Telefon analysiert anschließend die heruntergeladene Datei und aktualisiert den Parameter GPP_A entsprechend mit dem Wert 12345678.

Schritt 8 Stellen Sie sicher, dass der Parameter ordnungsgemäß aktualisiert wurde: Aktualisieren die Konfigurationsseite im PC-Webbrowser, und wählen Sie auf dieser Seite die Registerkarte **Sprache** > **Bereitstellung** aus.

Der Parameter GPP_A sollte jetzt den Wert 12345678 enthalten.

Syslog zum Protokollieren von Nachrichten verwenden

Kurz bevor sich das Gerät mit einem Bereitstellungsserver synchronisiert, sendet das Telefon eine Syslog-Meldung an den festgelegten Syslog-Server. Nachdem die Resynchronisierung abgeschlossen wurde oder fehlgeschlagen ist, sendet das Gerät eine weitere Syslog-Meldung. Um diesen Server anzugeben, können Sie auf die Webseite für die Telefonverwaltung zugreifen (siehe Auf die Webseite des Telefons zugreifen, auf Seite 9), **Sprache** > **System** auswählen und den Server im Parameter **Syslog-Server** im Abschnitt **Optionale Netzwerkkonfiguration** angeben. Konfigurieren Sie die IP-Adresse des Syslog-Servers im Gerät, und beachten Sie die Meldungen, die während der restlichen Verfahren generiert werden.

Prozedur

Schritt 1 Installieren und aktivieren Sie einen Syslog-Server auf dem lokalen PC.

Schritt 2 Tragen Sie die IP-Adresse des PCs in den Syslog Server-Parameter des Profils ein und senden Sie die Änderung:

```
<Syslog_Server>192.168.1.210</Syslog_Server>
```

Schritt 3 Klicken Sie auf die Registerkarte **System**, und geben Sie den Wert des lokalen Syslog-Servers im Syslog Server-Parameter ein.

Schritt 4 Wiederholen Sie die Resynchronisierung, wie in TFTP-Resynchronisierung, auf Seite 51 beschrieben.

Das Gerät generiert während der Resynchronisierung zwei Syslog-Meldungen. Die erste Meldung gibt an, dass gerade eine Anforderung ausgeführt wird. Die zweite Meldung zeigt den Erfolg oder das Fehlschlagen der Resynchronisierung an.

Schritt 5 Überprüfen Sie, ob Ihr Syslog-Server Meldungen empfängt, die etwa wie folgt aussehen:

```
CP-68xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txtc.txt
```

Detaillierte Meldungen sind verfügbar, wenn Sie den Parameter Debug_Server (statt des Parameters Syslog_Server) mit der IP-Adresse des Syslog-Servers verwenden und für Debug_Level einen Wert zwischen 0 und 3 angeben (wobei 3 die ausführlichste Meldungsausgabe generiert):

```
<Debug_Server>192.168.1.210</Debug_Server>
<Debug_Level>3</Debug_Level>
```

Der Inhalt dieser Meldungen kann mithilfe der folgenden Parameter konfiguriert werden:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Wenn für einen dieser Parameter kein Wert angegeben ist, wird keine entsprechende Syslog-Meldung generiert.

Ein Gerät automatisch resynchronisieren

Ein Gerät kann sich in regelmäßigen Abständen erneut mit dem Bereitstellungsserver synchronisieren, um sicherzustellen, dass auf dem Server vorgenommene Profiländerungen an das Endgerät übermittelt werden (statt eine explizite Resynchronisierungsanforderung an das Endgerät zu senden).

Damit sich das Telefon regelmäßig erneut mit einem Server synchronisiert, werden mit dem Parameter Profile_Rule eine Konfigurationsprofil-URL und mit dem Parameter Resync_Periodic ein Resynchronisierungszeitraum definiert.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Prozedur

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

Schritt 2 Definieren Sie den Parameter Profile_Rule. In diesem Beispiel hat der TFTP-Server die IP-Adresse 192.168.1.200.

Schritt 3 Geben Sie in das Feld **Periodische Resynchronisierung** einen kleinen Wert zum Testen ein, z. B. **30** Sekunden.

Schritt 4 Klicken Sie auf **Alle Änderungen übernehmen**.

Mit den neuen Parametereinstellungen synchronisiert sich das Telefon zweimal in der Minute mit der Konfigurationsdatei, die in der URL angegeben ist.

Schritt 5 Beachten Sie die resultierenden Meldungen in der Syslog-Ablaufverfolgung (wie im Abschnitt Syslog zum Protokollieren von Nachrichten verwenden, auf Seite 52 beschrieben).

Schritt 6 Stellen Sie sicher, dass das Feld **Resynchronisierung nach Neustart** auf **Ja** festgelegt ist.

```
<Resync_On_Reset>Yes</Resync_On_Reset>
```

Schritt 7 Schalten Sie das Telefon aus und wieder ein, um eine Resynchronisierung mit dem Bereitstellungsserver zu erzwingen.

Wenn die Resynchronisierung aus irgendeinem Grund fehlschlägt, z. B. weil der Server nicht antwortet, wartet das Gerät (die in **Resync Error Retry Delay** konfigurierte Anzahl von Sekunden), bevor es versucht, eine erneute Resynchronisierung durchzuführen. Wenn **Wiederholungsverzögerung bei fehlgeschlagener Resynchronisierung** auf 0 (Null) festgelegt ist, führt das Telefon nach einem fehlgeschlagenen Resynchronisierungsversuch keine erneute Resynchronisierung aus.

Schritt 8 (Optional) Legen Sie das Feld **Wiederholungsverzögerung bei fehlgeschlagener Resynchronisierung** auf einen kleinen Wert fest, wie z. B. **30**.

```
<Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
```

Schritt 9 Deaktivieren Sie den TFTP-Server, und sehen Sie sich die Ergebnisse in der Syslog-Ausgabe an.

Eindeutige Profile, Makroerweiterung und HTTP

In einer Bereitstellung, bei der jedes Telefon für einige Parameter, z. B. User_ID oder Display_Name, mit verschiedenen Werten konfiguriert werden muss, kann der Serviceanbieter für jedes bereitgestellte Gerät ein eindeutiges Profil erstellen und diese Profile auf einem Bereitstellungsserver hosten. Jedes Telefon muss wiederum so konfiguriert werden, dass es sein eigenes Profil gemäß einer zuvor festgelegten Profilnamenskonvention resynchronisiert.

Die Syntax für die Profil-URL kann für ein Telefon gerätespezifische Informationen, z. B. MAC-Adresse oder Seriennummer, enthalten. Diese können durch die Makroerweiterung integrierter Variablen angegeben

werden. Bei Verwendung einer Makroerweiterung müssen diese Werte nicht an mehreren Stellen in jedem Profil angegeben werden.

Für eine Profilregel wird eine Makroerweiterung durchgeführt, bevor die Regel auf das Telefon angewendet wird. Über die Makroerweiterung werden einige Werte gesteuert, zum Beispiel:

- $MA wird zur 12-stelligen MAC-Adresse (Hexadezimalzahlen in Kleinbuchstaben) des Geräts erweitert. Beispiel: 000e08abcdef.
- $SN wird zur Seriennummer des Geräts erweitert. Beispiel: 88012BA01234.

Andere Werte können ebenfalls auf diese Weise per Makro erweitert werden, einschließlich der allgemeinen Parameter GPP_A bis GPP_P. Ein Beispiel hierfür finden Sie in TFTP-Resynchronisierung, auf Seite 51. Die Makroerweiterung ist nicht auf den URL-Dateinamen beschränkt, sondern kann auch auf jeden beliebigen Teil des Profilregelparameters angewendet werden. Auf diese Parameter wird mit $A bis $P Bezug genommen. Eine vollständige Liste der Variablen, die zur Makroerweiterung verfügbar sind, finden Sie in Makroerweiterungsvariablen, auf Seite 79.

In dieser Übung wird ein Profil für ein Telefon auf einem TFTP-Server bereitgestellt.

Übung: Bereitstellung eines bestimmten IP-Telefonprofils auf einem TFTP-Server

Prozedur

Schritt 1 Entnehmen Sie der Produktbezeichnung die MAC-Adresse des Telefons. (Die MAC-Adresse ist die Hexadezimalzahl aus Zahlen und Kleinbuchstaben, z. B. 000e08aabbcc.

Schritt 2 Kopieren Sie die Konfigurationsdatei `basic.txt` (die in TFTP-Resynchronisierung, auf Seite 51 beschrieben wird) in eine neue Datei mit dem Namen `CP-xxxx-3PCC macaddress.cfg` (wobei `xxxx` durch die Modellnummer und `macaddress` durch die MAC-Adresse des Telefons ersetzt wird).

Schritt 3 Verschieben Sie die neue Datei in das virtuelle Stammverzeichnis des TFTP-Servers.

Schritt 4 Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Schritt 5 Wählen Sie **Sprache** > **Bereitstellung** aus.

Schritt 6 Geben Sie `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` in das Feld **Profilregel** ein.

```
<Profile_Rule>
  tftp://192.168.1.200/CP-6841-3PCC$MA.cfg
</Profile_Rule>
```

Schritt 7 Klicken Sie auf **Alle Änderungen übernehmen**. Dies führt zu einem sofortigen Neustart und einer Resynchronisierung.

Bei der nächsten Resynchronisierung ruft das Telefon die neue Datei ab, indem der Makroausdruck $MA zur MAC-Adresse des Geräts erweitert wird.

Resynchronisierung mit der HTTP-Methode GET

HTTP stellt einen zuverlässigeren Resynchronisierungsmechanismus als TFTP zur Verfügung, da HTTP eine TCP-Verbindung einrichtet und TFTP das weniger zuverlässige UDP-Protokoll verwendet. Darüber hinaus bieten HTTP-Server bessere Filter- und Protokollierungsfunktionen als TFTP-Server.

Für das Telefon als Client ist keine spezielle Konfigurationseinstellung auf dem Server erforderlich, um eine Resynchronisierung unter Verwendung von HTTP durchführen zu können. Die zur Verwendung von HTTP mit der GET-Methode erforderliche Syntax des Parameters Profile_Rule ähnelt der Syntax, die für TFTP verwendet wird. Wenn ein Standard-Webbrowser ein Profil von Ihrem HTTP-Server abrufen kann, dann sollte einem Telefon dies auch gelingen.

Übung: Resynchronisierung mit der HTTP-Methode GET

Prozedur

Schritt 1 Installieren Sie einen HTTP-Server auf dem lokalen Computer oder einem anderen zugänglichen Host.

Der Open-Source-Server Apache kann aus dem Internet heruntergeladen werden.

Schritt 2 Kopieren Sie das Konfigurationsprofil `basic.txt` (das in TFTP-Resynchronisierung, auf Seite 51 beschrieben wird) in das virtuelle Stammverzeichnis des installierten Servers.

Schritt 3 Um die ordnungsgemäße Serverinstallation und den Zugriff auf `basic.txt` zu überprüfen, greifen Sie mit einem Webbrowser auf das Profil zu.

Schritt 4 Ändern Sie den Parameter Profile_Rule für das Testtelefon, sodass er auf den HTTP-Server statt auf den TFTP-Server verweist, damit das Profil in regelmäßigen Abständen von diesem Server heruntergeladen wird.

Wenn der HTTP-Server z. B. die Adresse 192.168.1.300 hat, geben Sie den folgenden Wert ein:

```
<Profile_Rule>
http://192.168.1.200/basic.txt
</Profile_Rule>
```

Schritt 5 Klicken Sie auf **Alle Änderungen übernehmen**. Dies führt zu einem sofortigen Neustart und einer Resynchronisierung.

Schritt 6 Beachten Sie die Syslog-Nachrichten, die das Telefon sendet. In den regelmäßigen Resynchronisierungen sollte nun das Profil vom HTTP-Server bezogen werden.

Schritt 7 Beachten Sie in den HTTP-Serverprotokollen, wie die Informationen, die das Testtelefon identifizieren, im Protokoll der Benutzer-Agenten angezeigt werden.

Diese Informationen sollten den Hersteller, den Produktnamen, die aktuelle Firmware-Version und die Seriennummer enthalten.

Bereitstellung über Cisco XML

Für jedes der Telefone, hier als xxxx bezeichnet, können Sie die Bereitstellung über Cisco XML-Funktionen durchführen.

Sie können ein XML-Objekt an das Telefon mit einem SIP-Notify-Paket oder einem Aufruf der HTTP-Methode Post an die CGI-Benutzeroberfläche des Telefons senden: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC erweitert die Cisco XML-Funktion, um die Bereitstellung über ein XML-Objekt zu unterstützen:

```
<CP-xxxx-3PCCExecute>
        <ExecuteItem URL=Resync:[profile-rule]/>
</CP-xxxx-3PCCExecute>
```

Nach dem Erhalt des XML-Objekts lädt das Telefon die Bereitstellungsdatei von [profile-rule] herunter. Diese Regel verwendet Makros, um die Entwicklung der XML-Serviceanwendung zu vereinfachen.

URL-Auflösung mit Makroerweiterung

Unterverzeichnisse mit mehreren Profilen auf dem Server stellen eine praktische Methode zur Verwaltung einer großen Anzahl von bereitgestellten Geräten dar. Die Profil-URL kann Folgendes enthalten:

- Namen oder explizite IP-Adresse des Bereitstellungsservers. Wenn der Bereitstellungsserver im Profil namentlich genannt wird, dann führt das Telefon eine DNS-Suche aus, um den Namen aufzulösen.
- Ein nicht standardmäßiger Serverport, der in der URL mit der Standardsyntax `:port` nach dem Servernamen angegeben wird.
- Das Unterverzeichnis des virtuellen Stammverzeichnisses des Servers, in dem das Profil gespeichert ist und das im URL-Standardformat angegeben und per Makroerweiterung verwaltet wird.

Zum Beispiel wird mit den folgenden Angaben für Profile_Rule die Profildatei ($PN.cfg), die sich im Serverunterverzeichnis `/cisco/config` befindet, vom TFTP-Server angefordert, der auf dem Host prov.telco.com ausgeführt wird und den Port 6900 auf Verbindungsanforderungen überwacht:

```
<Profile_Rule>
tftp://prov.telco.com:6900/cisco/config/$PN.cfg
</Profile_Rule>
```

Für jedes Telefon kann in einem allgemeinen Parameter, auf dessen Wert in einer gemeinsamen Profilregel verwiesen wird, per Makroerweiterung ein eigenes Profil identifiziert werden.

Angenommen, der Parameter GPP_B ist als `Dj6Lmp23Q` definiert.

Der Parameter Profile_Rule hat folgenden Wert:

```
tftp://prov.telco.com/cisco/$B/$MA.cfg
```

Wenn das Gerät eine Resynchronisierung durchführt und die Makros erweitert werden, dann fordert das Telefon mit der MAC-Adresse 000e08012345 das Profil mit dem Namen, der die MAC-Adresse des Geräts enthält, von folgender URL an:

```
tftp://prov.telco.com/cisco/Dj6Lmp23Q/000e08012345.cfg
```

Sichere HTTPS-Resynchronisierung

Die folgenden Mechanismen sind beim Telefon für die Resynchronisierung unter Verwendung eines sicheren Kommunikationsverfahrens verfügbar:

- Grundlegende HTTPS-Resynchronisierung
- HTTPS mit Clientzertifikatauthentifizierung

- HTTPS-Clientfilterung und dynamischer Inhalt

Grundlegende HTTPS-Resynchronisierung

HTTPS fügt für die Remotebereitstellung SSL zu HTTP hinzu, damit:

- das Telefon den Bereitstellungsserver authentifizieren kann.
- der Bereitstellungsserver das Telefon authentifizieren kann.
- die Vertraulichkeit des Informationsaustausches zwischen dem Telefon und dem Bereitstellungsserver gewährleistet ist.

SSL generiert und tauscht geheime (symmetrische) Schlüssel für jede Verbindung zwischen dem Telefon und dem Server unter Verwendung von Paaren öffentlicher und privater Schlüssel, die auf dem Telefon und im Bereitstellungsserver vorinstalliert sind, aus.

Für das Telefon als Client ist keine spezielle Konfigurationseinstellung auf dem Server erforderlich, um eine Resynchronisierung unter Verwendung von HTTPS durchführen zu können. Die zur Verwendung von HTTPS mit der GET-Methode erforderliche Syntax des Parameters Profile_Rule ähnelt der Syntax, die für HTTP oder TFTP verwendet wird. Wenn ein Standard-Webbrowser ein Profil von einem HTTPS-Server abrufen kann, dann sollte dem Telefon dies auch gelingen.

Zusätzlich zur Installation eines HTTPS-Servers muss ein SSL-Serverzertifikat, das von Cisco signiert ist, auf dem Bereitstellungsserver installiert werden. Die Geräte können sich nur dann mit einem Server, der HTTPS verwendet, resynchronisieren, wenn der Server ein von Cisco signiertes Zertifikat bereitstellt. Anweisungen zum Erstellen von signierten SSL-Zertifikaten für Voice-Produkte finden Sie unter https://supportforums.cisco.com/docs/DOC-9852.

Übung: Grundlegende HTTPS-Resynchronisierung

Prozedur

Schritt 1 Installieren Sie einen HTTPS-Server auf einem Host, dessen IP-Adresse für den DNS-Server des Netzwerks durch normale Host-Namenübersetzung erkennbar ist.

Wenn der Open-Source-Server Apache mit dem Open-Source-Paket mod_ssl installiert wird, kann er so konfiguriert werden, dass er als HTTPS-Server fungiert.

Schritt 2 Generieren Sie eine Serverzertifikatsignieranforderung (Certificate Signing Request, CSR) für den Server. Für diesen Schritt müssen Sie das Open-Source-Paket OpenSSL oder eine entsprechende Software installieren. Bei Verwendung von OpenSSL lautet der Befehl zum Generieren der grundlegenden CSR-Datei wie folgt:

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

Dieser Befehl generiert ein Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel, das in der Datei `privkey.pem` gespeichert wird.

Schritt 3 Senden Sie die CSR-Datei (provserver.csr) zum Signieren an Cisco.

Zurückgegeben wird ein signiertes Serverzertifikat (provserver.cert) zusammen mit einem Sipura Clientstammzertifikat der Zertifizierungsstelle, spacroot.cert).

Weitere Informationen finden Sie unter https://supportforums.cisco.com/docs/DOC-9852.

Schritt 4 Speichern Sie das signierte Serverzertifikat, die Datei mit dem privaten Schlüsselpaar und das Clientstammzertifikat an den entsprechenden Speicherorten auf dem Server.

Im Fall einer Apache-Installation unter Linux lauten diese Speicherorte in der Regel wie folgt:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```

Schritt 5 Starten Sie den Server neu.

Schritt 6 Kopieren Sie die Konfigurationsdatei `basic.txt` (die in TFTP-Resynchronisierung, auf Seite 51 beschrieben wird) in das virtuelle Stammverzeichnis des HTTPS-Servers.

Schritt 7 Überprüfen Sie, ob der Server ordnungsgemäß funktioniert, indem Sie `basic.txt` mit einem Standard-Webbrowser vom HTTPS-Server auf den lokalen PC herunterladen.

Schritt 8 Überprüfen Sie das Serverzertifikat, das der Server bereitstellt.

Der Browser erkennt wahrscheinlich das Zertifikat nicht als gültig an, wenn er nicht so vorkonfiguriert wurde, dass er Cisco als Stammzertifizierungsstelle akzeptiert. Die Telefone erwarten allerdings ein solches signiertes Zertifikat.

Ändern Sie den Parameter Profile_Rule des Testgeräts, sodass er einen Verweis auf den HTTPS-Server enthält, z. B.:

```
<Profile_Rule>
https://my.server.com/basic.txt
</Profile_Rule>
```

In diesem Beispiel wird davon ausgegangen, dass der Name des HTTPS-Servers **`my.server.com`** lautet.

Schritt 9 Klicken Sie auf **Alle Änderungen übernehmen**.

Schritt 10 Beachten Sie die Syslog-Ablaufverfolgung, die das Telefon sendet.

Die Syslog-Meldung sollten angeben, dass durch die Resynchronisierung das Profil vom HTTPS-Server abgerufen wurde.

Schritt 11 (optional) Verwenden Sie einen Ethernet-Protokoll-Analyzer im Telefon-Subnetz, um sicherzustellen, dass die Pakete verschlüsselt werden.

In dieser Übung wurde die Clientzertifikatverifizierung nicht aktiviert. Die Verbindung zwischen dem Telefon und dem Server wird verschlüsselt. Die Übertragung ist jedoch nicht sicher, da jeder Client eine Verbindung mit dem Server herstellen und die Datei abrufen kann, wenn er den Dateinamen und den Speicherort des Verzeichnisses kennt. Für eine sichere Resynchronisierung muss auch der Server den Client authentifizieren, wie in der in HTTPS mit Clientzertifikatauthentifizierung, auf Seite 60 beschriebenen Übung veranschaulicht wird.

HTTPS mit Clientzertifikatauthentifizierung

In der werksseitigen Standardkonfiguration fordert der Server von Clients kein SSL-Clientzertifikat an. Die Übertragung des Profils ist nicht sicher, da jeder Client eine Verbindung mit dem Server herstellen und das Profil anfordern kann. Sie können die Konfiguration bearbeiten, um die Clientauthentifizierung zu aktivieren. Der Server braucht ein Clientzertifikat, um das Telefon zu authentifizieren, bevor er die Verbindungsanforderung akzeptiert.

Deswegen kann die Resynchronisierung mit einem Browser, der nicht über die richtigen Anmeldeinformationen verfügt, nicht unabhängig getestet werden. Der SSL-Schlüsselaustausch in der HTTPS-Verbindung zwischen dem Testtelefon und dem Server kann mit dem Utility ssldump beobachtet werden. Das Utility trace zeigt die Interaktion zwischen Client und Server.

Übung: HTTPS mit Clientzertifikatauthentifizierung

Prozedur

Schritt 1 Aktivieren Sie die Clientzertifikatauthentifizierung auf dem HTTPS-Server.

Schritt 2 Legen Sie in Apache (v.2) folgende Einstellung in der Serverkonfigurationsdatei fest:

```
SSLVerifyClient  require
```

Stellen Sie außerdem sicher, dass die Datei „spacroot.cert“ so gespeichert wurde, wie in der Übung Grundlegende HTTPS-Resynchronisierung, auf Seite 58 gezeigt.

Schritt 3 Starten Sie den HTTPS-Server neu, und beobachten Sie die Syslog-Ablaufverfolgung des Telefons.

Bei jeder Resynchronisierung mit dem Server wird jetzt eine symmetrische Authentifizierung durchgeführt, sodass das Serverzertifikat und das Clientzertifikat überprüft werden, bevor das Profil übertragen wird.

Schritt 4 Erfassen Sie mit ssldump eine Resynchronisierungsverbindung zwischen dem Telefon und dem HTTPS-Server.

Wenn die Überprüfung des Clientzertifikats auf dem Server ordnungsgemäß aktiviert ist, zeigt die ssldump-Ablaufverfolgung den symmetrischen Austausch der Zertifikate (zuerst vom Server an den Client und anschließend vom Client an den Server), bevor die verschlüsselten Pakete, die das Profil enthalten, übertragen werden.

Wenn die Clientauthentifizierung aktiviert ist, kann nur ein Telefon mit einer MAC-Adresse, die einem gültigen Clientzertifikat entspricht, das Profil vom Bereitstellungsserver anfordern. Der Server lehnt Anforderungen von einem normalen Browser oder anderen nicht autorisierten Geräten ab.

HTTPS-Clientfilterung und dynamischer Inhalt

Wenn der HTTPS-Server so konfiguriert ist, dass ein Clientzertifikat erforderlich ist, werden durch die im Zertifikat enthaltenen Informationen das Telefon, welches die Resynchronisierung durchführt, identifiziert und die richtigen Konfigurationsinformationen bereitgestellt.

Der HTTPS-Server macht die Zertifikatinformationen für CGI-Skripts (oder kompilierte CGI Programme) verfügbar, die als Bestandteil der Resynchronisierungsanforderung aufgerufen werden. Zur Veranschaulichung

wird in dieser Übung die Open Source-Skriptsprache Perl verwendet und davon ausgegangen, dass Apache (v.2) als HTTPS-Server verwendet wird.

Prozedur

Schritt 1 Installieren Sie Perl auf dem Host, auf dem der HTTPS-Server ausgeführt wird.

Schritt 2 Generieren Sie das folgende Perl-Reflector-Skript:

```
#!/usr/bin/perl -wT
use strict;
print "Content-Type: text/plain\n\n";
print "<flat-profile><GPP_D>";

print "OU=$ENV{'SSL_CLIENT_I_DN_OU'},\n";
print "L=$ENV{'SSL_CLIENT_I_DN_L'},\n";
print "S=$ENV{'SSL_CLIENT_I_DN_S'}\n";
print "</GPP_D></flat-profile>";
```

Schritt 3 Speichern Sie diese Datei unter dem Dateinamen `reflect.pl`, mit der Berechtigung einer ausführbaren Datei (chmod 755 unter Linux), im Verzeichnis mit den CGI-Skripts auf dem HTTPS-Server.

Schritt 4 Überprüfen Sie die Zugriffsmöglichkeit von CGI-Skripts auf dem Server (d. h. `/cgi-bin/...`).

Schritt 5 Ändern Sie den Parameter Profile_Rule auf dem Testgerät, um die Resynchronisierung mit dem Reflextor-Skript durchzuführen, wie im folgenden Beispiel gezeigt:

```
https://prov.server.com/cgi-bin/reflect.pl?
```

Schritt 6 Klicken Sie auf **Alle Änderungen übernehmen**.

Schritt 7 Beobachten Sie die Syslog-Ablaufverfolgung, um eine erfolgreiche Resynchronisierung sicherzustellen.

Schritt 8 Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Schritt 9 Wählen Sie **Sprache** > **Bereitstellung** aus.

Schritt 10 Überprüfen Sie, ob der Parameter GPP_D die Informationen enthält, die vom Skript erfasst wurden.

Diese Informationen beinhalten den Produktnamen, die MAC-Adresse und die Seriennummer, wenn das Testgerät über ein eindeutiges Zertifikat des Herstellers verfügt. Die Informationen enthalten allgemeine Zeichenfolgen, wenn das Gerät vor Firmware-Version 2.0 hergestellt wurde.

Ein ähnliches Skript kann Informationen über das resynchronisierende Gerät ermitteln und dem Gerät dann die entsprechenden Konfigurationsparameterwerte bereitstellen.

HTTPS-Zertifikate

Das Telefon stellt eine zuverlässige und sichere Bereitstellungsstrategie bereit, die auf HTTPS-Anfragen vom Gerät an den Bereitstellungsserver basiert. Ein Serverzertifikat und ein Clientzertifikat werden verwendet, um das Telefon gegenüber dem Server und den Server gegenüber dem Telefon zu authentifizieren.

Damit HTTPS mit dem Telefon verwendet werden kann, müssen Sie eine CSR (Certificate Signing Request, Zertifikatsignierungsanforderung) generieren und an Cisco senden. Das Telefon generiert ein Zertifikat zur

Installation auf dem Bereitstellungsserver. Das Telefon akzeptiert das Zertifikat, wenn es versucht, eine HTTPS-Verbindung mit dem Bereitstellungsserver herzustellen.

HTTPS-Methode

HTTPS verschlüsselt die Kommunikation zwischen einem Client und einem Server und schützt dadurch den Nachrichtentext vor anderen Netzwerkgeräten. Die Verschlüsselungsmethode für den Textkörper der Kommunikation zwischen einem Client und einem Server basiert auf symmetrischen Schlüsseln. Bei Verwendung der Verschlüsselung mit symmetrischen Schlüsseln nutzen ein Client und ein Server gemeinsam einen einzigen geheimen Schlüssel über einen sicheren Kanal, der durch die Verschlüsselung mit öffentlichen und privaten Schlüssel geschützt ist.

Mit einem geheimen Schlüssel verschlüsselte Nachrichten können nur mit demselben Schlüssel entschlüsselt werden. HTTPS unterstützt eine Vielzahl von symmetrischen Verschlüsselungsalgorithmen. Das Telefon kann neben der 128-Bit-RC4-Verschlüsselung eine symmetrische 256-Bit-Verschlüsselung unter Verwendung von AES (American Encryption Standard) implementieren.

HTTPS ermöglicht auch die Authentifizierung eines Servers und eines Clients, die an einer sicheren Transaktion beteiligt sind. Diese Funktion stellt sicher, dass ein Bereitstellungsserver und einzelne Clients nicht von anderen Geräten im Netzwerk manipuliert werden können. Diese Funktion ist im Rahmen der Bereitstellung von Remote-Endpunkten unabdingbar.

Server- und Clientauthentifizierung erfolgen mittels Verschlüsselung mit öffentlichen und privaten Schlüsseln und mit einem Zertifikat, das den öffentlichen Schlüssel enthält. Text, der mit einem öffentlichen Schlüssel verschlüsselt worden ist, kann nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden (und umgekehrt). Das Telefon unterstützt den Rivest-Shamir-Adleman (RSA)-Algorithmus für die Verschlüsselung mit öffentlichen und privaten Schlüsseln.

SSL-Serverzertifikat

Für jeden sicheren Bereitstellungsserver wird ein SSL-Serverzertifikat (Secure Sockets Layer) ausgestellt, das von Cisco direkt signiert wird. Die Firmware, die auf dem Telefon ausgeführt wird, erkennt nur Cisco Zertifikate als gültig an. Wenn ein Client über HTTPS eine Verbindung mit einem Server herstellt, werden alle Serverzertifikate, die nicht von Cisco signiert sind, abgelehnt.

Diese Methode schützt Serviceanbieter vor unbefugten Zugriffen auf das Telefon und jeglichen Versuchen, den Bereitstellungsserver zu manipulieren. Ohne einen solchen Schutz könnte ein Angreifer möglicherweise das Telefon erneut bereitstellen, um in den Besitz von Konfigurationsinformationen zu gelangen oder einen anderen VoIP-Dienst zu nutzen. Ohne den privaten Schlüssel, der zu einem gültigen Serverzertifikat gehört, kann der Angreifer keine Kommunikation mit einem Telefon aufbauen.

Beziehen eines Serverzertifikats

Prozedur

Schritt 1 Wenden Sie sich an einen Cisco Support-Mitarbeiter, der Sie beim Beziehen des Zertifikats unterstützt. Wenn Sie nicht mit einem bestimmten Support-Mitarbeiter zusammenarbeiten, senden Sie Ihre Anforderung per E-Mail an ciscosb-certadmin@cisco.com.

Schritt 2 Generieren Sie einen privaten Schlüssel für eine CSR (Certificate Signing Request, Anforderung zur Zertifikatsignierung). Dieser Schlüssel ist privat, und Sie müssen ihn nicht an den Cisco Support weitergeben. Generieren Sie den Schlüssel mit dem Open-Source-Programm „openssl“. Beispiel:

```
openssl genrsa -out <file.key> 1024
```

Schritt 3 Generieren Sie eine CSR, die Felder enthält, die Ihr Unternehmen und Ihren Standort identifizieren. Beispiel:

```
openssl req -new -key <file.key> -out <file.csr>
```

Sie benötigen die folgende Informationen:

- Betrefffeld: Geben Sie den allgemeinen Namen (CN) in Form eines vollständigen Domänennamens (FQDN, Fully Qualified Domain Name) ein. Während des SSL-Authentifizierungshandshake prüft das Telefon, ob das Zertifikat, das es erhält, von dem Computer stammt, der es übermittelt hat.
- Serverhost-Name: Beispiel: provserv.domain.com.
- E-Mail-Adresse: Geben Sie eine E-Mail-Adresse ein, damit der Kundensupport Sie bei Bedarf kontaktieren kann. Diese E-Mail-Adresse ist in der CSR sichtbar.

Schritt 4 Senden Sie die CSR (im Zip-Dateiformat) per E-Mail an den Cisco Support-Mitarbeiter oder an ciscosb-certadmin@cisco.com. Das Zertifikat wird von Cisco signiert. Cisco sendet Ihnen das Zertifikat zu, damit Sie es auf Ihrem System installieren.

Client-Zertifikat

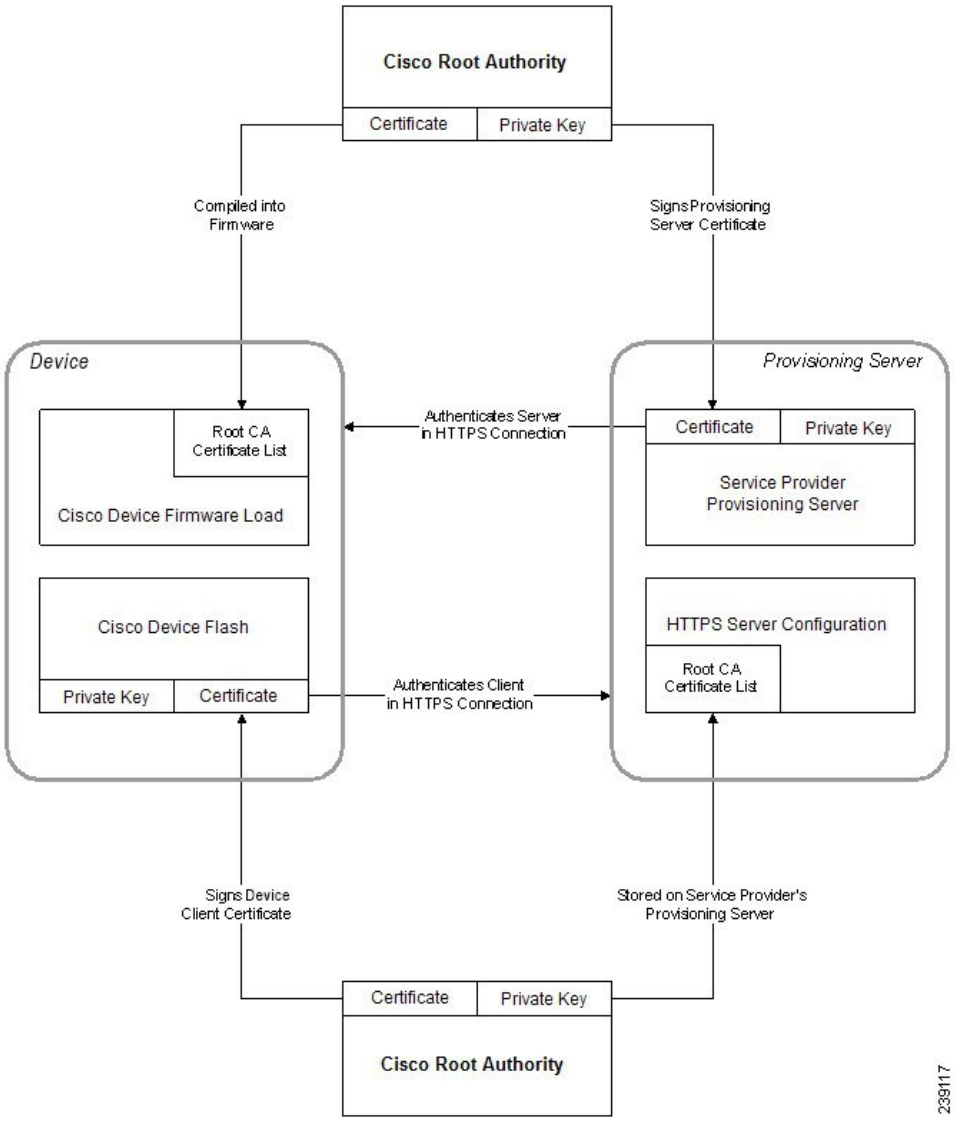
Angreifer können nicht nur einen direkten Angriff auf das Telefon ausüben, sondern auch versuchen, einen Bereitstellungsserver über einen Standard-Webbrowser oder einen anderen HTTPS-Client zu kontaktieren, um das Konfigurationsprofil vom Bereitstellungsserver abzurufen. Um diese Art von Angriffen zu verhindern, verfügt jedes Telefon auch über ein eindeutiges, von Cisco signiertes Clientzertifikat, das Informationen zum Identifizieren der einzelnen Endpunkte enthält. Jeder Serviceanbieter erhält ein Certificate Authority(CA)-Stammzertifikat, mit dem das Clientzertifikat des Geräts authentifiziert werden kann. Dieser Authentifizierungspfad ermöglicht es dem Bereitstellungsserver, unbefugte Konfigurationsprofilanforderungen abzulehnen.

Zertifikatstruktur

Durch diese Kombination von Serverzertifikat und Clientzertifikat wird eine sichere Kommunikation zwischen dem Bereitstellungsserver und einem Remote-Telefon gewährleistet. Die Abbildung unten zeigt die Beziehung und Position der Zertifikate, der Paare aus öffentlichen und privaten Schlüsseln und der signierenden Stammzertifizierungsstellen zwischen Cisco Client, Bereitstellungsserver und Zertifizierungsstelle.

Die obere Hälfte des Diagramms zeigt die Bereitstellungsserver-Stammzertifizierungsstelle, die zum Signieren der einzelnen Bereitstellungsserverzertifikate verwendet wird. Da das entsprechende Stammzertifikat in die Firmware eingebunden wird, kann das Telefon die autorisierten Bereitstellungsserver authentifizieren.

Abbildung 2: Certificate Authority – Ablauf



Konfigurieren einer benutzerdefinierten Certificate Authority

Mithilfe von digitalen Zertifikaten können Netzwerkgeräte und Benutzer im Netzwerk authentifiziert werden. Sie können zum Aushandeln von IPSec-Sitzungen zwischen Netzwerkknoten verwendet werden.

Dritte verwenden ein Certificate Authority(CA)-Zertifikat, um zwei oder mehr Knoten, die eine Verbindung herzustellen versuchen, zu überprüfen und zu authentifizieren. Jeder Knoten verfügt über einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel dient zum Verschlüsseln der Daten. Der private Schlüssel wird zum Entschlüsseln der Daten verwendet. Da die Knoten ihre Zertifikate von der gleichen Quelle bezogen haben, sind ihre jeweiligen Identitäten gesichert.

Das Gerät kann mit den von einer Drittanbieter-Certificate Authority (CA) bereitgestellten digitalen Zertifikaten IPSec-Verbindungen authentifizieren.

Die Telefone unterstützen eine Reihe von vorinstallierten Root Certificate Authoritys, die in die Firmware eingebettet sind:

- Cisco Small Business CA-Zertifikat
- CyberTrust CA-Zertifikat
- VeriSign CA-Zertifikat
- Sipura Stamm-CA-Zertifikat
- Linksys Stamm-CA-Zertifikat

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe unter Auf die Webseite des Telefons zugreifen, auf Seite 9.

Prozedur

Schritt 1 Wählen Sie **Info** > **Status** aus.

Schritt 2 Navigieren Sie zu **Benutzerdefinierter CA-Status**, und beachten Sie die folgenden Felder:

- Benutzerdefinierter CA-Bereitstellungsstatus: Gibt den Bereitstellungsstatus an.
  - Letzte Bereitstellung erfolgreich: mm/tt/jjjj HH:MM:SS
  - Letzte Bereitstellung fehlgeschlagen: mm/tt/jjjj HH:MM:SS
- Benutzerdefinierte CA-Informationen: Enthält Informationen über die benutzerdefinierte CA.
  - Installiert: Zeigt den CN-Wert an, der der Wert des CN-Parameters für das Feld Betreff im ersten Zertifikat ist.
  - Nicht installiert: Zeigt an, wenn kein benutzerdefiniertes CA-Zertifikat installiert ist.

Profilverwaltung

In diesem Abschnitt wird gezeigt, wie Konfigurationsprofile zum Herunterladen vorbereitet werden. Zur Erläuterung der Funktionalität wird als Resynchronisierungsmethode TFTP von einem lokalen PC eingesetzt. HTTP oder HTTPS könnten aber ebenso verwendet werden.

Offenes Profil mit Gzip komprimieren

Ein Konfigurationsprofil im XML-Format kann sehr groß werden, wenn im Profil alle Parameter einzeln angegeben werden. Um die Auslastung des Bereitstellungsservers zu verringern, unterstützt das Telefon die Komprimierung der XML-Datei im Deflate Komprimierungsformat, das vom Utility Gzip (RFC 1951) unterstützt wird.

Hinweis Die Komprimierung muss vor der Verschlüsselung erfolgen, damit das Telefon ein komprimiertes und verschlüsseltes XML-Profil erkennt.

Für die Integration in benutzerdefinierte Back-End-Bereitstellungsserverlösungen kann die Open-Source-Komprimierungsbibliothek zlib statt des eigenständigen Utility Gzip zum Komprimieren des Profils verwendet werden. Allerdings erwartet das Telefon eine Datei mit gültigem Gzip-Header.

Prozedur

Schritt 1 Installieren Sie Gzip auf dem lokalen Computer.

Schritt 2 Komprimieren Sie das Konfigurationsprofil `basic.txt` (das in TFTP-Resynchronisierung, auf Seite 51 beschrieben wird), indem Sie gzip in der Befehlszeile aufrufen:

```
gzip basic.txt
```

Dadurch wird die komprimierte Datei `basic.txt.gz` generiert.

Schritt 3 Speichern Sie die Datei `basic.txt.gz` im virtuellen Stammverzeichnis des TFTP-Servers.

Schritt 4 Ändern Sie den Parameter Profile_Rule auf dem Testgerät, sodass die Resynchronisierung mit der dekomprimierten Datei statt der ursprünglichen XML-Datei erfolgt, wie im folgenden Beispiel dargestellt:

```
tftp://192.168.1.200/basic.txt.gz
```

Schritt 5 Klicken Sie auf **Alle Änderungen übernehmen**.

Schritt 6 Beachten Sie die Syslog-Ablaufverfolgung des Telefons.

Bei der Resynchronisierung lädt das Telefon die neue Datei herunter und verwendet sie zum Aktualisieren der Geräteparameter.

Verwandte Themen

Open-Format-Profil – Komprimierung, auf Seite 20

Ein Profil mit OpenSSL verschlüsseln

Komprimierte und unkomprimierte Profile können verschlüsselt werden (allerdings müssen die Dateien vor der Verschlüsselung komprimiert werden). Die Verschlüsselung ist nützlich, wenn die Vertraulichkeit der Profilinformationen besonders wichtig ist, z. B. wenn TFTP oder HTTP für die Kommunikation zwischen dem Telefon und dem Bereitstellungsserver verwendet wird.

Das Telefon unterstützt die Verschlüsselung mit symmetrischen Schlüsseln mit einem 256-Bit-AES-Algorithmus. Diese Verschlüsselung kann mithilfe des Open-Source-Pakets OpenSSL durchgeführt werden.

Prozedur

Schritt 1 Installieren Sie OpenSSL auf einem lokale PC. Möglicherweise muss die Anwendung OpenSSL neu kompiliert werden, um AES zu aktivieren.

Schritt 2 Generieren Sie unter Verwendung der Konfigurationsdatei `basic.txt` (die in TFTP-Resynchronisierung, auf Seite 51 beschrieben wird) eine verschlüsselte Datei mit dem folgenden Befehl:

```
>openssl enc -aes-256-cbc -k MyOwnSecret -in basic.txt -out basic.cfg
```

Die komprimierte Datei `basic.txt.gz`, die in Offenes Profil mit Gzip komprimieren, auf Seite 65 erstellt wurde, kann auch verwendet werden, weil das XML-Profil sowohl komprimiert als auch verschlüsselt sein kann.

Schritt 3 Speichern Sie die verschlüsselte Datei `basic.cfg` im virtuellen Stammverzeichnis des TFTP-Servers.

Schritt 4 Ändern Sie den Parameter Profile_Rule auf dem Testgerät, sodass die verschlüsselte Datei statt der ursprünglichen XML-Datei zum Resynchronisieren verwendet wird. Der Verschlüsselungsschlüssel wird mit der folgenden URL-Option für das Telefon offengelegt:

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

Schritt 5 Klicken Sie auf **Alle Änderungen übernehmen**.

Schritt 6 Beachten Sie die Syslog-Ablaufverfolgung des Telefons.

Bei der Resynchronisierung lädt das Telefon die neue Datei herunter und verwendet sie zum Aktualisieren der Geräteparameter.

Verwandte Themen

AES-256-CBC-Verschlüsselung, auf Seite 21

Partitionierte Profile erstellen

Während jeder Resynchronisierung lädt ein Telefon mehrere separate Profile herunter. Dieses Verfahren ermöglicht es, verschiedene Arten von Profilinformationen auf unterschiedlichen Servern zu verwalten und allgemeine Konfigurationsparameterwerte getrennt von kontospezifischen Werten zu pflegen.

Prozedur

Schritt 1 Erstellen Sie ein neues XML-Profil namens `basic2.txt`, das einen Wert für einen Parameter angibt und sich dadurch von den früheren Übungen unterscheidet. Fügen Sie z. B. dem Profil `basic.txt` Folgendes hinzu:

```
<GPP_B>ABCD</GPP_B>
```

Schritt 2 Speichern Sie das Profil `basic2.txt` im virtuellen Stammverzeichnis des TFTP-Servers.

Schritt 3 Lassen Sie die erste Profilregel aus den früheren Übungen im Ordner, konfigurieren Sie die zweite Profilregel (Profile_Rule_B) jedoch so, dass sie auf die neue Datei verweist:

```
<Profile_Rule_B>tftp://192.168.1.200/basic2.txt
</Profile_Rule_B>
```

Schritt 4 Klicken Sie auf **Alle Änderungen übernehmen**.

Wenn eine Resynchronisierung fällig ist, synchronisiert sich das Telefon jetzt zuerst mit dem ersten und dann mit dem zweiten Profil.

Schritt 5 Beobachten Sie die Syslog-Ablaufverfolgung, um zu überprüfen, ob sich das Gerät erwartungsgemäß verhält.

Privatfunktion-Header für Telefon einrichten

Ein Privatfunktion-Header eines Benutzers in der SIP-Nachricht legt die Benutzerdatenschutz-Anforderungen des vertrauenswürdigen Netzwerks fest.

Sie können den Wert des Privatfunktion-Headers eines Benutzers für jede einzelne Durchwahl mithilfe eines XML-Tags in der Datei `config.xml` festlegen.

Die Privatfunktion-Header-Optionen lauten:

- Deaktiviert (Standardwert)
- Keine: Der Benutzer fordert, dass ein Datenschutzservice keine Privatfunktionen für die SIP-Nachricht anwendet.
- Header: Der Benutzer fordert, dass ein Datenschutzservice Header verdeckt, deren identifizierende Informationen nicht bereinigt werden können.
- Sitzung: Der Benutzer fordert, dass ein Datenschutzservice Anonymität für die Sitzungen bereitstellt.
- Benutzer: Der Benutzer fordert die Verwendung von Privatfunktionen nur von Vermittlern.
- ID: Der Benutzer fordert, dass das System eine Ersatz-ID verwendet, die weder IP-Adresse noch Host-Namen veröffentlicht.

Prozedur

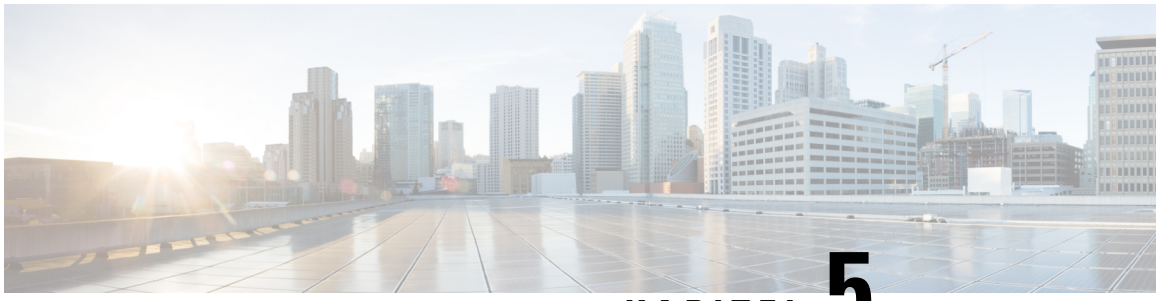
Schritt 1 Bearbeiten Sie die Telefondatei `config.xml` in einem Text- oder XML-Editor.

Schritt 2 Fügen Sie das Tag **<Privacy_Header_N_ ua="na">*Wert*</Privacy_Header_N_>** ein, wobei N für die Durchwahlnummer (1–10) steht, und verwenden Sie einen der folgenden Werte.

- Standardwert: **Deaktiviert**
- **Keine**
- **Kopfzeile**
- **Sitzung**
- **Benutzer**
- **ID**

Schritt 3 (optional) Stellen Sie etwaige weitere Durchwahlen mit dem gleichen Tag und der Durchwahlnummer bereit.

Schritt 4 Speichern Sie die Änderungen an der Datei `config.xml`.



KAPITEL 5

Bereitstellungsparameter

Bereitstellungsparameter – Übersicht

In diesem Kapitel werden die Bereitstellungsparameter erläutert, die in Konfigurationsprofilskripts verwendet werden können.

Konfigurationsprofilparameter

In der folgenden Tabelle werden die Funktion und Verwendung der einzelnen Parameter im Abschnitt **Konfigurationsprofilparameter** auf der Registerkarte **Bereitstellung** definiert.

Parametername	Beschreibung und Standardwert
Provision Enable (Bereitstellung aktivieren)	Alle Resynchronisierungsaktionen werden unabhängig von Firmware-Upgrade-Aktionen gesteuert. Wählen Sie **Ja** aus, um die Remotebereitstellung zu aktivieren. Der Standardwert lautet „Ja“.
Resync On Reset (Resynchronisierung nach Neustart)	Nach jedem Neustart wird eine Neusynchronisierung ausgelöst. Ausnahmen sind Neustarts als Folge von Parameteraktualisierungen und Firmware-Upgrades. Der Standardwert lautet „Ja“.

Parametername	Beschreibung und Standardwert
Resync Random Delay (Zufällige Resynchronisierungsverzögerung)	Eine zufällige Verzögerung (in Sekunden) nach dem Einschalten bevor der Neustart ausgeführt wird. In einem Pool mit IP-Telefoniegeräten, die planmäßig gleichzeitig gestartet werden, werden die Zeiten verteilt, zu denen jede Einheit eine Resynchronisierungsanforderung an den Bereitstellungsserver sendet. Diese Funktion kann bei einer großen lokalen Bereitstellung nützlich sein, wenn ein Stromausfall auftritt. Der Wert für dieses Feld muss eine Ganzzahl zwischen 0 und 65535 sein. Standardwert: 2.
Erneute Synchronisierung um (HHmm)	Die Zeitdauer der erneuten Synchronisierung des Geräts mit dem Bereitstellungsserver in Stunden und Minuten (HHmm). Der Wert für dieses Feld muss eine vierstellige Zahl im Bereich von 0000 bis 2400 sein, um die Uhrzeit im Format HHmm anzugeben. Beispielsweise steht 0959 für 09:59. Der Standardwert ist leer. Wenn der Wert ungültig ist, wird der Parameter ignoriert. Wenn dieser Parameter auf einen gültigen Wert festgelegt ist, wird der Parameter für die regelmäßige Resynchronisierung ignoriert.
Resync At Random Delay (Zufällige Verzögerung für die erneute Synchronisierung)	Verhindert eine Überlastung des Bereitstellungsservers, wenn eine große Anzahl an Geräten gleichzeitig eingeschaltet wird. Um zu verhindern, dass der Server mit Anforderungen für Resynchronisierungen von mehreren Telefonen überlastet wird, startet das Telefon die Resynchronisierung innerhalb des Bereichs der angegebenen Stunden und Minuten, plus ggf. die zufällige Verzögerungszeit (hhmm, hhmm + zufällige Verzögerung). Wenn beispielsweise die zufällige Verzögerung = (Erneute Synchronisierung bei zufälliger Verzögerung + 30)/60 Minuten beträgt, wird der eingegebene Wert in Sekunden in Minuten umgewandelt und auf die nächste volle Minute aufgerundet, um das endgültige Intervall der zufälligen Verzögerung zu berechnen. Der gültige Wert liegt zwischen 0 und 65535. Wenn Sie den Parameter auf 0 setzen, wird die Funktion deaktiviert. Der Standardwert ist 600 Sekunden (10 Minuten).

Parametername	Beschreibung und Standardwert
Resync Periodic (Periodische Resynchronisierung)	Zeitintervall zwischen periodischen Resynchronisierungen mit dem Bereitstellungsserver. Der zugehörige Timer für die Resynchronisierung wird erst nach der ersten erfolgreichen Synchronisierung mit dem Server aktiviert. Dies sind die gültigen Formate: • Eine Ganzzahl Beispiel: Die Eingabe von **3000** gibt an, dass die nächste erneute Synchronisierung in 3000 Sekunden stattfindet. • Mehrere Ganzzahlen Beispiel: Die Eingabe von **600, 1200, 300** gibt an, dass die erste erneute Synchronisierung in 600 Sekunden stattfindet, die zweite erneute Synchronisierung in 1200 Sekunden nach der ersten und die dritte erneute Synchronisierung in 300 Sekunden nach der zweiten. • Zeitbereich Beispiel: Die Eingabe von **2400 + 30** gibt an, dass die nächste erneute Synchronisierung zwischen 2400 und 2430 Sekunden nach einer erfolgreichen erneuten Synchronisierung erfolgt. Setzen Sie diesen Parameter auf 0, um die regelmäßige Resynchronisierung zu deaktivieren. Der Standardwert beträgt 3600 Sekunden.

Parametername	Beschreibung und Standardwert
Resync Error Retry Delay (Wiederholungsverzögerung bei fehlgeschlagener Resynchronisierung)	Wenn eine Resynchronisierung fehlschlägt, weil das IP-Telefoniegerät kein Profil vom Server abrufen konnte, die heruntergeladene Datei beschädigt ist oder ein interner Fehler auftritt, versucht das Gerät, erneut eine Resynchronisierung nach der in Sekunden festgelegten Zeitdauer auszuführen. Dies sind die gültigen Formate: • Eine Ganzzahl Beispiel: Die Eingabe von **300** gibt an, dass die nächste Wiederholung für die erneute Synchronisierung in 300 Sekunden auftritt. • Mehrere Ganzzahlen Beispiel: Die Eingabe von **600, 1200, 300** gibt an, dass die erste Wiederholung in 600 Sekunden nach dem Fehler stattfindet, die zweite Wiederholung in 1200 Sekunden nach dem Fehler der ersten Wiederholung und die dritte Wiederholung in 300 Sekunden nach dem Fehler der zweiten Wiederholung. • Zeitbereich Beispiel: Die Eingabe von **2400 + 30** gibt an, dass die nächste Wiederholung zwischen 2400 und 2430 Sekunden nach einer fehlerhaften erneuten Synchronisierung stattfindet. Wenn die Verzögerung auf 0 festgelegt ist, führt das Gerät keine erneute Synchronisierung aus, nachdem eine erneute Synchronisierung fehlgeschlagen ist.

Parametername	Beschreibung und Standardwert
Forced Resync Delay (Erzwungene Resynchronisierungsverzögerung)	Höchstwert für die Verzögerung (in Sekunden), bis das Telefon eine Resynchronisierung durchführt. Das Gerät führt keine Resynchronisierung durch, solange eine der Telefonleitungen aktiv ist. Da eine Resynchronisierung mehrere Sekunden dauern kann, sollte das Gerät vor der Resynchronisierung längere Zeit inaktiv gewesen sein. So können Benutzer mehrere Anrufe nacheinander tätigen, ohne unterbrochen zu werden. Das Gerät verfügt über einen Timer, der rückwärts zu laufen beginnt, sobald alle Leitungen inaktiv sind. Dieser Parameter ist der Anfangswert des Zählers. Resynchronisierungen erfolgen erst, wenn der Zähler bei 0 angelangt ist. Der gültige Wert liegt zwischen 0 und 65535. Der Standardwert ist 14.400 Sekunden.
Resync From SIP (Resynchronisierung über SIP)	Eine Resynchronisierung kann von einer SIP-NOTIFY-Nachricht ausgelöst werden. Der Standardwert lautet „Ja“.
Resync After Upgrade Attempt (Resynchronisierung nach versuchtem Upgrade)	Aktiviert oder deaktiviert den Resynchronisierungsvorgang nach einer Aktualisierung. Wenn „Ja“ ausgewählt ist, wird eine Synchronisierung ausgelöst. Der Standardwert lautet „Ja“.
Resync Trigger 1, Resync Trigger 2 (Resynchronisierungs-Trigger 1, Resynchronisierungs-Trigger 2)	Konfigurierbare Bedingungen zum Auslösen einer Resynchronisierung. Eine Resynchronisierung wird ausgelöst, wenn die logische Gleichung in diesen Parametern TRUE ergibt. Der Standardwert ist „Leer“.
Resync Fails On FNF (Fehlgeschlagene Resynchronisierung aufgrund von FNF)	Eine erneute Synchronisierung wird als fehlgeschlagen betrachtet, wenn ein angefordertes Profil vom Server nicht empfangen wird. Dies kann mit diesem Parameter überschrieben werden. Wenn Sie **Nein** festlegen, akzeptiert das Gerät eine `Datei-nicht-gefunden`-Antwort vom Server als erfolgreiche Resynchronisierung. Der Standardwert lautet „Ja“.

Parametername	Beschreibung und Standardwert
Profilregel Profile Rule B (Profilregel B) Profile Rule C (Profilregel C) Profile Rule D (Profilregel D)	Jede Profilregel teilt dem Telefon eine Quelle mit, über die das Telefon ein Profil (Konfigurationsdatei) erhalten kann. Bei jedem erneuten Synchronisierungsvorgang wendet das Telefon alle Profile nacheinander an. Standard: **`/$PSN.xml`** Wenn Sie die AES-256-CBC-Verschlüsselung auf die Konfigurationsdateien anwenden, geben Sie den Verschlüsselungsschlüssel mit dem Keyword **`--key`** wie folgt an: **`[--key <encryption key>]`** Sie können den Verschlüsselungsschlüssel optional in Anführungszeichen (") einschließen.
DHCP Option To Use (Zu verwendende DHCP-Option)	Durch Kommas getrennte DHCP-Optionen, die zum Abrufen der Firmware und Profile verwendet werden. Der Standardwert ist 66,160,159,150,60,43,125.
Protokollmeldung über Anfragen	Dieser Parameter enthält die Nachricht, die zu Beginn eines Resynchronisierungsversuchs an den Syslog-Server gesendet wird. Der Standardwert ist `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`.
Protokollmeldung über erfolgreiche Synchronisierung	Die syslog-Meldung, die nach dem erfolgreichen Abschluss eines Resynchronisierungsversuchs ausgegeben wird. Der Standardwert ist `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Protokollmeldung über fehlgeschlagene Synchronisierung	Die syslog-Meldung, die nach dem Fehlschlagen eines Resynchronisierungsversuchs ausgegeben wird. Der Standardwert ist `$PN $MAC -- Resync failed: $ERR`.
Vom Benutzer konfigurierbare erneute Synchronisierung	Erlaubt dem Benutzer, das Telefon über den IP-Telefonbildschirm erneut zu synchronisieren. Der Standardwert lautet „Ja“.

Parameter für Firmware-Upgrades

In der folgenden Tabelle werden die Funktion und Verwendung der einzelnen Parameter im Abschnitt **Firmware-Upgrade** der Registerkarte **Bereitstellung** definiert.

Parametername	Beschreibung und Standardwert
Upgrade Enable (Upgrade aktivieren)	Mit dieser Option werden Firmware-Upgrade-Aktionen unabhängig von Resynchronisierungsaktionen aktiviert. Der Standardwert lautet „Ja“.
Upgrade Error Retry Delay (Wiederholungsverzögerung bei fehlgeschlagenem Upgrade)	Das Upgrade-Intervall (in Sekunden), das nach einem fehlgeschlagenen Upgrade angewendet wird. Das Gerät verfügt über einen Timer für fehlgeschlagene Firmware-Upgrades. Dieser wird nach einem fehlgeschlagenen Firmware-Upgrade-Versuch aktiviert wird. Der Wert dieses Parameters dient zur Initialisierung des Timers. Der nächste Firmware-Upgrade-Versuch erfolgt, wenn der Timer bei 0 angelangt ist. Der Standardwert ist 3600 Sekunden.
Upgrade Rule (Upgrade-Regel)	Ein Skript für das Firmware-Upgrade, das die Upgrade-Bedingungen und zugehörigen Firmware-URLs definiert. Das Skript verwendet die gleiche Syntax wie die Profilregel. Geben Sie die Upgrade-Regel im folgenden Format ein: **<tftp|http|https>://<ip address>/image/<load name>** Beispiel: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Wenn kein Protokoll angegeben ist, wird TFTP verwendet. Wenn kein Servername angegeben ist, wird der Host, der die URL anfordert, als Servername verwendet. Wenn kein Port angegeben ist, wird der Standardport verwendet (69 für TFTP, 80 für HTTP oder 443 für HTTPS). Der Standardwert lautet „Leer“.
Log Upgrade Request Msg (Protokollmeldung über Upgrade-Anfragen)	Diese Syslog-Meldung wird zu Beginn eines Firmware-Upgrade-Versuchs ausgegeben. Standard: `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg (Protokollmeldung über erfolgreiches Firmware-Upgrade)	Diese Syslog-Meldung wird nach erfolgreichem Abschluss eines Firmware-Upgrade-Versuchs ausgegeben. Der Standardwert ist `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.

Parametername	Beschreibung und Standardwert
Log Upgrade Failure Msg (Protokollmeldung über fehlgeschlagenes Firmware-Upgrade)	Diese Syslog-Meldung wird nach einem fehlgeschlagenen Firmware-Upgrade-Versuch ausgegeben. Der Standardwert ist `$PN $MAC -- Upgrade failed: $ERR`.
Peer-Firmware-Freigabe	Aktiviert oder deaktiviert die Peer-Firmware-Freigabe-Funktion. Wählen Sie **Ja** oder **Nein** aus, um die Funktion zu aktivieren bzw. deaktivieren. Standard: Yes (Ja)
Peer-Firmware-Freigabe-Log-Server	Gibt die IP-Adresse und den Port an, an die bzw. den die UDP-Nachricht gesendet wird. Beispiel: 10.98.76.123:514, dabei steht 10.98.76.123 für die IP-Adresse und 514 für die Portnummer.

Allgemeine Parameter

In der folgenden Tabelle werden die Funktion und Verwendung der einzelnen Parameter im Abschnitt **Allgemeine Parameter** der Registerkarte **Bereitstellung** definiert.

Parametername	Beschreibung und Standardwert
GPP A – GPP P	Die allgemeinen GPP_*-Parameter werden als freie Zeichenfolgen verwendet, die registriert werden, wenn die Telefone für die Interaktion mit einer bestimmten Bereitstellungsserverlösung konfiguriert werden. Die Parameter können mit verschiedenen Werten konfiguriert werden: • Verschlüsselungscodes. • URLs. • Statusinformationen für die mehrstufige Bereitstellung. • Vorlagen für POST-Anforderungen. • Zuordnungen von Parameter-Namensaliasen. • Teilweise Zeichenfolgenwerte, die in vollständige Parameterwerten zusammengefasst werden. Der Standardwert lautet „Leer“.

Makroerweiterungsvariablen

Bestimmte Makrovariablen werden in den folgenden Bereitstellungsparametern erkannt:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (unter bestimmten Bedingungen)

In diesen Parametern werden Syntaxarten wie $NAME oder $(NAME) erkannt und erweitert.

Unterzeichenfolgen von Makrovariablen können mit der Schreibweise $(NAME:p) und $(NAME:p:q) angegeben werden, wobei p und q nicht-negative Ganzzahlen sind (ab Version 2.0.11 verfügbar). Die resultierende Makroerweiterung erfolgt so, dass die Unterzeichenfolge ab Zeichenversatz p beginnt und eine Länge von q aufweist (bzw. bis zum Ende der Zeichenfolge verläuft, wenn q nicht angegeben ist). Wenn GPP_A beispielsweise ABCDEF enthält, wird $(A:2) zu CDEF und $(A:2:3) zu CDE erweitert.

Ein nicht erkannter Name wird nicht übersetzt, und die Form $NAME oder $(NAME) bleibt nach der Erweiterung unverändert im Parameterwert bestehen.

Parametername	Beschreibung und Standardwert
$	$$ wird auf ein einzelnes $-Zeichen erweitert.
A bis P	Durch den Inhalt der allgemeinen Parameter GPP_A bis GPP_P ersetzt.
SA bis SD	Durch spezielle Parameter GPP_SA bis GPP_SD ersetzt. Diese Parameter enthalten Schlüssel oder Kennwörter, die in der Bereitstellung verwendet werden. **Hinweis** $SA bis $SD werden als Argumente für den optionalen URL-Qualifizierer der Resynchronisierung erkannt, --Schlüssel.
MA	MAC-Adresse mit Hexadezimalzeichen in Kleinbuchstaben, z. B. 000e08aabbcc.
MAU	MAC-Adresse mit Hexadezimalzeichen in Großbuchstaben, z. B. 000E08AABBCC.
MAC	MAC-Adresse mit Hexadezimalzeichen in Kleinbuchstaben und Doppelpunkten, um die Hexadezimalzeichenpaare zu trennen. Zum Beispiel: 00:0e:08:aa:bb:cc.
PN	Produktname, Beispiel: CP-6841-3PCC.

Parametername	Beschreibung und Standardwert
PSN	Produktseriennummer, Beispiel: 6841-3PCC.
SN	Zeichenfolge der Seriennummer. Beispiel: 88012BA01234.
CCERT	SSL-Clientzertifikatstatus: installiert oder nicht installiert.
IP	IP-Adresse des Telefons innerhalb des lokalen Subnetzes. Beispiel: 192.168.1.100.
EXTIP	Externe IP-Adresse des Telefons, wie sie im Internet angezeigt wird. Beispiel: 66.43.16.52.
SWVER	Zeichenfolge der Software-Version, Beispiel: sip68xx.11-0-1MPP.
HWVER	Zeichenfolge der Hardware-Version. Beispiel: 2.0.1.
PRVST	Bereitstellungsstatus (numerische Zeichenfolge): -1 = explizite Anforderung für Resynchronisierung 0 = Resynchronisierung durchführen 1 = regelmäßige Resynchronisierung 2 = Resynchronisierung fehlgeschlagen, Neuversuch
UPGST	Upgrade-Status (numerische Zeichenfolge): 1 = erster Upgrade-Versuch 2 = Upgrade fehlgeschlagen, Neuversuch
UPGERR	Ergebnisnachricht (ERR) des vorherigen Upgrade-Versuchs; beispielsweise „http_get failed“.
PRVTMR	Sekunden seit dem letzten Resynchronisierungsversuch.
UPGTMR	Sekunden seit dem letzten Upgrade-Versuch.
REGTMR1	Sekunden, die vergangen sind, seitdem die Registrierung von Leitung 1 beim SIP-Server verloren ging.
REGTMR2	Sekunden, die vergangen sind, seitdem die Registrierung von Leitung 2 beim SIP-Server verloren ging.
UPGCOND	Name des älteren Makros.

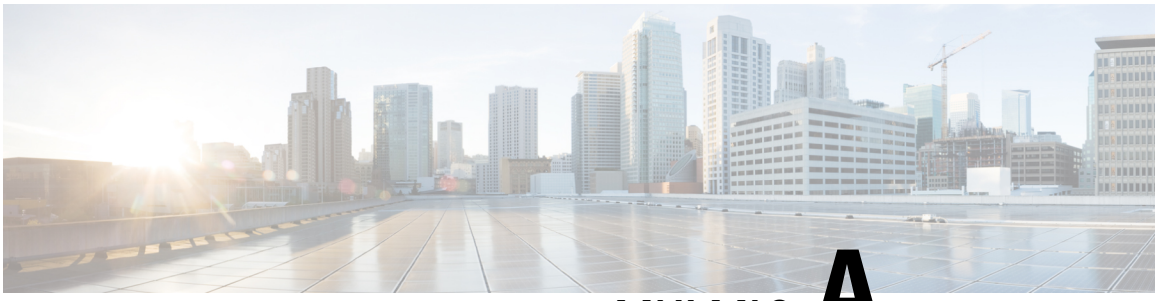
Parametername	Beschreibung und Standardwert
SCHEME	Dateizugriffsschema (entweder TFTP, HTTP oder HTTPS, ermittelt nach der Analyse der URL für die Resynchronisierung oder das Upgrade).
SERV	Host-Name des Anforderungszielservers, ermittelt nach der Analyse der URL für die Resynchronisierung oder das Upgrade.
SERVIP	IP-Adresse des Anforderungszielservers, ermittelt nach der Analyse der URL für die Resynchronisierung oder das Upgrade, möglicherweise nach der DNS-Suche.
Port	UDP-/TCP-Port des Anforderungsziels, ermittelt nach der Analyse der URL für die Resynchronisierung oder das Upgrade.
PATH	Dateipfad des Anforderungsziels, ermittelt nach der Analyse der URL für die Resynchronisierung oder das Upgrade.
ERR	Ergebnisnachricht bei Versuch der Resynchronisierung oder eines Upgrades. Nur bei der Generierung von Ergebnis-syslog-Nachrichten hilfreich. Der Wert wird im Falle von Upgrade-Versuchen in der Variablen UPGERR beibehalten.
UIDn	Der Wert des Benutzer-ID-Konfigurationsparameters für Leitung n
EMS	Extension Mobility-Status
MUID	Extension Mobility-Benutzer-ID
MPWD	Extension Mobility-Kennwort

Interne Fehlercodes

Auf dem Telefon werden eine Reihe von internen Fehlercodes (X00–X 99) definiert, um die Konfiguration für eine genauere Kontrolle über das Verhalten des Geräts unter bestimmten Fehlerbedingungen zu erleichtern.

Parametername	Beschreibung und Standardwert
X00	Transport Layer- (oder ICMP-)Fehler beim Senden einer SIP-Anforderung.
X20	Zeitüberschreitung der SIP-Anforderung beim Warten auf Antwort.

Parametername	Beschreibung und Standardwert
X40	Allgemeiner SIP-Protokollfehler (z. B. ungültiger Codec in SDP bei 200- und ACK-Nachrichten oder Zeitüberschreitung beim Warten auf ACK).
X60	Gewählte Nummer laut vorliegendem Rufnummernplan ungültig.



ANHANG A

Beispiel-Konfigurationsprofile

Beispiel für XML-Open-Format

```
<flat-profile>
 <!--  System Configuration  -->
<Restricted_Access_Domains ua="na"/>
<Enable_Web_Server ua="na">Yes</Enable_Web_Server>
<Enable_Protocol ua="na">Http</Enable_Protocol>
<!--  available options: Http|Https  -->
<Enable_Direct_Action_Url ua="na">Yes</Enable_Direct_Action_Url>
<Session_Max_Timeout ua="na">3600</Session_Max_Timeout>
<Session_Idle_Timeout ua="na">3600</Session_Idle_Timeout>
<Web_Server_Port ua="na">80</Web_Server_Port>
<Enable_Web_Admin_Access ua="na">Yes</Enable_Web_Admin_Access>
 <!--  <Admin_Password ua="na"/>  -->
 <!--  <User_Password ua="rw"/>  -->
<Phone-UI-readonly ua="na">No</Phone-UI-readonly>
<Phone-UI-User-Mode ua="na">No</Phone-UI-User-Mode>
<User_Password_Prompt ua="na">Yes</User_Password_Prompt>
<Block_Nonproxy_SIP ua="na">No</Block_Nonproxy_SIP>
 <!--  Power Settings  -->
<PoE_Power_Required ua="na">Normal</PoE_Power_Required>
<!--  available options: Normal|Maximum  -->
 <!--  Network Settings  -->
<IP_Mode ua="rw">Dual Mode</IP_Mode>
<!--  available options: IPv4 Only|IPv6 Only|Dual Mode  -->
 <!--  IPv4 Settings  -->
<Connection_Type ua="rw">DHCP</Connection_Type>
<!--  available options: DHCP|Static IP  -->
<Static_IP ua="rw"/>
<NetMask ua="rw"/>
<Gateway ua="rw"/>
<Primary_DNS ua="rw"/>
<Secondary_DNS ua="rw"/>
 <!--  IPv6 Settings  -->
<IPv6_Connection_Type ua="rw">DHCP</IPv6_Connection_Type>
<!--  available options: DHCP|Static IP  -->
<IPv6_Static_IP ua="rw"/>
<Prefix_Length ua="rw">1</Prefix_Length>
<IPv6_Gateway ua="rw"/>
<IPv6_Primary_DNS ua="rw"/>
<IPv6_Secondary_DNS ua="rw"/>
<Broadcast_Echo ua="rw">Disabled</Broadcast_Echo>
```

Beispiel-Konfigurationsprofile

```
<!--  available options: Disabled|Enabled  -->
<Auto_Config ua="rw">Enabled</Auto_Config>
<!--  available options: Disabled|Enabled  -->
 <!--  802.1X Authentication  -->
<Enable_802.1X_Authentication ua="rw">No</Enable_802.1X_Authentication>
 <!--  Optional Network Configuration  -->
<Host_Name ua="rw"/>
<Domain ua="rw"/>
<DNS_Server_Order ua="na">Manual,DHCP</DNS_Server_Order>
<!--  available options: Manual|Manual,DHCP|DHCP,Manual  -->
<DNS_Query_Mode ua="na">Parallel</DNS_Query_Mode>
<!--  available options: Parallel|Sequential  -->
<DNS_Caching_Enable ua="na">Yes</DNS_Caching_Enable>
<Switch_Port_Config ua="na">AUTO</Switch_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_Port_Config ua="na">AUTO</PC_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_PORT_Enable ua="na">Yes</PC_PORT_Enable>
<Enable_PC_Port_Mirror ua="na">No</Enable_PC_Port_Mirror>
<Syslog_Server ua="na"/>
<Syslog_Identifier ua="na">None</Syslog_Identifier>
<!--  available options: None|$MA|$MAU|$MAC|$SN  -->
<Debug_Level ua="na">NOTICE</Debug_Level>
<!--
 available options: EMERGENCY|ALERT|CRITICAL|ERROR|WARNING|NOTICE|INFO|DEBUG
-->
<Primary_NTP_Server ua="rw"/>
<Secondary_NTP_Server ua="rw"/>
<Enable_SSLv3 ua="na">No</Enable_SSLv3>
<Use_Config_TOS ua="na">No</Use_Config_TOS>
 <!--  VLAN Settings  -->
<Enable_VLAN ua="rw">No</Enable_VLAN>
<VLAN_ID ua="rw">1</VLAN_ID>
<PC_Port_VLAN_ID ua="na">1</PC_Port_VLAN_ID>
<Enable_CDP ua="na">Yes</Enable_CDP>
<Enable_LLDP-MED ua="na">Yes</Enable_LLDP-MED>
<Network_Startup_Delay ua="na">3</Network_Startup_Delay>
<DHCP_VLAN_Option ua="na"/>
 <!--  Wi-Fi Settings  -->
<Phone-wifi-on ua="rw">Yes</Phone-wifi-on>
<Phone-wifi-type ua="na">WLAN</Phone-wifi-type>
<!--  available options: WLAN|WPS  -->
 <!--  Wi-Fi Profile 1  -->
<Network_Name_1_ ua="rw">wipp</Network_Name_1_>
<Security_Mode_1_ ua="rw">Auto</Security_Mode_1_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_1_ ua="rw">user1</Wi-Fi_User_ID_1_>
 <!--
 <Wi-Fi_Password_1_ ua="rw">**********</Wi-Fi_Password_1_>
-->
 <!--  <WEP_Key_1_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_1_ ua="rw"/>  -->
<Frequency_Band_1_ ua="rw">Auto</Frequency_Band_1_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_1_ ua="rw">1</Wi-Fi_Profile_Order_1_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 2  -->
<Network_Name_2_ ua="rw">internet</Network_Name_2_>
```

```
<Security_Mode_2_ ua="rw">None</Security_Mode_2_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_2_ ua="rw"/>
 <!--  <Wi-Fi_Password_2_ ua="rw"/>  -->
 <!--  <WEP_Key_2_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_2_ ua="rw"/>  -->
<Frequency_Band_2_ ua="rw">Auto</Frequency_Band_2_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_2_ ua="rw">2</Wi-Fi_Profile_Order_2_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 3  -->
<Network_Name_3_ ua="rw"/>
<Security_Mode_3_ ua="rw">None</Security_Mode_3_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_3_ ua="rw"/>
 <!--  <Wi-Fi_Password_3_ ua="rw"/>  -->
 <!--  <WEP_Key_3_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_3_ ua="rw"/>  -->
<Frequency_Band_3_ ua="rw">Auto</Frequency_Band_3_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_3_ ua="rw">3</Wi-Fi_Profile_Order_3_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 4  -->
<Network_Name_4_ ua="rw"/>
<Security_Mode_4_ ua="rw">None</Security_Mode_4_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_4_ ua="rw"/>
 <!--  <Wi-Fi_Password_4_ ua="rw"/>  -->
 <!--  <WEP_Key_4_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_4_ ua="rw"/>  -->
<Frequency_Band_4_ ua="rw">Auto</Frequency_Band_4_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_4_ ua="rw">4</Wi-Fi_Profile_Order_4_>
<!--  available options: 1|2|3|4  -->
 <!--  Inventory Settings  -->
<Asset_ID ua="na"/>
 <!--  SIP Parameters  -->
<Max_Forward ua="na">70</Max_Forward>
<Max_Redirection ua="na">5</Max_Redirection>
<Max_Auth ua="na">2</Max_Auth>
<SIP_User_Agent_Name ua="na">$VERSION</SIP_User_Agent_Name>
<SIP_Server_Name ua="na">$VERSION</SIP_Server_Name>
<SIP_Reg_User_Agent_Name ua="na"/>
<SIP_Accept_Language ua="na"/>
<DTMF_Relay_MIME_Type ua="na">application/dtmf-relay</DTMF_Relay_MIME_Type>
<Hook_Flash_MIME_Type ua="na">application/hook-flash</Hook_Flash_MIME_Type>
<Remove_Last_Reg ua="na">No</Remove_Last_Reg>
<Use_Compact_Header ua="na">No</Use_Compact_Header>
<Escape_Display_Name ua="na">No</Escape_Display_Name>
<Talk_Package ua="na">No</Talk_Package>
<Hold_Package ua="na">No</Hold_Package>
<Conference_Package ua="na">No</Conference_Package>
<RFC_2543_Call_Hold ua="na">Yes</RFC_2543_Call_Hold>
<Random_REG_CID_on_Reboot ua="na">No</Random_REG_CID_on_Reboot>
<SIP_TCP_Port_Min ua="na">5060</SIP_TCP_Port_Min>
<SIP_TCP_Port_Max ua="na">5080</SIP_TCP_Port_Max>
<Caller_ID_Header ua="na">PAID-RPID-FROM</Caller_ID_Header>
<!--
```

Beispiel-Konfigurationsprofile

```
 available options: PAID-RPID-FROM|PAID-FROM|RPID-PAID-FROM|RPID-FROM|FROM
-->
<Hold_Target_Before_Refer ua="na">No</Hold_Target_Before_Refer>
<Dialog_SDP_Enable ua="na">No</Dialog_SDP_Enable>
<Keep_Referee_When_Refer_Failed ua="na">No</Keep_Referee_When_Refer_Failed>
<Display_Diversion_Info ua="na">No</Display_Diversion_Info>
<Display_Anonymous_From_Header ua="na">No</Display_Anonymous_From_Header>
<Sip_Accept_Encoding ua="na">none</Sip_Accept_Encoding>
<!--  available options: none|gzip  -->
<SIP_IP_Preference ua="na">IPv4</SIP_IP_Preference>
<!--  available options: IPv4|IPv6  -->
<Disable_Local_Name_To_Header ua="na">No</Disable_Local_Name_To_Header>
 <!--  SIP Timer Values (sec)  -->
<SIP_T1 ua="na">.5</SIP_T1>
<SIP_T2 ua="na">4</SIP_T2>
<SIP_T4 ua="na">5</SIP_T4>
<SIP_Timer_B ua="na">16</SIP_Timer_B>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
<SIP_Timer_H ua="na">16</SIP_Timer_H>
<SIP_Timer_D ua="na">16</SIP_Timer_D>
<SIP_Timer_J ua="na">16</SIP_Timer_J>
<INVITE_Expires ua="na">240</INVITE_Expires>
<ReINVITE_Expires ua="na">30</ReINVITE_Expires>
<Reg_Min_Expires ua="na">1</Reg_Min_Expires>
<Reg_Max_Expires ua="na">7200</Reg_Max_Expires>
<Reg_Retry_Intvl ua="na">30</Reg_Retry_Intvl>
<Reg_Retry_Long_Intvl ua="na">1200</Reg_Retry_Long_Intvl>
<Reg_Retry_Random_Delay ua="na">0</Reg_Retry_Random_Delay>
<Reg_Retry_Long_Random_Delay ua="na">0</Reg_Retry_Long_Random_Delay>
<Reg_Retry_Intvl_Cap ua="na">0</Reg_Retry_Intvl_Cap>
<Sub_Min_Expires ua="na">10</Sub_Min_Expires>
<Sub_Max_Expires ua="na">7200</Sub_Max_Expires>
<Sub_Retry_Intvl ua="na">10</Sub_Retry_Intvl>
 <!--  Response Status Code Handling  -->
<Try_Backup_RSC ua="na"/>
<Retry_Reg_RSC ua="na"/>
 <!--  RTP Parameters  -->
<RTP_Port_Min ua="na">16384</RTP_Port_Min>
<RTP_Port_Max ua="na">16482</RTP_Port_Max>
<RTP_Packet_Size ua="na">0.030</RTP_Packet_Size>
<Max_RTP_ICMP_Err ua="na">0</Max_RTP_ICMP_Err>
<RTCP_Tx_Interval ua="na">0</RTCP_Tx_Interval>
<SDP_IP_Preference ua="na">IPv4</SDP_IP_Preference>
<!--  available options: IPv4|IPv6  -->
 <!--  SDP Payload Types  -->
<G711u_Codec_Name ua="na">PCMU</G711u_Codec_Name>
<G711a_Codec_Name ua="na">PCMA</G711a_Codec_Name>
<G729a_Codec_Name ua="na">G729a</G729a_Codec_Name>
<G729b_Codec_Name ua="na">G729ab</G729b_Codec_Name>
<G722_Codec_Name ua="na">G722</G722_Codec_Name>
<G722.2_Codec_Name ua="na">AMR-WB</G722.2_Codec_Name>
<iLBC_Codec_Name ua="na">iLBC</iLBC_Codec_Name>
<OPUS_Codec_Name ua="na">OPUS</OPUS_Codec_Name>
<AVT_Codec_Name ua="na">telephone-event</AVT_Codec_Name>
<G722.2_Dynamic_Payload ua="na">96</G722.2_Dynamic_Payload>
<G722.2_OA_Dynamic_Payload ua="na">103</G722.2_OA_Dynamic_Payload>
<iLBC_Dynamic_Payload ua="na">97</iLBC_Dynamic_Payload>
<iLBC_30ms_Dynamic_Payload ua="na">105</iLBC_30ms_Dynamic_Payload>
<OPUS_Dynamic_Payload ua="na">99</OPUS_Dynamic_Payload>
<AVT_Dynamic_Payload ua="na">101</AVT_Dynamic_Payload>
<AVT_16kHz_Dynamic_Payload ua="na">107</AVT_16kHz_Dynamic_Payload>
<AVT_48kHz_Dynamic_Payload ua="na">108</AVT_48kHz_Dynamic_Payload>
<INFOREQ_Dynamic_Payload ua="na"/>
 <!--  NAT Support Parameters  -->
```

```
<Handle_VIA_received ua="na">No</Handle_VIA_received>
<Handle_VIA_rport ua="na">No</Handle_VIA_rport>
<Insert_VIA_received ua="na">No</Insert_VIA_received>
<Insert_VIA_rport ua="na">No</Insert_VIA_rport>
<Substitute_VIA_Addr ua="na">No</Substitute_VIA_Addr>
<Send_Resp_To_Src_Port ua="na">No</Send_Resp_To_Src_Port>
<STUN_Enable ua="na">No</STUN_Enable>
<STUN_Test_Enable ua="na">No</STUN_Test_Enable>
<STUN_Server ua="na"/>
<EXT_IP ua="na"/>
<EXT_RTP_Port_Min ua="na">0</EXT_RTP_Port_Min>
<NAT_Keep_Alive_Intvl ua="na">15</NAT_Keep_Alive_Intvl>
<Redirect_Keep_Alive ua="na">No</Redirect_Keep_Alive>
 <!--  Configuration Profile  -->
<Provision_Enable ua="na">Yes</Provision_Enable>
<Resync_On_Reset ua="na">Yes</Resync_On_Reset>
<Resync_Random_Delay ua="na">2</Resync_Random_Delay>
<Resync_At__HHmm_ ua="na"/>
<Resync_At_Random_Delay ua="na">30</Resync_At_Random_Delay>
<Resync_Periodic ua="na">60</Resync_Periodic>
<Resync_Error_Retry_Delay ua="na">360</Resync_Error_Retry_Delay>
<Forced_Resync_Delay ua="na">1440</Forced_Resync_Delay>
<Resync_From_SIP ua="na">Yes</Resync_From_SIP>
<Resync_After_Upgrade_Attempt ua="na">Yes</Resync_After_Upgrade_Attempt>
<Resync_Trigger_1 ua="na"/>
<Resync_Trigger_2 ua="na"/>
<User_Configurable_Resync ua="na">Yes</User_Configurable_Resync>
<Resync_Fails_On_FNF ua="na">Yes</Resync_Fails_On_FNF>
<Profile_Authentication_Type ua="na">Basic Http Authentication</Profile_Authentication_Type>
<!--
 available options: Disabled|Basic Http Authentication|XSI Authentication
-->
<Profile_Rule ua="na">/$PSN-a.xml</Profile_Rule>
<Profile_Rule_B ua="na">/$PSN-b.xml</Profile_Rule_B>
<Profile_Rule_C ua="na"/>
<Profile_Rule_D ua="na"/>
<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>
<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>
<Log_Request_Msg ua="na">
$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH
</Log_Request_Msg>
<Log_Success_Msg ua="na">
$PN $MAC -- Successful resync $SCHEME://$SERVIP:$PORT$PATH
</Log_Success_Msg>
<Log_Failure_Msg ua="na">$PN $MAC -- Resync failed: $ERR</Log_Failure_Msg>
 <!--  Upload Configuration Options  -->
<Report_Rule ua="na"/>
<HTTP_Report_Method ua="na">POST</HTTP_Report_Method>
<!--  available options: POST|PUT  -->
<Report_To_Server ua="na">On Request</Report_To_Server>
<!--
 available options: On Request|On Local Change|Periodically
-->
<Periodic_Upload_To_Server ua="na">3600</Periodic_Upload_To_Server>
<Upload_Delay_On_Local_Change ua="na">60</Upload_Delay_On_Local_Change>
 <!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na"/>
<Log_Upgrade_Request_Msg ua="na">
$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH
</Log_Upgrade_Request_Msg>
<Log_Upgrade_Success_Msg ua="na">
$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR
```

Beispiel-Konfigurationsprofile

```
</Log_Upgrade_Success_Msg>
<Log_Upgrade_Failure_Msg ua="na">$PN $MAC -- Upgrade failed: $ERR</Log_Upgrade_Failure_Msg>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Peer_Firmware_Sharing_Log_Server ua="na"/>
 <!--  CA Settings  -->
<Custom_CA_Rule ua="na"/>
 <!--  HTTP Settings  -->
<HTTP_User_Agent_Name ua="na">$VERSION ($MA)</HTTP_User_Agent_Name>
 <!--  Problem Report Tool  -->
<PRT_Upload_Rule ua="na"/>
<PRT_Upload_Method ua="na">POST</PRT_Upload_Method>
<!--  available options: POST|PUT  -->
<PRT_Max_Timer ua="na"/>
<PRT_Name ua="na"/>
 <!--  General Purpose Parameters  -->
<GPP_A ua="na"/>
<GPP_B ua="na"/>
<GPP_C ua="na"/>
<GPP_D ua="na"/>
<GPP_E ua="na"/>
<GPP_F ua="na"/>
<GPP_G ua="na"/>
<GPP_H ua="na"/>
<GPP_I ua="na"/>
<GPP_J ua="na"/>
<GPP_K ua="na"/>
<GPP_L ua="na"/>
<GPP_M ua="na"/>
<GPP_N ua="na"/>
<GPP_O ua="na"/>
<GPP_P ua="na"/>
 <!--  Call Progress Tones  -->
<Dial_Tone ua="na">350@-19,440@-19;10(*/0/1+2)</Dial_Tone>
<Outside_Dial_Tone ua="na">420@-16;10(*/0/1)</Outside_Dial_Tone>
<Prompt_Tone ua="na">520@-19,620@-19;10(*/0/1+2)</Prompt_Tone>
<Busy_Tone ua="na">480@-19,620@-19;10(.5/.5/1+2)</Busy_Tone>
<Reorder_Tone ua="na">480@-19,620@-19;10(.25/.25/1+2)</Reorder_Tone>
<Off_Hook_Warning_Tone ua="na">480@-10,620@0;10(.125/.125/1+2)</Off_Hook_Warning_Tone>
<Ring_Back_Tone ua="na">440@-19,480@-19;*(2/4/1+2)</Ring_Back_Tone>
<Call_Waiting_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Waiting_Tone>
<Confirm_Tone ua="na">600@-16;1(.25/.25/1)</Confirm_Tone>
<MWI_Dial_Tone ua="na">350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)</MWI_Dial_Tone>
<Cfwd_Dial_Tone ua="na">350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2)</Cfwd_Dial_Tone>
<Holding_Tone ua="na">600@-19;25(.1/.1/1,.1/.1/1,.1/9.5/1)</Holding_Tone>
<Conference_Tone ua="na">350@-19;20(.1/.1/1,.1/9.7/1)</Conference_Tone>
<Secure_Call_Indication_Tone
ua="na">397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2)</Secure_Call_Indication_Tone>
<Page_Tone ua="na">600@-16;.3(.05/0.05/1)</Page_Tone>
<Alert_Tone ua="na">600@-19;.2(.05/0.05/1)</Alert_Tone>
<Mute_Tone ua="na">600@-19;.2(.1/0.1/1)</Mute_Tone>
<Unmute_Tone ua="na">600@-19;.3(.1/0.1/1)</Unmute_Tone>
<System_Beep ua="na">600@-16;.1(.05/0.05/1)</System_Beep>
<Call_Pickup_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Pickup_Tone>
 <!--  Distinctive Ring Patterns  -->
<Cadence_1 ua="na">60(2/4)</Cadence_1>
<Cadence_2 ua="na">60(.3/.2,1/.2,.3/4)</Cadence_2>
<Cadence_3 ua="na">60(.8/.4,.8/4)</Cadence_3>
<Cadence_4 ua="na">60(.4/.2,.3/.2,.8/4)</Cadence_4>
<Cadence_5 ua="na">60(.2/.2,.2/.2,.2/.2,1/4)</Cadence_5>
<Cadence_6 ua="na">60(.2/.4,.2/.4,.2/4)</Cadence_6>
<Cadence_7 ua="na">60(4.5/4)</Cadence_7>
<Cadence_8 ua="na">60(0.25/9.75)</Cadence_8>
<Cadence_9 ua="na">60(.4/.2,.4/2)</Cadence_9>
 <!--  Control Timer Values (sec)  -->
```

```
<Reorder_Delay ua="na">255</Reorder_Delay>
<Interdigit_Long_Timer ua="na">10</Interdigit_Long_Timer>
<Interdigit_Short_Timer ua="na">3</Interdigit_Short_Timer>
 <!--  Vertical Service Activation Codes  -->
<Call_Return_Code ua="na">*69</Call_Return_Code>
<Blind_Transfer_Code ua="na">*95</Blind_Transfer_Code>
<Cfwd_All_Act_Code ua="na">*72</Cfwd_All_Act_Code>
<Cfwd_All_Deact_Code ua="na">*73</Cfwd_All_Deact_Code>
<Cfwd_Busy_Act_Code ua="na">*90</Cfwd_Busy_Act_Code>
<Cfwd_Busy_Deact_Code ua="na">*91</Cfwd_Busy_Deact_Code>
<Cfwd_No_Ans_Act_Code ua="na">*92</Cfwd_No_Ans_Act_Code>
<Cfwd_No_Ans_Deact_Code ua="na">*93</Cfwd_No_Ans_Deact_Code>
<CW_Act_Code ua="na">*56</CW_Act_Code>
<CW_Deact_Code ua="na">*57</CW_Deact_Code>
<CW_Per_Call_Act_Code ua="na">*71</CW_Per_Call_Act_Code>
<CW_Per_Call_Deact_Code ua="na">*70</CW_Per_Call_Deact_Code>
<Block_CID_Act_Code ua="na">*61</Block_CID_Act_Code>
<Block_CID_Deact_Code ua="na">*62</Block_CID_Deact_Code>
<Block_CID_Per_Call_Act_Code ua="na">*81</Block_CID_Per_Call_Act_Code>
<Block_CID_Per_Call_Deact_Code ua="na">*82</Block_CID_Per_Call_Deact_Code>
<Block_ANC_Act_Code ua="na">*77</Block_ANC_Act_Code>
<Block_ANC_Deact_Code ua="na">*87</Block_ANC_Deact_Code>
<DND_Act_Code ua="na">*78</DND_Act_Code>
<DND_Deact_Code ua="na">*79</DND_Deact_Code>
<Secure_All_Call_Act_Code ua="na">*16</Secure_All_Call_Act_Code>
<Secure_No_Call_Act_Code ua="na">*17</Secure_No_Call_Act_Code>
<Secure_One_Call_Act_Code ua="na">*18</Secure_One_Call_Act_Code>
<Secure_One_Call_Deact_Code ua="na">*19</Secure_One_Call_Deact_Code>
<Paging_Code ua="na">*96</Paging_Code>
<Call_Park_Code ua="na">*68</Call_Park_Code>
<Call_Pickup_Code ua="na">*97</Call_Pickup_Code>
<Call_Unpark_Code ua="na">*88</Call_Unpark_Code>
<Group_Call_Pickup_Code ua="na">*98</Group_Call_Pickup_Code>
<Referral_Services_Codes ua="na"/>
<Feature_Dial_Services_Codes ua="na"/>
 <!--  Vertical Service Announcement Codes  -->
<Service_Annc_Base_Number ua="na"/>
<Service_Annc_Extension_Codes ua="na"/>
 <!--  Outbound Call Codec Selection Codes  -->
<Prefer_G711u_Code ua="na">*017110</Prefer_G711u_Code>
<Force_G711u_Code ua="na">*027110</Force_G711u_Code>
<Prefer_G711a_Code ua="na">*017111</Prefer_G711a_Code>
<Force_G711a_Code ua="na">*027111</Force_G711a_Code>
<Prefer_G722_Code ua="na">*01722</Prefer_G722_Code>
<Force_G722_Code ua="na">*02722</Force_G722_Code>
<Prefer_G722.2_Code ua="na">*01724</Prefer_G722.2_Code>
<Force_G722.2_Code ua="na">*02724</Force_G722.2_Code>
<Prefer_G729a_Code ua="na">*01729</Prefer_G729a_Code>
<Force_G729a_Code ua="na">*02729</Force_G729a_Code>
<Prefer_iLBC_Code ua="na">*01016</Prefer_iLBC_Code>
<Force_iLBC_Code ua="na">*02016</Force_iLBC_Code>
<Prefer_OPUS_Code ua="na">*01056</Prefer_OPUS_Code>
<Force_OPUS_Code ua="na">*02056</Force_OPUS_Code>
 <!--  Time  -->
<Set_Local_Date__mm_dd_yyyy_ ua="na"/>
<Set_Local_Time__HH_mm_ ua="na"/>
<Time_Zone ua="na">GMT-06:00</Time_Zone>
<!--
 available options:
[illegible]

-->
<Time_Offset__HH_mm_ ua="na">-00/08</Time_Offset__HH_mm_>
<Ignore_DHCP_Time_Offset ua="na">Yes</Ignore_DHCP_Time_Offset>
```

Beispiel-Konfigurationsprofile

```
<Daylight_Saving_Time_Rule
ua="na">start=3/-1/7/2;end=10/-1/7/2;save=1</Daylight_Saving_Time_Rule>
<Daylight_Saving_Time_Enable ua="na">Yes</Daylight_Saving_Time_Enable>
 <!--  Language  -->
<Dictionary_Server_Script ua="na"/>
<Language_Selection ua="na">English-US</Language_Selection>
<Locale ua="na">en-US</Locale>
<!--
 available options:
en-US|en-CA|en-AU|en-GB|fr-FR|fr-CA|es-ES|it-IT|de-DE|nn-NO|pt-PT|nl-NL|sv-SE|pt-BZ|es-MX|en-NZ|da-DK|ru-RU|pl-PL|tr-TR|cs-CZ|hu-HU|fi-FI|sk-SK|bg-BG|hr-HR|ja-JP|ko-KR|zh-CN|zh-HK

-->
 <!--  General  -->
<Station_Name ua="na">arupiSSomSok</Station_Name>
<Station_Display_Name ua="na">RCDN Time</Station_Display_Name>
<Voice_Mail_Number ua="na"/>
<WideBand_Handset_Enable ua="na">No</WideBand_Handset_Enable>
 <!--  Video Configuration  -->
 <!--  Handsfree  -->
<Bluetooth_Mode ua="na">Phone</Bluetooth_Mode>
<!--  available options: Phone|Handsfree|Both  -->
<Line ua="na">5</Line>
<!--
 available options: 1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|Disabled
-->
<Extension_1_ ua="na">1</Extension_1_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_1_ ua="na">$USER hot</Short_Name_1_>
<Share_Call_Appearance_1_ ua="na">private</Share_Call_Appearance_1_>
<!--  available options: private|shared  -->
<Extended_Function_1_ ua="na"/>
<Extension_2_ ua="na">2</Extension_2_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_2_ ua="na">$USER</Short_Name_2_>
<Share_Call_Appearance_2_ ua="na">private</Share_Call_Appearance_2_>
<!--  available options: private|shared  -->
<Extended_Function_2_ ua="na"/>
<Extension_3_ ua="na">3</Extension_3_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_3_ ua="na">$USER</Short_Name_3_>
<Share_Call_Appearance_3_ ua="na">private</Share_Call_Appearance_3_>
<!--  available options: private|shared  -->
<Extended_Function_3_ ua="na"/>
<Extension_4_ ua="na">4</Extension_4_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_4_ ua="na">$USER</Short_Name_4_>
<Share_Call_Appearance_4_ ua="na">private</Share_Call_Appearance_4_>
<!--  available options: private|shared  -->
<Extended_Function_4_ ua="na"/>
 <!--  Miscellaneous Line Key Settings  -->
<Line_ID_Mapping ua="na">Vertical First</Line_ID_Mapping>
<!--  available options: Horizontal First|Vertical First  -->
<SCA_Barge-In-Enable ua="na">No</SCA_Barge-In-Enable>
<SCA_Sticky_Auto_Line_Seize ua="na">No</SCA_Sticky_Auto_Line_Seize>
<Call_Appearances_Per_Line ua="na">2</Call_Appearances_Per_Line>
<!--  available options: 2|3|4|5|6|7|8|9|10  -->
 <!--  Supplementary Services  -->
<Conference_Serv ua="na">Yes</Conference_Serv>
<Attn_Transfer_Serv ua="na">Yes</Attn_Transfer_Serv>
<Blind_Transfer_Serv ua="na">Yes</Blind_Transfer_Serv>
<DND_Serv ua="na">Yes</DND_Serv>
<Block_ANC_Serv ua="na">Yes</Block_ANC_Serv>
<Block_CID_Serv ua="na">Yes</Block_CID_Serv>
<Secure_Call_Serv ua="na">Yes</Secure_Call_Serv>
```

```
<Cfwd_All_Serv ua="na">Yes</Cfwd_All_Serv>
<Cfwd_Busy_Serv ua="na">Yes</Cfwd_Busy_Serv>
<Cfwd_No_Ans_Serv ua="na">Yes</Cfwd_No_Ans_Serv>
<Paging_Serv ua="na">Yes</Paging_Serv>
<Call_Park_Serv ua="na">Yes</Call_Park_Serv>
<Call_Pick_Up_Serv ua="na">Yes</Call_Pick_Up_Serv>
<ACD_Login_Serv ua="na">No</ACD_Login_Serv>
<Group_Call_Pick_Up_Serv ua="na">Yes</Group_Call_Pick_Up_Serv>
<Service_Annc_Serv ua="na">No</Service_Annc_Serv>
<Call_Recording_Serv ua="na">No</Call_Recording_Serv>
<Reverse_Phone_Lookup_Serv ua="na">Yes</Reverse_Phone_Lookup_Serv>
 <!--  Ringtone  -->
<Ring1 ua="na">n=Sunrise;w=file://Sunrise.rwb;c=1</Ring1>
<Ring2 ua="na">n=Chirp 1;w=file://chirp1.raw;c=1</Ring2>
<Ring3 ua="na">n=Chirp 2;w=file://chirp2.raw;c=1</Ring3>
<Ring4 ua="na">n=Delight;w=file://Delight.rwb;c=1</Ring4>
<Ring5 ua="na">n=Evolve;w=file://Evolve.rwb;c=1</Ring5>
<Ring6 ua="na">n=Mellow;w=file://Mellow.rwb;c=1</Ring6>
<Ring7 ua="na">n=Mischief;w=file://Mischief.rwb;c=1</Ring7>
<Ring8 ua="na">n=Reflections;w=file://Reflections.rwb;c=1</Ring8>
<Ring9 ua="na">n=Ringer;w=file://Ringer.rwb;c=1</Ring9>
<Ring10 ua="na">n=Ascent;w=file://Ascent.rwb;c=1</Ring10>
<Ring11 ua="na">n=Are you there;w=file://AreYouThereF.raw;c=1</Ring11>
<Ring12 ua="na">n=Chime;w=file://Chime.raw;c=1</Ring12>
<Silent_Ring_Duration ua="na">60</Silent_Ring_Duration>
 <!--  Extension Mobility  -->
<EM_Enable ua="na">No</EM_Enable>
<EM_User_Domain ua="na"/>
<Session_Timer_m_ ua="na">480</Session_Timer_m_>
<Countdown_Timer_s_ ua="na">10</Countdown_Timer_s_>
<Preferred_Password_Input_Mode ua="na">Alpha-numeric</Preferred_Password_Input_Mode>
<!--  available options: Alphanumeric|Numeric  -->
 <!--  XSI Phone Service  -->
<XSI_Host_Server ua="na"/>
<XSI_Authentication_Type ua="na">Login Credentials</XSI_Authentication_Type>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID ua="na"/>
 <!--  <Login_Password ua="na"/>  -->
<SIP_Auth_ID ua="na"/>
 <!--  <SIP_Password ua="na"/>  -->
<Directory_Enable ua="na">No</Directory_Enable>
<Directory_Name ua="na"/>
<Directory_Type ua="na">Enterprise</Directory_Type>
<!--
 available options: Enterprise|Group|Personal|Enterprise Common|Group Common
-->
<CallLog_Enable ua="na">No</CallLog_Enable>
<CallLog_Associated_Line ua="na">1</CallLog_Associated_Line>
<!--  available options: 1|2|3|4  -->
<Display_Recents_From ua="na">Phone</Display_Recents_From>
<!--  available options: Phone|Server  -->
 <!--  Broadsoft XMPP  -->
<XMPP_Enable ua="na">No</XMPP_Enable>
<XMPP_Server ua="na"/>
<XMPP_Port ua="na">5222</XMPP_Port>
<XMPP_User_ID ua="na"/>
 <!--  <XMPP_Password ua="na"/>  -->
<Login_Invisible ua="na">No</Login_Invisible>
<XMPP_Retry_Interval ua="na">30</XMPP_Retry_Interval>
 <!--  Informacast  -->
<Page_Service_URL ua="na"/>
 <!--  XML Service  -->
```

Beispiel-Konfigurationsprofile

```
<XML_Directory_Service_Name ua="na"/>
<XML_Directory_Service_URL ua="na"/>
<XML_Application_Service_Name ua="na"/>
<XML_Application_Service_URL ua="na"/>
<XML_User_Name ua="na"/>
 <!--  <XML_Password ua="na"/>  -->
<CISCO_XML_EXE_Enable ua="na">No</CISCO_XML_EXE_Enable>
<CISCO_XML_EXE_Auth_Mode ua="na">Local Credential</CISCO_XML_EXE_Auth_Mode>
<!--
 available options: Trusted|Local Credential|Remote Credential
-->
 <!--  Multiple Paging Group Parameters  -->
<Group_Paging_Script ua="na">
pggrp=224.168.168.168:34560;name=All;num=800;listen=yes;
</Group_Paging_Script>
 <!--  LDAP  -->
<LDAP_Dir_Enable ua="na">No</LDAP_Dir_Enable>
<LDAP_Corp_Dir_Name ua="na"/>
<LDAP_Server ua="na"/>
<LDAP_Search_Base ua="na"/>
<LDAP_Client_DN ua="na"/>
<LDAP_Username ua="na"/>
 <!--  <LDAP_Password ua="na"/>  -->
<LDAP_Auth_Method ua="na">None</LDAP_Auth_Method>
<!--  available options: None|Simple|DIGEST-MD5  -->
<LDAP_Last_Name_Filter ua="na"/>
<LDAP_First_Name_Filter ua="na"/>
<LDAP_Search_Item_3 ua="na"/>
<LDAP_Item_3_Filter ua="na"/>
<LDAP_Search_Item_4 ua="na"/>
<LDAP_Item_4_Filter ua="na"/>
<LDAP_Display_Attrs ua="na"/>
<LDAP_Number_Mapping ua="na"/>
 <!--  Programmable Softkeys  -->
<Programmable_Softkey_Enable ua="na">No</Programmable_Softkey_Enable>
<Idle_Key_List ua="na">
em_login;acd_login;acd_logout;astate;avail;unavail;redial;recents;cfwd;dnd;lcr;pickup;gpickup;unpark;em_logout;guestin;guestout;
</Idle_Key_List>
<Missed_Call_Key_List ua="na">lcr|1;miss|4;</Missed_Call_Key_List>
<Off_Hook_Key_List ua="na">
option;redial;cancel;dir;cfwd;dnd;lcr;unpark;pickup;gpickup;
</Off_Hook_Key_List>
<Dialing_Input_Key_List
ua="na">option|1;call|2;delchar|3;cancel|4;left|5;right|6;</Dialing_Input_Key_List>
<Progressing_Key_List ua="na">endcall|2;</Progressing_Key_List>
<Connected_Key_List ua="na">
hold|1;endcall|2;conf|3;xfer|4;bxfer;confLx;xferLx;park;phold;crdstart;crdpause;crdresume;crdstop;dnd;
</Connected_Key_List>
<Start-Xfer_Key_List ua="na">hold|1;endcall|2;xfer|3;dnd;</Start-Xfer_Key_List>
<Start-Conf_Key_List ua="na">hold|1;endcall|2;conf|3;dnd;</Start-Conf_Key_List>
<Conferencing_Key_List ua="na">
hold|1;endcall|2;join|4;phold;crdstart|5;crdpause|5;crdresume|5;crdstop|6;dnd;
</Conferencing_Key_List>
<Releasing_Key_List ua="na">endcall|2;</Releasing_Key_List>
<Hold_Key_List ua="na">resume|1;endcall|2;newcall|3;redial;dir;cfwd;dnd;</Hold_Key_List>
<Ringing_Key_List ua="na">answer|1;ignore|2;</Ringing_Key_List>
<Shared_Active_Key_List
ua="na">newcall|1;barge|2;bargesilent|3;cfwd|4;dnd|5;</Shared_Active_Key_List>
<Shared_Held_Key_List ua="na">resume|1;barge|2;cfwd|3;dnd|4;</Shared_Held_Key_List>
<PSK_1 ua="na"/>
<PSK_2 ua="na"/>
<PSK_3 ua="na"/>
<PSK_4 ua="na"/>
<PSK_5 ua="na"/>
```

```
<PSK_6 ua="na"/>
<PSK_7 ua="na"/>
<PSK_8 ua="na"/>
<PSK_9 ua="na"/>
<PSK_10 ua="na"/>
<PSK_11 ua="na"/>
<PSK_12 ua="na"/>
<PSK_13 ua="na"/>
<PSK_14 ua="na"/>
<PSK_15 ua="na"/>
<PSK_16 ua="na"/>
 <!--  General  -->
<Line_Enable_1_ ua="na">Yes</Line_Enable_1_>
 <!--  Share Line Appearance  -->
<Share_Ext_1_ ua="na">No</Share_Ext_1_>
<Shared_User_ID_1_ ua="na"/>
<Subscription_Expires_1_ ua="na">3600</Subscription_Expires_1_>
<Restrict_MWI_1_ ua="na">No</Restrict_MWI_1_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_1_ ua="na">No</NAT_Mapping_Enable_1_>
<NAT_Keep_Alive_Enable_1_ ua="na">No</NAT_Keep_Alive_Enable_1_>
<NAT_Keep_Alive_Msg_1_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_1_>
<NAT_Keep_Alive_Dest_1_ ua="na">$PROXY</NAT_Keep_Alive_Dest_1_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_1_ ua="na">0x68</SIP_TOS_DiffServ_Value_1_>
<RTP_TOS_DiffServ_Value_1_ ua="na">0xb8</RTP_TOS_DiffServ_Value_1_>
 <!--  SIP Settings  -->
<SIP_Transport_1_ ua="na">UDP</SIP_Transport_1_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_1_ ua="na">5060</SIP_Port_1_>
<SIP_100REL_Enable_1_ ua="na">No</SIP_100REL_Enable_1_>
<EXT_SIP_Port_1_ ua="na">0</EXT_SIP_Port_1_>
<Auth_Resync-Reboot_1_ ua="na">Yes</Auth_Resync-Reboot_1_>
<SIP_Proxy-Require_1_ ua="na"/>
<SIP_Remote-Party-ID_1_ ua="na">No</SIP_Remote-Party-ID_1_>
<Referor_Bye_Delay_1_ ua="na">4</Referor_Bye_Delay_1_>
<Refer-To_Target_Contact_1_ ua="na">No</Refer-To_Target_Contact_1_>
<Referee_Bye_Delay_1_ ua="na">0</Referee_Bye_Delay_1_>
<Refer_Target_Bye_Delay_1_ ua="na">0</Refer_Target_Bye_Delay_1_>
<Sticky_183_1_ ua="na">No</Sticky_183_1_>
<Auth_INVITE_1_ ua="na">No</Auth_INVITE_1_>
<Ntfy_Refer_On_1xx-To-Inv_1_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_1_>
<Set_G729_annexb_1_ ua="na">yes</Set_G729_annexb_1_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_1_ ua="na"/>
<VQ_Report_Interval_1_ ua="na">0</VQ_Report_Interval_1_>
<User_Equal_Phone_1_ ua="na">No</User_Equal_Phone_1_>
<Call_Recording_Protocol_1_ ua="na">SIPREC</Call_Recording_Protocol_1_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_1_ ua="na">Disabled</Privacy_Header_1_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_1_ ua="na">No</P-Early-Media_Support_1_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_1_ ua="na">No</Blind_Attn-Xfer_Enable_1_>
<Message_Waiting_1_ ua="na">No</Message_Waiting_1_>
<Auth_Page_1_ ua="na">No</Auth_Page_1_>
<Default_Ring_1_ ua="rw">1</Default_Ring_1_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
```

Beispiel-Konfigurationsprofile

```
<Auth_Page_Realm_1_ ua="na"/>
<Conference_Bridge_URL_1_ ua="na"/>
<Conference_Single_Hardkey_1_ ua="na">No</Conference_Single_Hardkey_1_>
 <!--  <Auth_Page_Password_1_ ua="na"/>  -->
<Mailbox_ID_1_ ua="na"/>
<Voice_Mail_Server_1_ ua="na"/>
<Voice_Mail_Subscribe_Interval_1_ ua="na">86400</Voice_Mail_Subscribe_Interval_1_>
<Auto_Ans_Page_On_Active_Call_1_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_1_>
<Feature_Key_Sync_1_ ua="na">No</Feature_Key_Sync_1_>
<Call_Park_Monitor_Enable_1_ ua="na">No</Call_Park_Monitor_Enable_1_>
<Enable_Broadsoft_Hoteling_1_ ua="na">No</Enable_Broadsoft_Hoteling_1_>
<Hoteling_Subscription_Expires_1_ ua="na">3600</Hoteling_Subscription_Expires_1_>
<Secure_Call_Option_1_ ua="na">Optional</Secure_Call_Option_1_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_1_ ua="na">No</Broadsoft_ACD_1_>
<Call_Information_Enable_1_ ua="na">No</Call_Information_Enable_1_>
<Disposition_Code_Enable_1_ ua="na">No</Disposition_Code_Enable_1_>
<Trace_Enable_1_ ua="na">No</Trace_Enable_1_>
<Emergency_Escalation_Enable_1_ ua="na">No</Emergency_Escalation_Enable_1_>
<Queue_Status_Notification_Enable_1_ ua="na">No</Queue_Status_Notification_Enable_1_>
 <!--  Proxy and Registration  -->
<Proxy_1_ ua="na">as1bsoft.sipurash.com</Proxy_1_>
<Outbound_Proxy_1_ ua="na"/>
<Alternate_Proxy_1_ ua="na"/>
<Alternate_Outbound_Proxy_1_ ua="na"/>
<Use_OB_Proxy_In_Dialog_1_ ua="na">Yes</Use_OB_Proxy_In_Dialog_1_>
<Register_1_ ua="na">Yes</Register_1_>
<Make_Call_Without_Reg_1_ ua="na">No</Make_Call_Without_Reg_1_>
<Register_Expires_1_ ua="na">3600</Register_Expires_1_>
<Ans_Call_Without_Reg_1_ ua="na">No</Ans_Call_Without_Reg_1_>
<Use_DNS_SRV_1_ ua="na">No</Use_DNS_SRV_1_>
<DNS_SRV_Auto_Prefix_1_ ua="na">Yes</DNS_SRV_Auto_Prefix_1_>
<Proxy_Fallback_Intvl_1_ ua="na">3600</Proxy_Fallback_Intvl_1_>
<Proxy_Redundancy_Method_1_ ua="na">Normal</Proxy_Redundancy_Method_1_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_1_ ua="na">No</Dual_Registration_1_>
<Auto_Register_When_Failover_1_ ua="na">No</Auto_Register_When_Failover_1_>
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
 <!--  Subscriber Information  -->
<Display_Name_1_ ua="na"/>
<User_ID_1_ ua="na">4085263127</User_ID_1_>
 <!--  <Password_1_ ua="na">**************</Password_1_>  -->
<Auth_ID_1_ ua="na">AUN3127</Auth_ID_1_>
<Reversed_Auth_Realm_1_ ua="na"/>
<SIP_URI_1_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_1_ ua="na"/>
<XSI_Authentication_Type_1_ ua="na">Login Credentials</XSI_Authentication_Type_1_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_1_ ua="na"/>
 <!--  <Login_Password_1_ ua="na"/>  -->
<Anywhere_Enable_1_ ua="na">No</Anywhere_Enable_1_>
<Block_CID_Enable_1_ ua="na">No</Block_CID_Enable_1_>
<DND_Enable_1_ ua="na">No</DND_Enable_1_>
<CFWD_Enable_1_ ua="na">No</CFWD_Enable_1_>
 <!--  Audio Configuration  -->
<Preferred_Codec_1_ ua="na">G711u</Preferred_Codec_1_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_1_ ua="na">No</Use_Pref_Codec_Only_1_>
```

```
<Second_Preferred_Codec_1_ ua="na">Unspecified</Second_Preferred_Codec_1_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_1_ ua="na">Unspecified</Third_Preferred_Codec_1_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_1_ ua="na">Yes</G711u_Enable_1_>
<G711a_Enable_1_ ua="na">Yes</G711a_Enable_1_>
<G729a_Enable_1_ ua="na">Yes</G729a_Enable_1_>
<G722_Enable_1_ ua="na">Yes</G722_Enable_1_>
<G722.2_Enable_1_ ua="na">Yes</G722.2_Enable_1_>
<iLBC_Enable_1_ ua="na">Yes</iLBC_Enable_1_>
<OPUS_Enable_1_ ua="na">Yes</OPUS_Enable_1_>
<Silence_Supp_Enable_1_ ua="na">No</Silence_Supp_Enable_1_>
<DTMF_Tx_Method_1_ ua="na">Auto</DTMF_Tx_Method_1_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_1_ ua="na">Default</Codec_Negotiation_1_>
<!--  available options: Default|List All  -->
<Encryption_Method_1_ ua="na">AES 128</Encryption_Method_1_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_1_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_1_>
<Caller_ID_Map_1_ ua="na"/>
<Enable_URI_Dialing_1_ ua="na">No</Enable_URI_Dialing_1_>
<Emergency_Number_1_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_1_ ua="na"/>
<Primary_Request_URL_1_ ua="na"/>
<Secondary_Request_URL_1_ ua="na"/>
 <!--  General  -->
<Line_Enable_2_ ua="na">Yes</Line_Enable_2_>
 <!--  Share Line Appearance  -->
<Share_Ext_2_ ua="na">No</Share_Ext_2_>
<Shared_User_ID_2_ ua="na"/>
<Subscription_Expires_2_ ua="na">3600</Subscription_Expires_2_>
<Restrict_MWI_2_ ua="na">No</Restrict_MWI_2_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_2_ ua="na">No</NAT_Mapping_Enable_2_>
<NAT_Keep_Alive_Enable_2_ ua="na">No</NAT_Keep_Alive_Enable_2_>
<NAT_Keep_Alive_Msg_2_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_2_>
<NAT_Keep_Alive_Dest_2_ ua="na">$PROXY</NAT_Keep_Alive_Dest_2_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_2_ ua="na">0x68</SIP_TOS_DiffServ_Value_2_>
<RTP_TOS_DiffServ_Value_2_ ua="na">0xb8</RTP_TOS_DiffServ_Value_2_>
 <!--  SIP Settings  -->
<SIP_Transport_2_ ua="na">UDP</SIP_Transport_2_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_2_ ua="na">5061</SIP_Port_2_>
<SIP_100REL_Enable_2_ ua="na">No</SIP_100REL_Enable_2_>
<EXT_SIP_Port_2_ ua="na">0</EXT_SIP_Port_2_>
<Auth_Resync-Reboot_2_ ua="na">Yes</Auth_Resync-Reboot_2_>
<SIP_Proxy-Require_2_ ua="na"/>
<SIP_Remote-Party-ID_2_ ua="na">No</SIP_Remote-Party-ID_2_>
<Referor_Bye_Delay_2_ ua="na">4</Referor_Bye_Delay_2_>
<Refer-To_Target_Contact_2_ ua="na">No</Refer-To_Target_Contact_2_>
<Referee_Bye_Delay_2_ ua="na">0</Referee_Bye_Delay_2_>
<Refer_Target_Bye_Delay_2_ ua="na">0</Refer_Target_Bye_Delay_2_>
```

Beispiel-Konfigurationsprofile

```
<Sticky_183_2_ ua="na">No</Sticky_183_2_>
<Auth_INVITE_2_ ua="na">No</Auth_INVITE_2_>
<Ntfy_Refer_On_1xx-To-Inv_2_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_2_>
<Set_G729_annexb_2_ ua="na">yes</Set_G729_annexb_2_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_2_ ua="na"/>
<VQ_Report_Interval_2_ ua="na">0</VQ_Report_Interval_2_>
<User_Equal_Phone_2_ ua="na">No</User_Equal_Phone_2_>
<Call_Recording_Protocol_2_ ua="na">SIPREC</Call_Recording_Protocol_2_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_2_ ua="na">Disabled</Privacy_Header_2_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_2_ ua="na">No</P-Early-Media_Support_2_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_2_ ua="na">No</Blind_Attn-Xfer_Enable_2_>
<Message_Waiting_2_ ua="na">No</Message_Waiting_2_>
<Auth_Page_2_ ua="na">No</Auth_Page_2_>
<Default_Ring_2_ ua="rw">1</Default_Ring_2_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_2_ ua="na"/>
<Conference_Bridge_URL_2_ ua="na"/>
<Conference_Single_Hardkey_2_ ua="na">No</Conference_Single_Hardkey_2_>
 <!--  <Auth_Page_Password_2_ ua="na"/>  -->
<Mailbox_ID_2_ ua="na"/>
<Voice_Mail_Server_2_ ua="na"/>
<Voice_Mail_Subscribe_Interval_2_ ua="na">86400</Voice_Mail_Subscribe_Interval_2_>
<Auto_Ans_Page_On_Active_Call_2_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_2_>
<Feature_Key_Sync_2_ ua="na">No</Feature_Key_Sync_2_>
<Call_Park_Monitor_Enable_2_ ua="na">No</Call_Park_Monitor_Enable_2_>
<Enable_Broadsoft_Hoteling_2_ ua="na">No</Enable_Broadsoft_Hoteling_2_>
<Hoteling_Subscription_Expires_2_ ua="na">3600</Hoteling_Subscription_Expires_2_>
<Secure_Call_Option_2_ ua="na">Optional</Secure_Call_Option_2_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_2_ ua="na">No</Broadsoft_ACD_2_>
<Call_Information_Enable_2_ ua="na">No</Call_Information_Enable_2_>
<Disposition_Code_Enable_2_ ua="na">No</Disposition_Code_Enable_2_>
<Trace_Enable_2_ ua="na">No</Trace_Enable_2_>
<Emergency_Escalation_Enable_2_ ua="na">No</Emergency_Escalation_Enable_2_>
<Queue_Status_Notification_Enable_2_ ua="na">No</Queue_Status_Notification_Enable_2_>
 <!--  Proxy and Registration  -->
<Proxy_2_ ua="na">10.74.51.158</Proxy_2_>
<Outbound_Proxy_2_ ua="na"/>
<Alternate_Proxy_2_ ua="na"/>
<Alternate_Outbound_Proxy_2_ ua="na"/>
<Use_OB_Proxy_In_Dialog_2_ ua="na">Yes</Use_OB_Proxy_In_Dialog_2_>
<Register_2_ ua="na">Yes</Register_2_>
<Make_Call_Without_Reg_2_ ua="na">No</Make_Call_Without_Reg_2_>
<Register_Expires_2_ ua="na">360</Register_Expires_2_>
<Ans_Call_Without_Reg_2_ ua="na">No</Ans_Call_Without_Reg_2_>
<Use_DNS_SRV_2_ ua="na">No</Use_DNS_SRV_2_>
<DNS_SRV_Auto_Prefix_2_ ua="na">Yes</DNS_SRV_Auto_Prefix_2_>
<Proxy_Fallback_Intvl_2_ ua="na">3600</Proxy_Fallback_Intvl_2_>
<Proxy_Redundancy_Method_2_ ua="na">Normal</Proxy_Redundancy_Method_2_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_2_ ua="na">No</Dual_Registration_2_>
<Auto_Register_When_Failover_2_ ua="na">No</Auto_Register_When_Failover_2_>
<TLS_Name_Validate_2_ ua="na">Yes</TLS_Name_Validate_2_>
```

```
 <!--  Subscriber Information  -->
<Display_Name_2_ ua="na"/>
<User_ID_2_ ua="na">158165</User_ID_2_>
 <!--  <Password_2_ ua="na"/>  -->
<Auth_ID_2_ ua="na"/>
<Reversed_Auth_Realm_2_ ua="na"/>
<SIP_URI_2_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_2_ ua="na"/>
<XSI_Authentication_Type_2_ ua="na">Login Credentials</XSI_Authentication_Type_2_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_2_ ua="na"/>
 <!--  <Login_Password_2_ ua="na"/>  -->
<Anywhere_Enable_2_ ua="na">No</Anywhere_Enable_2_>
<Block_CID_Enable_2_ ua="na">No</Block_CID_Enable_2_>
<DND_Enable_2_ ua="na">No</DND_Enable_2_>
<CFWD_Enable_2_ ua="na">No</CFWD_Enable_2_>
 <!--  Audio Configuration  -->
<Preferred_Codec_2_ ua="na">G711u</Preferred_Codec_2_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_2_ ua="na">No</Use_Pref_Codec_Only_2_>
<Second_Preferred_Codec_2_ ua="na">Unspecified</Second_Preferred_Codec_2_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_2_ ua="na">Unspecified</Third_Preferred_Codec_2_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_2_ ua="na">Yes</G711u_Enable_2_>
<G711a_Enable_2_ ua="na">Yes</G711a_Enable_2_>
<G729a_Enable_2_ ua="na">Yes</G729a_Enable_2_>
<G722_Enable_2_ ua="na">Yes</G722_Enable_2_>
<G722.2_Enable_2_ ua="na">Yes</G722.2_Enable_2_>
<iLBC_Enable_2_ ua="na">Yes</iLBC_Enable_2_>
<OPUS_Enable_2_ ua="na">Yes</OPUS_Enable_2_>
<Silence_Supp_Enable_2_ ua="na">No</Silence_Supp_Enable_2_>
<DTMF_Tx_Method_2_ ua="na">Auto</DTMF_Tx_Method_2_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_2_ ua="na">Default</Codec_Negotiation_2_>
<!--  available options: Default|List All  -->
<Encryption_Method_2_ ua="na">AES 128</Encryption_Method_2_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_2_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_2_>
<Caller_ID_Map_2_ ua="na"/>
<Enable_URI_Dialing_2_ ua="na">No</Enable_URI_Dialing_2_>
<Emergency_Number_2_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_2_ ua="na"/>
<Primary_Request_URL_2_ ua="na"/>
<Secondary_Request_URL_2_ ua="na"/>
 <!--  General  -->
<Line_Enable_3_ ua="na">Yes</Line_Enable_3_>
 <!--  Share Line Appearance  -->
```

Beispiel-Konfigurationsprofile

```
<Share_Ext_3_ ua="na">No</Share_Ext_3_>
<Shared_User_ID_3_ ua="na"/>
<Subscription_Expires_3_ ua="na">3600</Subscription_Expires_3_>
<Restrict_MWI_3_ ua="na">No</Restrict_MWI_3_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_3_ ua="na">No</NAT_Mapping_Enable_3_>
<NAT_Keep_Alive_Enable_3_ ua="na">No</NAT_Keep_Alive_Enable_3_>
<NAT_Keep_Alive_Msg_3_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_3_>
<NAT_Keep_Alive_Dest_3_ ua="na">$PROXY</NAT_Keep_Alive_Dest_3_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_3_ ua="na">0x68</SIP_TOS_DiffServ_Value_3_>
<RTP_TOS_DiffServ_Value_3_ ua="na">0xb8</RTP_TOS_DiffServ_Value_3_>
 <!--  SIP Settings  -->
<SIP_Transport_3_ ua="na">UDP</SIP_Transport_3_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_3_ ua="na">5062</SIP_Port_3_>
<SIP_100REL_Enable_3_ ua="na">No</SIP_100REL_Enable_3_>
<EXT_SIP_Port_3_ ua="na">0</EXT_SIP_Port_3_>
<Auth_Resync-Reboot_3_ ua="na">Yes</Auth_Resync-Reboot_3_>
<SIP_Proxy-Require_3_ ua="na"/>
<SIP_Remote-Party-ID_3_ ua="na">No</SIP_Remote-Party-ID_3_>
<Referor_Bye_Delay_3_ ua="na">4</Referor_Bye_Delay_3_>
<Refer-To_Target_Contact_3_ ua="na">No</Refer-To_Target_Contact_3_>
<Referee_Bye_Delay_3_ ua="na">0</Referee_Bye_Delay_3_>
<Refer_Target_Bye_Delay_3_ ua="na">0</Refer_Target_Bye_Delay_3_>
<Sticky_183_3_ ua="na">No</Sticky_183_3_>
<Auth_INVITE_3_ ua="na">No</Auth_INVITE_3_>
<Ntfy_Refer_On_1xx-To-Inv_3_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_3_>
<Set_G729_annexb_3_ ua="na">yes</Set_G729_annexb_3_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_3_ ua="na"/>
<VQ_Report_Interval_3_ ua="na">0</VQ_Report_Interval_3_>
<User_Equal_Phone_3_ ua="na">No</User_Equal_Phone_3_>
<Call_Recording_Protocol_3_ ua="na">SIPREC</Call_Recording_Protocol_3_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_3_ ua="na">Disabled</Privacy_Header_3_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_3_ ua="na">No</P-Early-Media_Support_3_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_3_ ua="na">No</Blind_Attn-Xfer_Enable_3_>
<Message_Waiting_3_ ua="na">No</Message_Waiting_3_>
<Auth_Page_3_ ua="na">No</Auth_Page_3_>
<Default_Ring_3_ ua="rw">1</Default_Ring_3_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_3_ ua="na"/>
<Conference_Bridge_URL_3_ ua="na"/>
<Conference_Single_Hardkey_3_ ua="na">No</Conference_Single_Hardkey_3_>
 <!--  <Auth_Page_Password_3_ ua="na"/>  -->
<Mailbox_ID_3_ ua="na"/>
<Voice_Mail_Server_3_ ua="na"/>
<Voice_Mail_Subscribe_Interval_3_ ua="na">86400</Voice_Mail_Subscribe_Interval_3_>
<Auto_Ans_Page_On_Active_Call_3_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_3_>
<Feature_Key_Sync_3_ ua="na">No</Feature_Key_Sync_3_>
<Call_Park_Monitor_Enable_3_ ua="na">No</Call_Park_Monitor_Enable_3_>
<Enable_Broadsoft_Hoteling_3_ ua="na">No</Enable_Broadsoft_Hoteling_3_>
<Hoteling_Subscription_Expires_3_ ua="na">3600</Hoteling_Subscription_Expires_3_>
<Secure_Call_Option_3_ ua="na">Optional</Secure_Call_Option_3_>
<!--  available options: Optional|Required  -->
```

```
 <!--  ACD Settings  -->
<Broadsoft_ACD_3_ ua="na">No</Broadsoft_ACD_3_>
<Call_Information_Enable_3_ ua="na">No</Call_Information_Enable_3_>
<Disposition_Code_Enable_3_ ua="na">No</Disposition_Code_Enable_3_>
<Trace_Enable_3_ ua="na">No</Trace_Enable_3_>
<Emergency_Escalation_Enable_3_ ua="na">No</Emergency_Escalation_Enable_3_>
<Queue_Status_Notification_Enable_3_ ua="na">No</Queue_Status_Notification_Enable_3_>
 <!--  Proxy and Registration  -->
<Proxy_3_ ua="na"/>
<Outbound_Proxy_3_ ua="na"/>
<Alternate_Proxy_3_ ua="na"/>
<Alternate_Outbound_Proxy_3_ ua="na"/>
<Use_OB_Proxy_In_Dialog_3_ ua="na">Yes</Use_OB_Proxy_In_Dialog_3_>
<Register_3_ ua="na">Yes</Register_3_>
<Make_Call_Without_Reg_3_ ua="na">No</Make_Call_Without_Reg_3_>
<Register_Expires_3_ ua="na">3600</Register_Expires_3_>
<Ans_Call_Without_Reg_3_ ua="na">No</Ans_Call_Without_Reg_3_>
<Use_DNS_SRV_3_ ua="na">No</Use_DNS_SRV_3_>
<DNS_SRV_Auto_Prefix_3_ ua="na">Yes</DNS_SRV_Auto_Prefix_3_>
<Proxy_Fallback_Intvl_3_ ua="na">3600</Proxy_Fallback_Intvl_3_>
<Proxy_Redundancy_Method_3_ ua="na">Normal</Proxy_Redundancy_Method_3_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_3_ ua="na">No</Dual_Registration_3_>
<Auto_Register_When_Failover_3_ ua="na">No</Auto_Register_When_Failover_3_>
<TLS_Name_Validate_3_ ua="na">Yes</TLS_Name_Validate_3_>
 <!--  Subscriber Information  -->
<Display_Name_3_ ua="na"/>
<User_ID_3_ ua="na"/>
 <!--  <Password_3_ ua="na"/>  -->
<Auth_ID_3_ ua="na"/>
<Reversed_Auth_Realm_3_ ua="na"/>
<SIP_URI_3_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_3_ ua="na"/>
<XSI_Authentication_Type_3_ ua="na">Login Credentials</XSI_Authentication_Type_3_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_3_ ua="na"/>
 <!--  <Login_Password_3_ ua="na"/>  -->
<Anywhere_Enable_3_ ua="na">No</Anywhere_Enable_3_>
<Block_CID_Enable_3_ ua="na">No</Block_CID_Enable_3_>
<DND_Enable_3_ ua="na">No</DND_Enable_3_>
<CFWD_Enable_3_ ua="na">No</CFWD_Enable_3_>
 <!--  Audio Configuration  -->
<Preferred_Codec_3_ ua="na">G711u</Preferred_Codec_3_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_3_ ua="na">No</Use_Pref_Codec_Only_3_>
<Second_Preferred_Codec_3_ ua="na">Unspecified</Second_Preferred_Codec_3_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_3_ ua="na">Unspecified</Third_Preferred_Codec_3_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_3_ ua="na">Yes</G711u_Enable_3_>
<G711a_Enable_3_ ua="na">Yes</G711a_Enable_3_>
<G729a_Enable_3_ ua="na">Yes</G729a_Enable_3_>
<G722_Enable_3_ ua="na">Yes</G722_Enable_3_>
<G722.2_Enable_3_ ua="na">Yes</G722.2_Enable_3_>
<iLBC_Enable_3_ ua="na">Yes</iLBC_Enable_3_>
```

Beispiel-Konfigurationsprofile

```
<OPUS_Enable_3_ ua="na">Yes</OPUS_Enable_3_>
<Silence_Supp_Enable_3_ ua="na">No</Silence_Supp_Enable_3_>
<DTMF_Tx_Method_3_ ua="na">Auto</DTMF_Tx_Method_3_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_3_ ua="na">Default</Codec_Negotiation_3_>
<!--  available options: Default|List All  -->
<Encryption_Method_3_ ua="na">AES 128</Encryption_Method_3_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_3_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_3_>
<Caller_ID_Map_3_ ua="na"/>
<Enable_URI_Dialing_3_ ua="na">No</Enable_URI_Dialing_3_>
<Emergency_Number_3_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_3_ ua="na"/>
<Primary_Request_URL_3_ ua="na"/>
<Secondary_Request_URL_3_ ua="na"/>
 <!--  General  -->
<Line_Enable_4_ ua="na">Yes</Line_Enable_4_>
 <!--  Share Line Appearance  -->
<Share_Ext_4_ ua="na">No</Share_Ext_4_>
<Shared_User_ID_4_ ua="na"/>
<Subscription_Expires_4_ ua="na">3600</Subscription_Expires_4_>
<Restrict_MWI_4_ ua="na">No</Restrict_MWI_4_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_4_ ua="na">No</NAT_Mapping_Enable_4_>
<NAT_Keep_Alive_Enable_4_ ua="na">No</NAT_Keep_Alive_Enable_4_>
<NAT_Keep_Alive_Msg_4_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_4_>
<NAT_Keep_Alive_Dest_4_ ua="na">$PROXY</NAT_Keep_Alive_Dest_4_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_4_ ua="na">0x68</SIP_TOS_DiffServ_Value_4_>
<RTP_TOS_DiffServ_Value_4_ ua="na">0xb8</RTP_TOS_DiffServ_Value_4_>
 <!--  SIP Settings  -->
<SIP_Transport_4_ ua="na">UDP</SIP_Transport_4_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_4_ ua="na">5063</SIP_Port_4_>
<SIP_100REL_Enable_4_ ua="na">No</SIP_100REL_Enable_4_>
<EXT_SIP_Port_4_ ua="na">0</EXT_SIP_Port_4_>
<Auth_Resync-Reboot_4_ ua="na">Yes</Auth_Resync-Reboot_4_>
<SIP_Proxy-Require_4_ ua="na"/>
<SIP_Remote-Party-ID_4_ ua="na">No</SIP_Remote-Party-ID_4_>
<Referor_Bye_Delay_4_ ua="na">4</Referor_Bye_Delay_4_>
<Refer-To_Target_Contact_4_ ua="na">No</Refer-To_Target_Contact_4_>
<Referee_Bye_Delay_4_ ua="na">0</Referee_Bye_Delay_4_>
<Refer_Target_Bye_Delay_4_ ua="na">0</Refer_Target_Bye_Delay_4_>
<Sticky_183_4_ ua="na">No</Sticky_183_4_>
<Auth_INVITE_4_ ua="na">No</Auth_INVITE_4_>
<Ntfy_Refer_On_1xx-To-Inv_4_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_4_>
<Set_G729_annexb_4_ ua="na">yes</Set_G729_annexb_4_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_4_ ua="na"/>
<VQ_Report_Interval_4_ ua="na">0</VQ_Report_Interval_4_>
<User_Equal_Phone_4_ ua="na">No</User_Equal_Phone_4_>
<Call_Recording_Protocol_4_ ua="na">SIPREC</Call_Recording_Protocol_4_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_4_ ua="na">Disabled</Privacy_Header_4_>
<!--
```

```
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_4_ ua="na">No</P-Early-Media_Support_4_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_4_ ua="na">No</Blind_Attn-Xfer_Enable_4_>
<Message_Waiting_4_ ua="na">No</Message_Waiting_4_>
<Auth_Page_4_ ua="na">No</Auth_Page_4_>
<Default_Ring_4_ ua="rw">1</Default_Ring_4_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_4_ ua="na"/>
<Conference_Bridge_URL_4_ ua="na"/>
<Conference_Single_Hardkey_4_ ua="na">No</Conference_Single_Hardkey_4_>
 <!--  <Auth_Page_Password_4_ ua="na"/>  -->
<Mailbox_ID_4_ ua="na"/>
<Voice_Mail_Server_4_ ua="na"/>
<Voice_Mail_Subscribe_Interval_4_ ua="na">86400</Voice_Mail_Subscribe_Interval_4_>
<Auto_Ans_Page_On_Active_Call_4_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_4_>
<Feature_Key_Sync_4_ ua="na">No</Feature_Key_Sync_4_>
<Call_Park_Monitor_Enable_4_ ua="na">No</Call_Park_Monitor_Enable_4_>
<Enable_Broadsoft_Hoteling_4_ ua="na">No</Enable_Broadsoft_Hoteling_4_>
<Hoteling_Subscription_Expires_4_ ua="na">3600</Hoteling_Subscription_Expires_4_>
<Secure_Call_Option_4_ ua="na">Optional</Secure_Call_Option_4_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_4_ ua="na">No</Broadsoft_ACD_4_>
<Call_Information_Enable_4_ ua="na">No</Call_Information_Enable_4_>
<Disposition_Code_Enable_4_ ua="na">No</Disposition_Code_Enable_4_>
<Trace_Enable_4_ ua="na">No</Trace_Enable_4_>
<Emergency_Escalation_Enable_4_ ua="na">No</Emergency_Escalation_Enable_4_>
<Queue_Status_Notification_Enable_4_ ua="na">No</Queue_Status_Notification_Enable_4_>
 <!--  Proxy and Registration  -->
<Proxy_4_ ua="na">as1bsoft.sipurash.com</Proxy_4_>
<Outbound_Proxy_4_ ua="na"/>
<Alternate_Proxy_4_ ua="na"/>
<Alternate_Outbound_Proxy_4_ ua="na"/>
<Use_OB_Proxy_In_Dialog_4_ ua="na">Yes</Use_OB_Proxy_In_Dialog_4_>
<Register_4_ ua="na">Yes</Register_4_>
<Make_Call_Without_Reg_4_ ua="na">No</Make_Call_Without_Reg_4_>
<Register_Expires_4_ ua="na">3600</Register_Expires_4_>
<Ans_Call_Without_Reg_4_ ua="na">No</Ans_Call_Without_Reg_4_>
<Use_DNS_SRV_4_ ua="na">No</Use_DNS_SRV_4_>
<DNS_SRV_Auto_Prefix_4_ ua="na">Yes</DNS_SRV_Auto_Prefix_4_>
<Proxy_Fallback_Intvl_4_ ua="na">3600</Proxy_Fallback_Intvl_4_>
<Proxy_Redundancy_Method_4_ ua="na">Normal</Proxy_Redundancy_Method_4_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_4_ ua="na">No</Dual_Registration_4_>
<Auto_Register_When_Failover_4_ ua="na">No</Auto_Register_When_Failover_4_>
<TLS_Name_Validate_4_ ua="na">Yes</TLS_Name_Validate_4_>
 <!--  Subscriber Information  -->
<Display_Name_4_ ua="na"/>
<User_ID_4_ ua="na">4085263128</User_ID_4_>
 <!--  <Password_4_ ua="na">*************</Password_4_>  -->
<Auth_ID_4_ ua="na">AUN3128</Auth_ID_4_>
<Reversed_Auth_Realm_4_ ua="na"/>
<SIP_URI_4_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_4_ ua="na"/>
<XSI_Authentication_Type_4_ ua="na">Login Credentials</XSI_Authentication_Type_4_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_4_ ua="na"/>
```

Beispiel-Konfigurationsprofile

```
 <!--  <Login_Password_4_ ua="na"/>  -->
<Anywhere_Enable_4_ ua="na">No</Anywhere_Enable_4_>
<Block_CID_Enable_4_ ua="na">No</Block_CID_Enable_4_>
<DND_Enable_4_ ua="na">No</DND_Enable_4_>
<CFWD_Enable_4_ ua="na">No</CFWD_Enable_4_>
 <!--  Audio Configuration  -->
<Preferred_Codec_4_ ua="na">G711u</Preferred_Codec_4_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_4_ ua="na">No</Use_Pref_Codec_Only_4_>
<Second_Preferred_Codec_4_ ua="na">Unspecified</Second_Preferred_Codec_4_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_4_ ua="na">Unspecified</Third_Preferred_Codec_4_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_4_ ua="na">Yes</G711u_Enable_4_>
<G711a_Enable_4_ ua="na">Yes</G711a_Enable_4_>
<G729a_Enable_4_ ua="na">Yes</G729a_Enable_4_>
<G722_Enable_4_ ua="na">Yes</G722_Enable_4_>
<G722.2_Enable_4_ ua="na">Yes</G722.2_Enable_4_>
<iLBC_Enable_4_ ua="na">Yes</iLBC_Enable_4_>
<OPUS_Enable_4_ ua="na">Yes</OPUS_Enable_4_>
<Silence_Supp_Enable_4_ ua="na">No</Silence_Supp_Enable_4_>
<DTMF_Tx_Method_4_ ua="na">Auto</DTMF_Tx_Method_4_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_4_ ua="na">Default</Codec_Negotiation_4_>
<!--  available options: Default|List All  -->
<Encryption_Method_4_ ua="na">AES 128</Encryption_Method_4_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_4_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_4_>
<Caller_ID_Map_4_ ua="na"/>
<Enable_URI_Dialing_4_ ua="na">No</Enable_URI_Dialing_4_>
<Emergency_Number_4_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_4_ ua="na"/>
<Primary_Request_URL_4_ ua="na"/>
<Secondary_Request_URL_4_ ua="na"/>
 <!--  Hold Reminder  -->
<Hold_Reminder_Timer ua="rw"/>
<Hold_Reminder_Ring ua="rw">2</Hold_Reminder_Ring>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12
-->
 <!--  Call Forward  -->
<Cfwd_Setting ua="rw">Yes</Cfwd_Setting>
<Cfwd_All_Dest ua="rw"/>
<Cfwd_Busy_Dest ua="rw"/>
<Cfwd_No_Ans_Dest ua="rw"/>
<Cfwd_No_Ans_Delay ua="rw">20</Cfwd_No_Ans_Delay>
 <!--  Speed Dial  -->
<Speed_Dial_2_Name ua="rw"/>
<Speed_Dial_2_Number ua="rw"/>
<Speed_Dial_3_Name ua="rw"/>
<Speed_Dial_3_Number ua="rw"/>
```

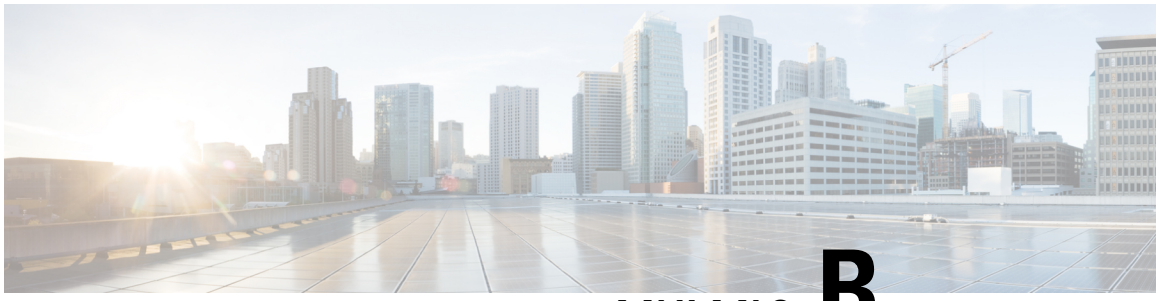
```
<Speed_Dial_4_Name ua="rw"/>
<Speed_Dial_4_Number ua="rw"/>
<Speed_Dial_5_Name ua="rw"/>
<Speed_Dial_5_Number ua="rw"/>
<Speed_Dial_6_Name ua="rw"/>
<Speed_Dial_6_Number ua="rw"/>
<Speed_Dial_7_Name ua="rw"/>
<Speed_Dial_7_Number ua="rw"/>
<Speed_Dial_8_Name ua="rw"/>
<Speed_Dial_8_Number ua="rw"/>
<Speed_Dial_9_Name ua="rw"/>
<Speed_Dial_9_Number ua="rw"/>
 <!--  Supplementary Services  -->
<CW_Setting ua="rw">Yes</CW_Setting>
<Block_CID_Setting ua="rw">No</Block_CID_Setting>
<Block_ANC_Setting ua="rw">No</Block_ANC_Setting>
<DND_Setting ua="rw">No</DND_Setting>
<Secure_Call_Setting ua="na">No</Secure_Call_Setting>
<Auto_Answer_Page ua="na">Yes</Auto_Answer_Page>
<Preferred_Audio_Device ua="na">None</Preferred_Audio_Device>
<!--  available options: Speaker|Headset|None  -->
<Time_Format ua="na">12hr</Time_Format>
<!--  available options: 12hr|24hr  -->
<Date_Format ua="na">month/day</Date_Format>
<!--  available options: month/day|day/month  -->
<Miss_Call_Shortcut ua="na">No</Miss_Call_Shortcut>
<Handset_LED_Alert ua="rw">Voicemail</Handset_LED_Alert>
<!--
 available options: Voicemail|Voicemail, Missed Call
-->
<Alert_Tone_Off ua="rw">No</Alert_Tone_Off>
<Log_Missed_Calls_for_EXT_1 ua="na">Yes</Log_Missed_Calls_for_EXT_1>
<Log_Missed_Calls_for_EXT_2 ua="na">Yes</Log_Missed_Calls_for_EXT_2>
<Log_Missed_Calls_for_EXT_3 ua="na">Yes</Log_Missed_Calls_for_EXT_3>
<Log_Missed_Calls_for_EXT_4 ua="na">Yes</Log_Missed_Calls_for_EXT_4>
<Shared_Line_DND_Cfwd_Enable ua="na">Yes</Shared_Line_DND_Cfwd_Enable>
 <!--  Camera Profile 1  -->
 <!--  Camera Profile 2  -->
 <!--  Camera Profile 3  -->
 <!--  Camera Profile 4  -->
 <!--  Audio Volume  -->
<Ringer_Volume ua="rw">5</Ringer_Volume>
<Speaker_Volume ua="rw">7</Speaker_Volume>
<Handset_Volume ua="rw">15</Handset_Volume>
<Headset_Volume ua="rw">10</Headset_Volume>
<Ehook_Enable ua="na">No</Ehook_Enable>
 <!--  Audio Compliance  -->
<Compliant_Standard ua="rw">TIA</Compliant_Standard>
<!--  available options: TIA|ETSI  -->
 <!--  Screen  -->
<Screen_Saver_Enable ua="rw">Yes</Screen_Saver_Enable>
<Screen_Saver_Type ua="rw">Clock</Screen_Saver_Type>
<!--  available options: Clock|Download Picture|Logo  -->
<Screen_Saver_Wait ua="rw">60</Screen_Saver_Wait>
<Screen_Saver_Refresh_Period ua="rw">10</Screen_Saver_Refresh_Period>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<!--  available options: Off|10s|20s|30s|Always On  -->
<LCD_Contrast ua="rw">9</LCD_Contrast>
<Boot_Display ua="na">Default</Boot_Display>
<!--
 available options: Default|Download Picture|Logo|Text
-->
<Text_Logo ua="na"/>
<Phone_Background ua="rw">Default</Phone_Background>
```

Beispiel-Konfigurationsprofile

```
<!--  available options: Default|Logo  -->
<Picture_Download_URL ua="rw"/>
<Logo_URL ua="rw"/>
 <!--  Video Configuration  -->
 <!--  General  -->
<Subscribe_Expires ua="na">1800</Subscribe_Expires>
<Subscribe_Retry_Interval ua="na">30</Subscribe_Retry_Interval>
<Number_of_Units ua="na">0</Number_of_Units>
<!--  available options: 0|1  -->
<Subscribe_Delay ua="na">1</Subscribe_Delay>
<Server_Type ua="na">Broadsoft</Server_Type>
<!--
 available options: Broadsoft|SPA9000|Asterisk|RFC3265_4235|Sylantro
-->
<BLF_List_URI ua="na"/>
<Use_Line_Keys_For_BLF_List ua="na">No</Use_Line_Keys_For_BLF_List>
<Customizable_PLK_Options ua="na">sd;</Customizable_PLK_Options>
<BLF_List ua="na">Show</BLF_List>
<!--  available options: Show|Hide  -->
<Call_Pickup_Audio_Notification ua="na">No</Call_Pickup_Audio_Notification>
<Attendant_Console_LCD_Contrast ua="na">8</Attendant_Console_LCD_Contrast>
<BXfer_To_Starcode_Enable ua="na">No</BXfer_To_Starcode_Enable>
<BXfer_On_Speed_Dial_Enable ua="na">No</BXfer_On_Speed_Dial_Enable>
<BXfer_To_Remote_Party_Number_Enable ua="na">No</BXfer_To_Remote_Party_Number_Enable>
<BLF_Label_Display_Mode ua="na">Both</BLF_Label_Display_Mode>
<!--  available options: Name|Ext|Both  -->
<Wake_up_phone_screen_when_BLF_pickup_is_ringing
ua="na">No</Wake_up_phone_screen_when_BLF_pickup_is_ringing>
 <!--  Unit 1  -->
<Unit_1_Key_1_ ua="na"/>
<Unit_1_Key_2_ ua="na"/>
<Unit_1_Key_3_ ua="na"/>
<Unit_1_Key_4_ ua="na"/>
<Unit_1_Key_5_ ua="na"/>
<Unit_1_Key_6_ ua="na"/>
<Unit_1_Key_7_ ua="na"/>
<Unit_1_Key_8_ ua="na"/>
<Unit_1_Key_9_ ua="na"/>
<Unit_1_Key_10_ ua="na"/>
<Unit_1_Key_11_ ua="na"/>
<Unit_1_Key_12_ ua="na"/>
<Unit_1_Key_13_ ua="na"/>
<Unit_1_Key_14_ ua="na"/>
<Unit_1_Key_15_ ua="na"/>
<Unit_1_Key_16_ ua="na"/>
<Unit_1_Key_17_ ua="na"/>
<Unit_1_Key_18_ ua="na"/>
<Unit_1_Key_19_ ua="na"/>
<Unit_1_Key_20_ ua="na"/>
<Unit_1_Key_21_ ua="na"/>
<Unit_1_Key_22_ ua="na"/>
<Unit_1_Key_23_ ua="na"/>
<Unit_1_Key_24_ ua="na"/>
<Unit_1_Key_25_ ua="na"/>
<Unit_1_Key_26_ ua="na"/>
<Unit_1_Key_27_ ua="na"/>
<Unit_1_Key_28_ ua="na"/>
 <!--  TR-069  -->
<Enable_TR-069 ua="na">No</Enable_TR-069>
<ACS_URL ua="na"/>
<ACS_Username ua="na"/>
 <!--  <ACS_Password ua="na"/>  -->
<Connection_Request_Username ua="na"/>
 <!--  <Connection_Request_Password ua="na"/>  -->
```

```
<Periodic_Inform_Interval ua="na">20</Periodic_Inform_Interval>
<Periodic_Inform_Enable ua="na">Yes</Periodic_Inform_Enable>
<TR-069_Traceability ua="na">No</TR-069_Traceability>
<CWMP_V1.2_Support ua="na">Yes</CWMP_V1.2_Support>
<TR-069_VoiceObject_Init ua="na">Yes</TR-069_VoiceObject_Init>
<TR-069_DHCPOption_Init ua="na">Yes</TR-069_DHCPOption_Init>
<TR-069_Fallback_Support ua="na">No</TR-069_Fallback_Support>
<BACKUP_ACS_URL ua="na"/>
<BACKUP_ACS_User ua="na"/>
 <!--  <BACKUP_ACS_Password ua="na"/>  -->
</flat-profile>
```

Beispiel-Konfigurationsprofile



ANHANG B

Abkürzungen

Abkürzungen

AC	Wechselstrom
ACS	Access Control Server
A/D	Analog-Digital-Wandler
AES	Advanced Encryption Standard
ANC	Anonymer Anruf
AP	Access Point
ASCII	American Standard Code for Information Interchange
B2BUA	Back-to-Back User Agent
BLF	Besetztlampenfeld
Bool	Boolesche Werte. Im Profil als „Ja“ und „Nein“ bzw. 1 und 0 angegeben.
BootP	Bootstrap-Protokoll
CA	Zertifizierungsstelle
CAS	CPE-Warnsignal
CDP	Cisco Discovery Protocol
CDR	Verbindungsdatensatz (Call Detail Record)
CGI	Computer-generierte Mmagery
CID	Anrufer-ID
CIDCW	Anrufer-ID wartender Anruf (Call Waiting Caller ID)

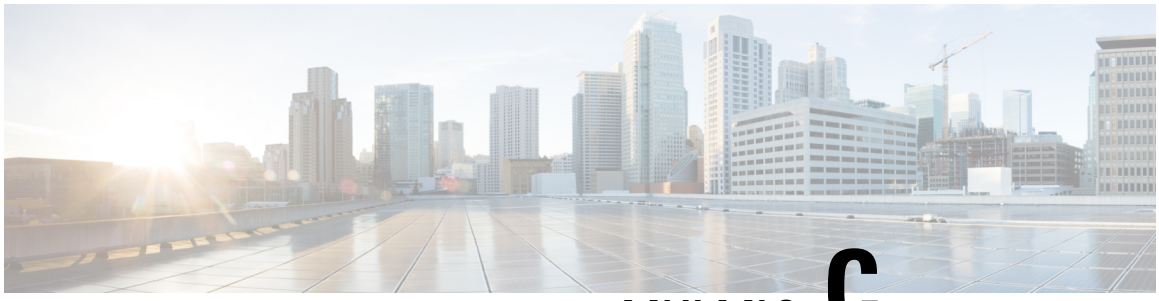
CNG	Komfortrauschen (Comfort Noise Generation)
CPC	Steuerung der anrufenden Partei (Calling Party Control)
CPE	Customer Premises Equipment
CSV	Comma-Separated Value (Kommagetrennter Wert)
CWCID	Anrufer-ID wartender Anruf (Call Waiting Caller ID)
CWT	Call Waiting Tone (Ton für wartenden Anruf)
D/A	Digital-Analog-Wandler
dB	Dezibel
dBm	dB in Bezug auf 1 Milliwatt
DHCP	Dynamic Host Configuration Protocol (DHCP)
DND	Bitte nicht stören
DNS	Domain Name System (DNS)
DoS	Denial of Service
DRAM	Dynamischer Arbeitsspeicher (Dynamic Random Access Memory)
DSL	Digital Subscriber Loop
DSP	Digital Signal Processor
DST	Sommerzeit
DTAS	Datenterminal-Alarmsignal (wie CAS)
DTMF	Mehrfrequenzwahlverfahren (Dual Tone Multiple Frequency)
FQDN	Vollständiger Domänenname
FSK	Frequenzumtastung (Frequency Shift Keying)
FW	Firmware
FXS	Foreign eXchange Station
GMT	Greenwich Mean Time
GW	Gateway
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP über SSL
ICMP	Internet Control Message Protocol

IGMP (IGMP)	Internet Group Management Protocol (Protokoll zur Verwaltung von Internetgruppen)
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	Internetprotokoll Version 4
IPv6	Internetprotokoll Version 6
ISP	Internetdienstanbieter
ITSP	Internettelefonie-Serviceanbieter (Internet Telephony Service Provider)
ITU	International Telecommunication Union
IVR	Interactive Voice Response (Interaktive Sprachantwort)
LAN	Local Area Network
LBR	Niedrige Bitrate (Low Bit Rate)
LBRC	Codec niedrige Bitrate (Low Bit Rate Codec)
LCD	Liquid Crystal Display; auch als Bildschirm bekannt
LDAP	Lightweight Directory Access Protocol
LED	Light-Emiting Diode
MAC-Adresse	Media Access Control Address
MC	Mini-Zertifikat (Mini-Certificate)
MGCP	Media Gateway Control Protocol
MOH	Warteschleifenmusik (Music On Hold)
MOS	Mean Opinion Score (1-5, je höher, desto besser)
MPP	Multiplattform-Telefone
ms	Millisekunde
MSA	Musikquellenadapter (Music Source Adaptor)
MWI	Hinweis auf wartende Nachricht
NAT	Network Address Translation
NPS	Normaler Bereitstellungsserver
NTP	Network Time Protocol
OOB	Out-of-Band

OSI	Open Switching Interval
PBX	Private Branch Exchange
PCB	Leiterplatte (Printed Circuit Board)
PoE	Power over Ethernet
PR	Polaritätsumkehr
PS	Bereitstellungsserver (Provisioning Server)
PSQM	Perceptual Speech Quality Measurement (1-5, je niedriger, desto besser)
PSTN	Öffentliches Telefonnetz
QoS	Quality-of-Service
RC	Remove Customization
REQT	(SIP-)Anforderungsnachricht
RESP	(SIP-)Antwortnachricht
RSC	(SIP-)Antwort-Statuscode, z. B. 404, 302, 600
RTP	Real Time Protocol
RTT	Round Trip Time
SAS	Streaming-Audioserver
SDP	Session Description Protocol
SDRAM	Synchronous Dynamic Random Access Memory
Sek.	Sekunden
SIP	Session Initiation Protocol
SLA	Gemeinsame Leitungsdarstellung (Shared Line Appearance)
SLIC	Subscriber Line Interface Circuit
SP-	Service-Provider
SSL	Secure Socket Layer
STUN	Session Traversal UDP for NAT
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTL	Gültigkeitsdauer

ToS	Type of Service
UA	Benutzer-Agent
uC	Mikro-Controller
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VAR	Value Added Reseller
VLAN	Voice LAN
VM	Voicemail
VMWI	Visuelle(r) Nachrichtenanzeige/-indikator
VoIP	Voice over Internet Protocol
VQ	Sprachqualität
WAN	Wide Area Network
XML	Extensible Markup Language

Abkürzungen



ANHANG C

Zugehöriges Dokumentationsmaterial

Zugehöriges Dokumentationsmaterial

In den folgenden Abschnitten finden Sie zugehörige Informationen.

Dokumentation für die Cisco IP Phone 6800-Serie

Lesen Sie die Publikationen für Ihre Sprache, Ihr Telefonmodell und Ihre Multiplattform-Firmware-Version. Navigieren Sie über den folgenden Uniform Resource Locator (URL):

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/tsd-products-support-series-home.html

Cisco IP Phone-Firmware – Supportrichtlinie

Informationen zur Supportrichtlinie für Telefone finden Sie unter https://cisco.com/go/phonefirmwaresupport.