



## Bereitstellungsmethoden

---

- [Telefon mit dem BroadSoft-Server bereitstellen](#) , auf Seite 1
- [Bereitstellungsbeispiele – Übersicht](#), on page 2
- [Grundlagen der Resynchronisierung](#), on page 2
- [TFTP-Resynchronisierung](#), on page 3
- [Eindeutige Profile, Makroerweiterung und HTTP](#), on page 7
- [Ein Gerät automatisch resynchronisieren](#), on page 10
- [Ihre Telefone für die Onboard-Aktivierung des Aktivierungscodes einrichten](#), auf Seite 19
- [Direktes Migrieren des Telefons zu einem Unternehmenstelefon](#), auf Seite 21
- [Sichere HTTPS-Resynchronisierung](#), on page 22
- [Profilverwaltung](#), on page 30
- [Privatfunktion-Header für Telefon einrichten](#), auf Seite 33
- [Verlängern des MIC-Zertifikats](#), auf Seite 34

## Telefon mit dem BroadSoft-Server bereitstellen

Nur Benutzer von BroadSoft-Servern.

Sie können Ihre Cisco IP Multiplattform-Telefone auf einer BroadWorks-Plattform registrieren.

### Prozedur

---

- Schritt 1** Laden Sie das CPE-Kit von BroadSoft Xchange herunter. Um die neuesten CPE-Kits zu erhalten, gehen Sie zu dieser URL: <https://xchange.broadsoft.com>.
- Schritt 2** Laden Sie die aktuellste DTAF-Datei auf den BroadWorks-Server (Systemebene) hoch.  
Weitere Informationen finden Sie unter folgender URL: (<https://xchange.broadsoft.com/node/1031047>). Rufen Sie das *BroadSoft-Partner-Konfigurationshandbuch* auf und lesen Sie Abschnitt „*Konfiguration des BroadWorks-Geräteprofiltyps*“.
- Schritt 3** BroadWorks-Geräteprofiltyp konfigurieren.  
Weitere Informationen zum Konfigurieren des Geräteprofiltyps finden Sie unter folgender URL:

<https://xchange.broadsoft.com/node/1031047>. Rufen Sie das *BroadSoft-Partner-Konfigurationshandbuch* auf und lesen Sie Abschnitt „*Konfiguration des BroadWorks-Geräteprofiltyps*“.

---

## 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](#).

## Grundlagen der Resynchronisierung

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

### Syslog zum Protokollieren von Nachrichten verwenden

Ein Telefon kann so konfiguriert werden, dass Protokollnachrichten an einen Syslog-Server über UDP, einschließlich Nachrichten in Bezug auf die Bereitstellung, gesendet werden. Um diesen Server zu identifizieren, können Sie auf die Weboberfläche des Telefons zugreifen (siehe [Auf Weboberfläche des Telefons zugreifen](#)), wählen Sie **Sprache > System** aus und bestimmen Sie den Parameter **Syslog-Server** im Abschnitt **Optionale Netzwerkkonfiguration**. Konfigurieren Sie die IP-Adresse des Syslog-Servers im Gerät, und beachten Sie die Meldungen, die während der restlichen Verfahren generiert werden.

Um die Informationen abzurufen, können Sie auf die Weboberfläche des Telefons zugreifen, wählen Sie **Info > Debug-Info > Steuerprotokolle** und klicken Sie auf **Nachrichten**.

#### Before you begin

#### Procedure

---

- 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, on page 3](#) 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-88xx-3PCC 00:0e:08:ab:cd:ef -- Successful resync tftp://192.168.1.200/basic.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.

---

## 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](#). Im folgenden Verfahren wird ein Profil nach dem Herunterladen einer Datei von einem TFTP-Server geändert.

### Procedure

---

**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.

## Nachrichten an den Syslog-Server senden

Wenn ein Syslog-Server auf dem Telefon unter Verwendung der Parameter konfiguriert wird, werden bei den Resynchronisierungs- und Upgrade-Vorgängen 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.

Sie können die Parameter auch in der Konfigurationsdatei des Telefons mit XML-Code (`cfg.xml`) konfigurieren. Zur Konfiguration der einzelnen Parameter siehe Syntax der Zeichenfolge in [Systemprotokoll-Parameter, auf Seite 5](#).

### Vorbereitungen

- Ein Syslog-Server ist installiert und konfiguriert.
- Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe [Auf Weboberfläche des Telefons zugreifen](#).

### Prozedur

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

**Schritt 2** Geben Sie im Abschnitt **Optionale Netzwerkkonfiguration** die Server-IP in **Syslog-Server** ein und geben Sie optional eine **Syslog-ID** an, wie in [Systemprotokoll-Parameter, auf Seite 5](#) beschrieben.

**Schritt 3** Optional können Sie den Inhalt der Syslog-Nachrichten mithilfe von **Protokoll-Anforderungsnachricht**, **Protokoll-Erfolgsnachricht** und **Protokoll-Fehlschlagsnachricht** wie in [Systemprotokoll-Parameter, auf Seite 5](#) beschrieben definieren.

Die Felder, die den Inhalt der Syslog-Nachricht definieren, befinden sich im Abschnitt **Konfigurationsprofil** auf der Registerkarte **Sprache > Bereitstellung**. Wenn Sie den Nachrichteninhalte nicht angeben, werden die Standardeinstellungen in den Feldern verwendet. Wenn für eines dieser Felder kein Wert angegeben ist, wird keine entsprechende Syslog-Nachricht generiert.

**Schritt 4** Klicken Sie auf **Alle Änderungen annehmen**, um die Konfiguration anzuwenden.

**Schritt 5** Überprüfen Sie die Gültigkeit der Konfiguration.

a) Führen Sie eine TFTP-Neusynchronisierung durch. Siehe [TFTP-Resynchronisierung, auf Seite 3](#).

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.

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

```
CP-78xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txt
CP-88xx-3PCC 00:0e:08:ab:cd:ef -- Successful resync tftp://192.168.1.200/basic.txt
```

## Systemprotokoll-Parameter

In der folgenden Tabelle werden die Funktionen und die Verwendung der syslog-Parameter im Abschnitt **Optionale Netzwerkkonfiguration** in der Registerkarte **Sprache > system** in der Telefon-Webseite definiert. Außerdem wird die Syntax der Zeichenfolge definiert, die in der Telefon-Konfigurationsdatei mit dem XML-Code (cfg.xml) hinzugefügt wird, um einen Parameter zu konfigurieren.

**Tabelle 1: Syslog-Parameter**

Parametername	Beschreibung und Standardwert
Syslog-Server	<p>Geben Sie den Server an, um die Telefonsysteminformationen und kritische Ereignisse zu protokollieren. Wenn der Debug-Server und Syslog-Server angegeben sind, werden Syslog-Meldung auch auf dem Debug-Server protokolliert.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Syslog_Server ua="na"&gt;10.74.30.84&lt;/Syslog_Server&gt;</pre> </li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> den Syslog-Server an.</li> </ul>

Parametername	Beschreibung und Standardwert
Syslog-Bezeichner	<p>Wählen Sie die Geräte-ID aus, die in den Syslog-Nachrichten einbezogen werden soll, die auf den Syslog-Server hochgeladen werden. Die Geräte-ID wird nach dem Zeitstempel in jeder Nachricht angezeigt. Die Optionen für die Bezeichner sind:</p> <ul style="list-style-type: none"> <li>• Keine: Keine Geräte-ID.</li> <li>• \$MA: Die MAC-Adresse des Telefons, dargestellt als kontinuierliche Kleinbuchstaben und Ziffern. Beispiel: c4b9cd811e29</li> <li>• \$MAU: Die MAC-Adresse des Telefons, dargestellt als kontinuierliche Großbuchstaben und Ziffern. Beispiel: C4B9CD811E29</li> <li>• \$MAC: Die MAC-Adresse des Telefons im durch Doppelpunkte getrennten Standardformat. Beispiel: c4:b9:cd:81:1e:29</li> <li>• \$SN: Die Produktseriennummer des Telefons.</li> </ul> <p>• <b>Geben Sie in der XML-Konfigurationsdatei des Telefons (cfg.xml) eine Zeichenfolge in folgendem Format ein:</b></p> <pre>&lt;Syslog_Identifier ua="na"&gt;\$MAC&lt;/Syslog_Identifier&gt;</pre> <p>• <b>Wählen Sie auf der Telefon-Webseite einen Bezeichner aus der Liste aus.</b></p> <p>Standard: Keine</p>
Log Request Msg (Protokollmeldung über Anfragen)	<p>Die Nachricht, die zum Syslog-Server am Beginn eines Neusynchronisationsversuchs gesendet wird. Wenn kein Wert angegeben ist, wird die Syslog-Meldung nicht generiert.</p> <p>Der Standardwert ist <code>\$PN \$MAC -- Requesting resync</code>  <code>\$SCHEME://\$SERVIP:\$PORT\$PATH</code></p> <p>• <b>Geben Sie in der XML-Konfigurationsdatei des Telefons (cfg.xml) eine Zeichenfolge in folgendem Format ein:</b></p> <pre>&lt;Log_Request_Msg ua="na"&gt;\$PN \$MAC -- Requesting resync \$SCHEME://\$SERVIP:\$PORT\$PATH&lt;/Log_Request_Msg&gt;</pre>
Protokollmeldung über erfolgreiche Synchronisierung	<p>Die syslog-Meldung, die nach dem erfolgreichen Abschluss eines Resynchronisierungsversuchs ausgegeben wird. Wenn kein Wert angegeben ist, wird die Syslog-Meldung nicht generiert.</p> <p><b>Geben Sie in der Telefonkonfigurationsdatei mit XML (cfg.xml) eine Zeichenfolge im folgendem Format ein:</b> <code>&lt;Log_Success_Msg ua="na"&gt;\$PN \$MAC -- Successful resync \$SCHEME://\$SERVIP:\$PORT\$PATH&lt;/Log_Success_Msg&gt;</code></p>
Protokollmeldung über fehlgeschlagene Synchronisierung	<p>Die Syslog-Meldung, die nach dem Fehlschlagen eines Resynchronisierungsversuchs ausgegeben wird. Wenn kein Wert angegeben ist, wird die Syslog-Meldung nicht generiert.</p> <p>Der Standardwert ist <code>\$PN \$MAC -- Resync failed: \$ERR.</code></p> <p><b>Geben Sie in der Telefonkonfigurationsdatei mit XML (cfg.xml) eine Zeichenfolge im folgendem Format ein:</b> <code>&lt;Log_Failure_Msg ua="na"&gt;\$PN \$MAC -- Resync failed: \$ERR&lt;/Log_Failure_Msg&gt;</code></p>

# 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 Profilenameskonvention 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, on page 3](#). 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](#).

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

## Bereitstellung eines bestimmten IP-Telefonprofils auf einem TFTP-Server

### Procedure

- 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, on page 3](#) 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 [Auf Weboberfläche des Telefons zugreifen](#).
- Schritt 5** Wählen Sie **Sprache** > **Bereitstellung** aus.
- Schritt 6** Geben Sie `tftp://192.168.1.200/CP-8841-3PCC$MA.cfg` in das Feld **Profilregel** ein.

```
<Profile_Rule>  
  tftp://192.168.1.200/CP-8841-3PCC$MA.cfg  
</Profile_Rule>
```

- Schritt 7** Klicken Sie auf **Submit All Changes**. 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.

## Erneute Synchronisierung mit HTTP 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 3](#) 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 **Submit All Changes**. 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
```

# 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.

## Before you begin

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe [Auf Weboberfläche des Telefons zugreifen](#).

## Procedure

- 
- 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, on page 2](#) 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.
-

## Profil Resync-Parameter

Die folgende Tabelle definiert die Funktion und die Verwendung der Profil Resync-Parameter im Abschnitt **Konfigurationsprofil** auf der Registerkarte **Sprache > Bereitstellung** auf der Telefon-Webseite. Außerdem wird die Syntax der Zeichenfolge definiert, die in der Telefon-Konfigurationsdatei mit dem XML-Code (cfg.xml) hinzugefügt wird, um einen Parameter zu konfigurieren.

Parameter	Beschreibung
Provision Enable (Bereitstellung aktivieren)	<p>Erlaubt oder verbietet Neusynchronisationsaktionen des Konfigurationsprofils.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein:   <pre>&lt;Provision_Enable ua="na"&gt;Ja&lt;/Provision_Enable&gt;</pre> </li> <li>• <b>Legen Sie dieses Feld auf</b> der Telefon-Webseite auf <b>Ja</b> fest, um erneute Synchronisationsaktionen zuzulassen, oder <b>Nein</b>, um die Aktionen für die erneute Synchronisierung zu blockieren.</li> </ul> <p>Standard: Ja</p>
Resync On Reset (Resynchronisierung nach Neustart)	<p>Gibt an, ob das Telefon Konfigurationen mit dem Bereitstellungsserver nach dem Einschalten und nach jedem Upgrade-Versuch neu synchronisiert.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein:   <pre>&lt;Resync_On_Reset ua="na"&gt;Ja&lt;/Resync_On_Reset&gt;</pre> </li> <li>• <b>Legen Sie in diesem Feld</b> auf der Telefon-Webseite <b>Ja</b> fest, um die erneute Synchronisierung beim Einschalten oder beim Zurücksetzen zu ermöglichen, oder <b>Nein</b>, um die erneute Synchronisierung beim Einschalten oder Zurücksetzen zu blockieren.</li> </ul> <p>Standard: Ja</p>

Parameter	Beschreibung
Resync Random Delay (Zufällige Resynchronisierungszögerung)	<p>Verhindert eine Überlastung des Bereitstellungsservers, wenn eine große Anzahl an Geräten gleichzeitig eingeschaltet werden und eine Erstkonfiguration versuchen. Die Verzögerung gilt nur für den ersten Konfigurationsversuch nach dem Einschalten oder Zurücksetzen des Geräts.</p> <p>Der Parameter ist das maximal zulässige Zeitintervall, bis zum ersten Kontakt des Geräts mit dem Bereitstellungsserver. Bei der tatsächlichen Wartezeit handelt es sich um eine Pseudozufallszahl zwischen 0 und diesem Wert.</p> <p>Dieser Parameter wird in Einheiten von 20 Sekunden angegeben.</p> <p>Der gültige Wert liegt zwischen 0 und 65535.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Resync_Random_Delay ua="na"&gt;2&lt;/Resync_Random_Delay&gt;</pre> </li> <li>• <b>Geben Sie auf der Webseite des Telefons</b> die Anzahl der Einheiten (20 Sekunden) an, die das Telefon die Neusynchronisierung nach dem Einschalten oder Zurücksetzen verzögern soll.</li> </ul> <p>Der Standardwert ist 2 (40 Sekunden).</p>
Erneute Synchronisierung um (HHmm)	<p>Die Zeit (HHmm), in der sich das Telefon mit dem Bereitstellungsserver erneut synchronisiert.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Resync_At__HHmm_ ua="na"&gt;0959&lt;/Resync_At__HHmm_&gt;</pre> </li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> die Zeit im Format HHMM an, zu der das Telefon die Resynchronisierung startet.</li> </ul> <p>Der Standardwert ist leer. Wenn der Wert ungültig ist, wird der Parameter ignoriert. Falls dieser Parameter auf einen gültigen Wert festgelegt ist, wird der Parameter <b>Periodische Neusynchronisierung</b> ignoriert.</p>


Parameter	Beschreibung
Resync At Random Delay (Zufällige Verzögerung für die erneute Synchronisierung)	<p>Verhindert eine Überlastung des Bereitstellungsservers, wenn eine große Anzahl an Geräten gleichzeitig eingeschaltet wird.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre data-bbox="672 726 1435 751">&lt;Resync_At_Random_Delay ua="na"&gt;600&lt;/Resync_At_Random_Delay&gt;</pre> </li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> den Zeitraum in Sekunden an.</li> </ul> <p>Der gültige Wert liegt zwischen 600 und 65535.</p> <p>Wenn der Wert kleiner als 600 ist, liegt das Intervall der zufälligen Verzögerung zwischen 0 und 600.</p> <p>Der Standardwert ist 600 Sekunden (10 Minuten).</p>

Parameter	Beschreibung
Resync Periodic (Periodische Resynchronisierung)	<p>Das Zeit-Intervall zwischen periodischer Resynchronisierung mit dem Bereitstellungsserver. Der zugehörige Timer für die Resynchronisierung wird erst nach der ersten erfolgreichen Synchronisierung mit dem Server aktiviert.</p> <p>Dies sind die gültigen Formate:</p> <ul style="list-style-type: none"> <li>• Eine Ganzzahl Beispiel: Die Eingabe von <b>3000</b> gibt an, dass die nächste erneute Synchronisierung in 3000 Sekunden stattfindet.</li> <li>• Mehrere Ganzzahlen Beispiel: Die Eingabe von <b>600 , 1200 , 300</b> 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.</li> <li>• Zeitraum Beispiel: Die Eingabe von <b>2400 + 30</b> gibt an, dass die nächste erneute Synchronisierung zwischen 2400 und 2430 Sekunden nach einer erfolgreichen erneuten Synchronisierung erfolgt.</li> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein:   <pre>&lt;Resync_Periodic ua="na"&gt;3600&lt;/Resync_Periodic&gt;</pre> </li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> den Zeitraum in Sekunden an.</li> </ul> <p>Setzen Sie diesen Parameter auf 0, um die regelmäßige Resynchronisierung zu deaktivieren.</p> <p>Der Standardwert ist 3600 Sekunden.</p>

Parameter	Beschreibung
Resync Error Retry Delay (Wiederholungsverzögerung bei fehlgeschlagener Resynchronisierung)	<p>Falls ein Neusynchronisierungsvorgang fehlschlägt, da das Telefon nicht in der Lage war, ein Profil vom Server abzurufen, oder da die heruntergeladene Datei fehlerhaft ist, oder da ein interner Fehler aufgetreten ist, versucht das Telefon, nach einer festgelegten Zeit in Sekunden erneut zu synchronisieren.</p> <p>Dies sind die gültigen Formate:</p> <ul style="list-style-type: none"> <li>• Eine Ganzzahl              Beispiel: Die Eingabe von <b>300</b> gibt an, dass die nächste Wiederholung für die erneute Synchronisierung in 300 Sekunden auftritt.</li> <li>• Mehrere Ganzzahlen              Beispiel: Die Eingabe von <b>600 , 1200 , 300</b> 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.</li> <li>• Zeitraum              Beispiel: Die Eingabe von <b>2400 + 30</b> gibt an, dass die nächste Wiederholung zwischen 2400 und 2430 Sekunden nach einer fehlerhaften erneuten Synchronisierung stattfindet.</li> </ul> <p>Wenn die Verzögerung auf 0 festgelegt ist, führt das Gerät keine erneute Synchronisierung aus, nachdem eine erneute Synchronisierung fehlgeschlagen ist.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein:  <pre>&lt;Resync_Error_Retry_Delay ua="na"&gt;60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400&lt;/Resync_Error_Retry_Delay&gt;</pre></li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> den Zeitraum in Sekunden an.</li> </ul> <p>Standard: 60, 120, 240, 480, 960, 1920, 3840, 7680, 15360, 30720, 61440, 86400</p>

Parameter	Beschreibung
Forced Resync Delay (Erzwungene Resynchronisierungsverzögerung)	<p>Höchstwert für die Verzögerung (in Sekunden), bis das Telefon eine Resynchronisierung durchführt.</p> <p>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.</p> <p>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.</p> <p>Der gültige Wert liegt zwischen 0 und 65535.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Forced_Resync_Delay ua="na"&gt;14400&lt;/Forced_Resync_Delay&gt;</pre> </li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> den Zeitraum in Sekunden an.</li> </ul> <p>Der Standardwert ist 14.400 Sekunden.</p>
Resync From SIP (Resynchronisierung über SIP)	<p>Steuerungsanforderungen für Neusynchronisierungsvorgänge über ein SIP NOTIFY-Ereignis, das vom Proxyserver des Serviceanbieters an das Telefon gesendet wird. Wenn aktiviert, kann der Proxy eine erneute Synchronisierung anfordern, indem er eine SIP NOTIFY-Meldung an das Gerät sendet, die das Ereignis enthält.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Resync_From_SIP ua="na"&gt;Ja&lt;/Resync_From_SIP&gt;</pre> </li> <li>• <b>Wählen Sie auf der Telefon-Webseite Ja</b> aus, um diese Funktion zu aktivieren, oder <b>Nein</b>, um Sie zu deaktivieren.</li> </ul> <p>Standard: Ja</p>
Resync After Upgrade Attempt (Resynchronisierung nach versuchtem Upgrade)	<p>Aktiviert oder deaktiviert den Resynchronisierungsvorgang nach einem Upgrade. Falls <b>Ja</b> ausgewählt wird, wird Sync nach einem Firmware-Upgrade ausgelöst.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Resync_After_Upgrade_Attempt ua="na"&gt;Ja&lt;/Resync_After_Upgrade_Attempt&gt;</pre> </li> <li>• <b>Wählen Sie auf der Telefon-Webseite Ja</b> aus, um die erneute Synchronisierung nach einem Firmware-Upgrade zu starten, oder <b>Nein</b>, um nicht erneut zu synchronisieren.</li> </ul> <p>Standard: Ja</p>



Parameter	Beschreibung
Resync Trigger 1 (Resynchronisierungs-Tigger1)  Resync Trigger 2 (Resynchronisierungs-Tigger2)	<p>Falls eine Evaluierung der logischen Gleichung in diesen Parametern FALSE ergibt, wird keine Resynchronisierung ausgelöst, selbst wenn <b>Erneute Synchronisierung nach Neustart</b> auf <b>TRUE</b> festgelegt ist. Nur der Resync über eine direkte Aktion durch URL- und SIP-Benachrichtigung ignoriert diese Resync-Trigger.</p> <p>Die Parameter können mit einem bedingten Ausdruck programmiert werden, der einer Makroerweiterung unterliegt. Die gültigen Makroerweiterungen finden Sie unter <a href="#">Makroerweiterungsvariablen</a>.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Resync_Trigger_1 ua="na"&gt;\$UPGTMR gt 300 und \$PRVTMR ge 600&lt;/Resync_Trigger_1&gt; &lt;Resync_Trigger_2 ua="na"/&gt;</pre> </li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> die Trigger an.</li> </ul> <p>Standard: leer</p>
User Configurable Resync (Vom Benutzer konfigurierbare erneute Synchronisierung)	<p>Ermöglicht einem Benutzer, das Telefon aus dem Telefonbildschirmmenü erneut zu synchronisieren. Wenn diese Option auf <b>Ja</b> gesetzt ist, kann ein Benutzer die Telefonkonfiguration erneut synchronisieren, indem er die Profil-Regel auf dem Telefon eingibt. Wenn <b>Nein</b> festgelegt ist, wird der Parameter <b>Profil-Regel</b> nicht im Telefonbildschirm-Menü angezeigt. Der Parameter <b>Profil-Regel</b> befindet sich in <b>Verwaltung</b>  <b>&gt; Geräteanwendung</b>.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;User_Configurable_Resync ua="na"&gt;Ja&lt;/User_Configurable_Resync&gt;</pre> </li> <li>• <b>Wählen Sie auf der Telefon-Webseite</b> <b>Ja</b> aus, um den Parameter <b>Profil-Regel</b> im Telefonmenü anzuzeigen, oder wählen Sie <b>Nein</b> aus, um diesen Parameter auszublenden.</li> </ul> <p>Standard: Ja</p>
Resync Fails On FNF (Fehlgeschlagene Resynchronisierung aufgrund von FNF)	<p>Eine Resynchronisierung wird normalerweise als fehlgeschlagen betrachtet, wenn ein angefordertes Profil vom Server nicht empfangen wird. Dieser Parameter überschreibt dieses Verhalten. Wenn <b>Nein</b> festgelegt ist, akzeptiert das Gerät die Antwort <code>Datei-nicht-gefunden</code> vom Server als eine erfolgreiche Neusynchronisierung.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein: <pre>&lt;Resync_Fails_On_FNF ua="na"&gt;Ja&lt;/Resync_Fails_On_FNF&gt;</pre> </li> <li>• <b>Wählen Sie auf der Telefon-Webseite</b> <b>Ja</b> aus, um eine Antwort <code>Datei-nicht-gefunden</code> als nicht erfolgreiche Neusynchronisierung zu übernehmen, oder wählen Sie <b>Nein</b> aus, um eine Antwort <code>Datei-nicht-gefunden</code> als erfolgreiche Neusynchronisierung zu übernehmen.</li> </ul> <p>Standard: Ja</p>

Parameter	Beschreibung
Profil-Authentifizierungstyp	<p>Gibt die Anmeldeinformationen für die Authentifizierung des Profilkontos an. Folgende Optionen stehen hierbei zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> Deaktiviert die Profilkonto-Funktion. Wenn diese Funktion deaktiviert ist, wird das Menü <b>Profilkonto-Setup</b> nicht auf dem Telefonbildschirm angezeigt.</li> <li>• <b>HTTP-Basisauthentifizierung:</b> Die HTTP-Anmeldeinformationen werden zur Authentifizierung des Profilkontos verwendet.</li> <li>• <b>XSI-Authentifizierung:</b> Die XSI-Anmelde- oder XSI-SIP-Anmeldeinformationen werden verwendet, um das Profilkonto zu authentifizieren. Die Anmeldeinformationen für die Authentifizierung hängen vom <b>Authentifizierungstyp</b> für das Telefon ab:             <ul style="list-style-type: none"> <li>• Wenn der <b>XSI-Authentifizierungstyp</b> für das Telefon auf <b>Anmeldeinformationen</b> festgelegt ist, werden die XSI-Anmeldeinformationen verwendet.</li> <li>• Wenn der <b>XSI-Authentifizierungstyp</b> für das Telefon auf <b>SIP-Anmeldeinformationen</b> festgelegt ist, werden die XSI-SIP-Anmeldeinformationen verwendet.</li> </ul> </li> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein:             <pre data-bbox="630 1056 1295 1115" style="margin-left: 20px;">                     &lt;Profile_Authentication_Type ua="na"&gt;Grundlegende                     HTTP-Authentifizierung&lt;/Profile_Authentication_Type&gt;                 </pre> </li> <li>• <b>Wählen Sie auf der Telefon-Webseite</b> eine Option aus der Liste aus, für die das Telefon die Profil-Neusynchronisierung authentifizieren soll.</li> </ul> <p>Standard: Grundlegende HTTP-Authentifizierung</p>

Parameter	Beschreibung
Profilregel Profile Rule B (Profilregel B) Profile Rule C (Profilregel C) Profile Rule D (Profilregel D)	<p>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.</p> <p>Wenn Sie die AES-256-CBC-Verschlüsselung auf die Konfigurationsdateien anwenden, geben Sie den Verschlüsselungscode mit dem Schlüsselwort <b>--key</b> wie folgt an:</p> <p><b>[--key &lt;encryption key&gt;]</b></p> <p>Sie können den Verschlüsselungscode optional in Anführungszeichen (") einschließen.</p> <ul style="list-style-type: none"> <li>• <b>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML</b> eine Zeichenfolge im folgenden Format ein:           <pre>&lt;Profile_Rule ua="na"&gt;/\$PSN.xml&lt;/Profile_Rule&gt; &lt;Profile_Rule_B ua="na"/&gt; &lt;Profile_Rule_C ua="na"/&gt; &lt;Profile_Rule_D ua="na"/&gt;</pre> </li> <li>• <b>Geben Sie auf der Telefon-Webseite</b> die Profil-Regel an.</li> </ul> <p>Standard: <b>/\$PSN.xml</b></p>
DHCP Option To Use (Zu verwendende DHCP-Option)	<p>Durch Kommas getrennte DHCP-Optionen, die zum Abrufen der Firmware und Profile verwendet werden.</p> <p>Standard: 66,160,159,150,60,43,125</p>
Zu verwendende DHCPv6-Option	<p>Durch Kommas getrennte DHCP-Optionen, die zum Abrufen der Firmware und Profile verwendet werden.</p> <p>Standard: 17.160.159</p>

## Ihre Telefone für die Onboard-Aktivierung des Aktivierungscodes einrichten

Wenn Ihr Netzwerk für das Aktivierungscode-Onboarding konfiguriert ist, können Sie neue Telefone so konfigurieren, dass sie automatisch auf sichere Weise registriert werden. Sie generieren und stellen jedem Benutzer einen eindeutigen 16-stelligen Aktivierungscode zur Verfügung. Der Benutzer gibt den Aktivierungscode ein, und das Telefon wird automatisch registriert. Diese Funktion schützt Ihr Netzwerk, da das Telefon nicht registriert werden kann, bis der Benutzer einen gültigen Aktivierungscode eingibt.

Aktivierungscodes können nur einmal verwendet werden und haben ein Ablaufdatum. Wenn ein Benutzer einen abgelaufenen Code eingibt, zeigt das Telefon **Ungültiger Aktivierungscode** auf dem Display an. Wenn dies der Fall ist, geben Sie dem Benutzer einen neuen Code.

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. Gehen Sie hierzu wie folgt vor.

### Vorbereitungen

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

Wenn Sie einen Proxyserver für die Onboarding-Funktion einrichten möchten, stellen Sie sicher, dass der Proxyserver ordnungsgemäß konfiguriert ist. Siehe [Proxyserver einrichten](#).

Greifen Sie auf die Telefon-Webseite zu. [Auf Weboberfläche des Telefons zugreifen](#)

### Prozedur

- 
- Schritt 1** Setzen Sie das Telefon auf die Werkseinstellungen zurück.
- Schritt 2** Wählen Sie **Sprache > Bereitstellung > Konfigurationsprofil**.
- Schritt 3** Geben Sie im Feld **Profilregel** die Profilregel ein. Dieser Vorgang wird in der [Aktivierungscode Bereitstellungsparameter, auf Seite 20](#) Tabelle beschrieben.
- Schritt 4** (optional) Geben Sie im Abschnitt **Firmware-Upgrade** die Upgrade-Regel in das Feld **Upgrade-Regel** ein, wie in der Tabelle [Aktivierungscode Bereitstellungsparameter, auf Seite 20](#) beschrieben.
- Schritt 5** Übermitteln Sie Alle Änderungen.
- 

## Aktivierungscode Bereitstellungsparameter

Die folgende Tabelle definiert die Funktion und die Verwendung der Aktivierungscode-Parameter im Abschnitt **Konfigurationsprofil** auf der Registerkarte **Sprache > Bereitstellung** auf der Telefonwebsite. Außerdem wird die Syntax der Zeichenfolge definiert, die in der Telefon-Konfigurationsdatei mit dem XML-Code (cfg.xml) hinzugefügt wird, um einen Parameter zu konfigurieren.

Parameter	Beschreibung
Profilregel	Remote-Konfigurationsprofilregeln werden der Reihe nach evaluiert. Jede erneute Synchronisierung kann mehrere Dateien abrufen, die von verschiedenen Servern verwaltet werden.
Profile Rule B (Profilregel B)	Führen Sie eine der folgenden Aktionen aus:
Profile Rule C (Profilregel C)	<ul style="list-style-type: none"> <li>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML, eine Zeichenfolge im folgenden Format ein:</li> </ul>
Profile Rule D (Profilregel D)	<ul style="list-style-type: none"> <li>Geben Sie in der Telefon-Weboberfläche eine Zeichenfolge in folgendem Format ein:</li> </ul>
	<pre>gds://</pre>
	Standard: /\$PSN.xml

Parameter	Beschreibung
Upgrade-Regel	<p>Definiert das Upgrade-Skript für das Firmware Upgrade, das die Upgrade-Bedingungen und die damit in Verbindung stehenden Firmware URLs festlegt. Das Skript verwendet die gleiche Syntax wie die Profilregel.</p> <p>Führen Sie eine der folgenden Aktionen aus:</p> <ul style="list-style-type: none"> <li>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML, eine Zeichenfolge im folgenden Format ein: <pre>&lt;Upgrade_Rule ua="na"&gt;http://&lt;server ip address&gt;/ sip88xx.11-2-3MSR1-1.loads&lt;/Upgrade_Rule&gt;</pre> </li> <li>Geben Sie auf der Weboberfläche des Telefons die Upgrade-Regel ein: <pre>protocol://server[:port]/profile_pathname</pre> <p>Zum Beispiel:</p> <pre>tftp://192.168.1.5/image/sip88xx.11-2-3MSR1-1.loads</pre> </li> </ul> <p>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).</p> <p>Standard: leer</p>

## Direktes Migrieren des Telefons zu einem Unternehmenstelefon

Sie können Ihr Telefon jetzt problemlos in einem Schritt zu einem Unternehmenstelefon migrieren, ohne eine Übergangs-Firmware verwenden zu müssen.

### Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe [Auf Weboberfläche des Telefons zugreifen](#).

### Prozedur

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

**Schritt 2** Legen Sie im Feld **Upgrade-Regel** den Parameter für die Upgrade-Regel fest, indem Sie ein Firmware-Upgrade-Skript eingeben. Informationen zu den Syntaxdetails finden Sie unter der Definition für die Upgrade-Bedingungen und zugehörigen Firmware-URLs. Das Skript verwendet die gleiche Syntax wie die Profilregel. Geben Sie ein Skript ein und verwenden die folgendes Format, um die Upgrade-Regel einzugeben:

```
<tftp|http|https>://<ipaddress>/image/<load name>
```

Zum Beispiel:

```
tftp://192.168.1.5/image/sip78xx.14-1-1MN-366.loads
```

**Schritt 3** Konfigurieren Sie den Parameter **Transition Authorization Rule** (Übergangs-Autorisierungsregel), indem Sie einen Wert eingeben, mit dem Sie die Lizenz vom Server abrufen und sie autorisieren.

Sie können diesen Parameter ebenfalls in der Konfigurationsdatei (cfg.xml) konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

```
<Trans_Auth_Rule ua="na">http://10.74.51.81/prov/migration/E2312.lic</Trans_Auth_Rule>
```

**Schritt 4** Legen Sie im Parameter **Transition Authorization Type** (Übergangs-Autorisierungstyp) den Lizenztyp auf **Klassisch** fest.

Sie können diesen Parameter ebenfalls in der Konfigurationsdatei (cfg.xml) konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:

```
<Trans_Auth_Type ua="na">Classic</Trans_Auth_Type>
```

**Schritt 5** Klicken Sie auf **Submit All Changes**.

## 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>.

## Authentifizierung mit Basis-HTTPS-Neusynchronisierung

### Procedure

**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/privkey.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, on page 3](#) 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 **Submit All Changes**.

**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, on page 24](#) 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.

## HTTPS mit Client-Zertifikat authentifizieren

### Procedure

**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, on page 22](#) 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-Server für Clientfilterung und dynamischen Inhalt konfigurieren

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 Zertifikatsinformationen 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.

### Procedure

**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-Skripten auf dem HTTPS-Server.

**Schritt 4**

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

**Schritt 5**

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

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

**Schritt 6**

Klicken Sie auf **Submit All Changes**.

- Schritt 7** Beobachten Sie die Syslog-Ablaufverfolgung, um eine erfolgreiche Resynchronisierung sicherzustellen.
- Schritt 8** Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe [Auf Weboberfläche des Telefons zugreifen](#).
- 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.

Zusätzlich zu den von Cisco ausgestellten Zertifikaten akzeptiert das Telefon auch Serverzertifikate von einer Reihe häufig verwendeter SSL-Zertifikatsanbieter.

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

### Procedure

---

**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](mailto: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“. Zum Beispiel:

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

**Schritt 3** Generieren Sie eine CSR, die Felder enthält, die Ihr Unternehmen und Ihren Standort identifizieren. Zum 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 Domännennamens (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](mailto: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,

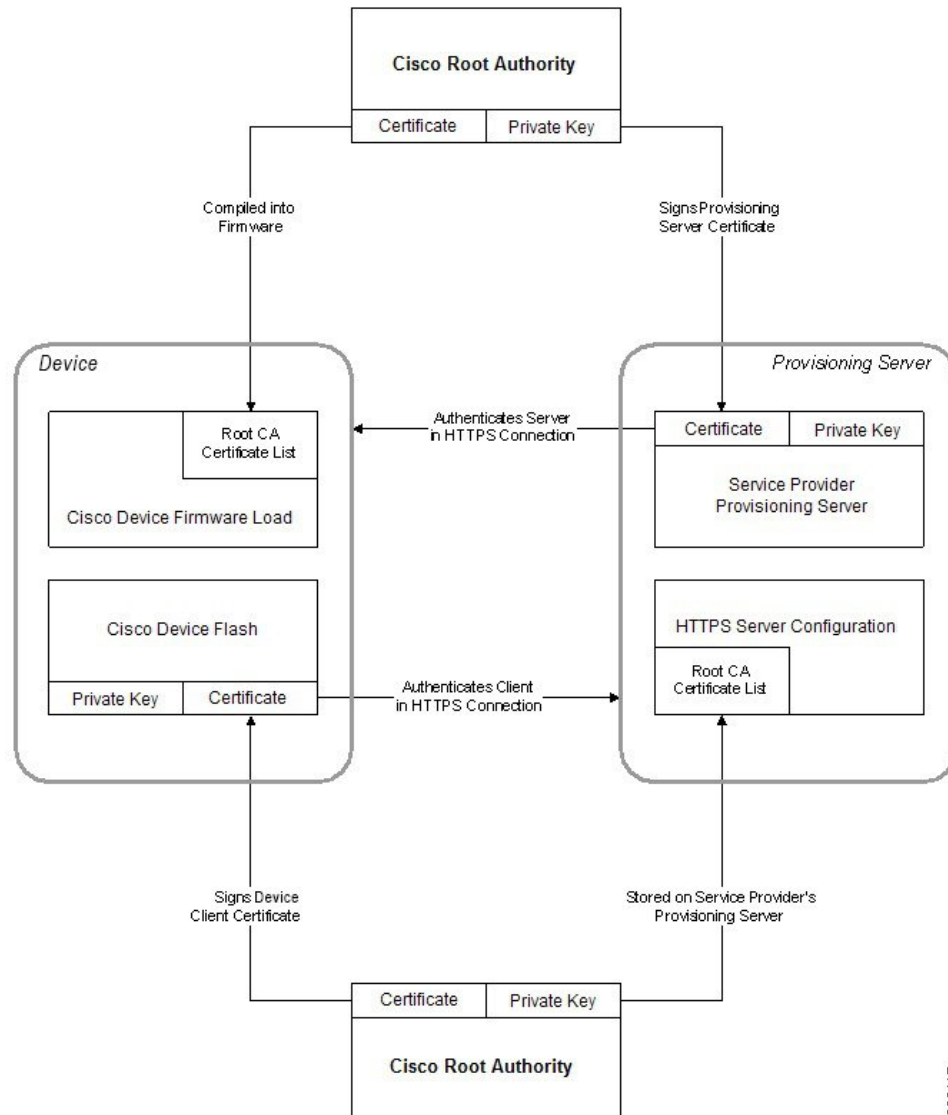
verfügt jedes Telefon auch über ein eindeutiges, von Cisco signiertes Clientzertifikat, das Informationen zum Identifizieren der einzelnen Endpunkte enthält. Jeder Serviceanbieter erhält ein Certificate Authority(CA)-Stammzertifikat, mit dem das Clientzertifikat des Geräts authentifiziert werden kann. 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.

Figure 1: 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

### Before you begin

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe [Auf Weboberfläche des Telefons zugreifen](#).

### Procedure

---

#### 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.



**Note** 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.

### Procedure

**Schritt 1** Installieren Sie Gzip auf dem lokalen Computer.

**Schritt 2** Komprimieren Sie das Konfigurationsprofil `basic.txt` (das in [TFTP-Resynchronisierung, on page 3](#) 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.

## 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 Profildaten 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.

## Procedure

---

**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, on page 3](#) 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, on page 30](#) 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 **Submit All Changes**.

**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.

---

## Partitionierte Profile erstellen

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

### Procedure

---

**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 **Submit All Changes**.

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.

- Standard: **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`.

---

## Verlängern des MIC-Zertifikats

Sie können das MIC (Manufacture Installed Certificate) durch den standardmäßigen oder den angegebenen SUDI-Dienst (Secure Unique Device Identifier) verlängern. Wenn das MIC-Zertifikat abläuft, funktionieren die Funktionen nicht, die SSL/TLS verwenden.

### Vorbereitungen

- Stellen Sie sicher, dass Sie den Dienst `sudirenewal.cisco.com` (Port 80) über Ihre Firewall zulassen, um die Verlängerung des MIC-Zertifikats zu ermöglichen.
- Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe [Auf Weboberfläche des Telefons zugreifen](#).

### Prozedur

---

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

**Schritt 2** Legen Sie im Abschnitt mit den **MIC-Zertifizierungseinstellungen** die Parameter wie in [Parameter für die MIC-Zertifikatsverlängerung durch SUDI-Service, auf Seite 34](#) definiert fest.

**Schritt 3** Klicken Sie auf **Submit All Changes**.

Nachdem die Zertifikatsverlängerung erfolgreich abgeschlossen wurde, wird das Telefon neu gestartet.

**Schritt 4** (optional) Überprüfen Sie den aktuellen Status der MIC-Zertifikatsverlängerung im Abschnitt mit dem **MIC-Zertifizierungsaktualisierungsstatus** unter **Info > Download-Status**.

**Hinweis** Wenn Sie das Telefon auf die Werkseinstellungen zurücksetzen, verwendet das Telefon das verlängerte Zertifikat weiterhin.

---

## Parameter für die MIC-Zertifikatsverlängerung durch SUDI-Service

In der folgenden Tabelle werden die Funktion und Verwendung der einzelnen Parameter im Abschnitt **MIC-Zertifikatseinstellungen** der Registerkarte **Sprache > Bereitstellung** definiert.

Tabelle 2: Parameter für die MIC-Zertifikatsverlängerung durch SUDI-Service

Parametername	Beschreibung und Standardwert
MIC CERT-Aktualisierung aktivieren	<p>Legt fest, ob die MIC-Verlängerung (Manufacture Installed Certificate) durch den standardmäßigen oder den angegebenen SUDI-Dienst (Secure Unique Device Identifier) aktiviert werden soll.</p> <p>Führen Sie eine der folgenden Aktionen aus:</p> <ul style="list-style-type: none"> <li>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML, eine Zeichenfolge im folgenden Format ein: <pre>&lt;MIC_Cert_Refresh_Enable ua="na"&gt;Yes&lt;/MIC_Cert_Refresh_Enable&gt;</pre> </li> <li>Wählen Sie auf der Weboberfläche des Telefons <b>Ja</b> oder <b>Nein</b> aus, um die Verlängerung des MIC-Zertifikats zu aktivieren oder zu deaktivieren.</li> </ul> <p>Gültige Werte: Ja und Nein Standard: Nein</p>
Regel für die MIC-Zertifizierungsaktualisierung	<p>Geben Sie die HTTP-URL des SUDI-Dienstes ein, der das verlängerte MIC-Zertifikat bereitstellt, zum Beispiel:</p> <pre>http://sudirenewal.cisco.com/</pre> <p><b>Hinweis</b> Ändern Sie die URL nicht. Für die Verlängerung des MIC-Zertifikats wird nur die standardmäßige URL unterstützt.</p> <p>Führen Sie eine der folgenden Aktionen aus:</p> <ul style="list-style-type: none"> <li>Geben Sie in der Telefonkonfigurationsdatei (cfg.xml) in XML, eine Zeichenfolge im folgenden Format ein: <pre>&lt;MIC_Cert_Refresh_Rule ua="na"&gt;http://sudirenewal.cisco.com/&lt;/MIC_Cert_Refresh_Rule&gt;</pre> </li> <li>Geben Sie in der Telefon-Weboberfläche die zu verwendende HTTP-URL ein.</li> </ul> <p>Zulässige Werte: eine gültige URL, die 1024 Zeichen nicht überschreitet Standard: http://sudirenewal.cisco.com/</p>

