

Autoprovisionierung verschlüsseln

Der UCware Server verschlüsselt die Provisionierung **unterstützter Telefone** standardmäßig mit einem selbstsignierten Zertifikat. Bei Bedarf können Sie dieses bei Bedarf durch ein ca-signiertes Zertifikat ersetzen Sie können dieses durch ein

Hierfür wird im Auslieferungszustand ein selbstsigniertes Zertifikat verwendet. Dieses kann gegen ein beliebiges Zertifikat ausgetauscht werden.

Grundlagen

UCware bietet zwei Methoden, um die Autoprovisionierung zu verschlüsseln:

- ohne Überprüfung der Gerätezertifikate
- mit Überprüfung der Gerätezertifikate

Im zweiten Fall müssen sich die angeschlossenen Geräte als zum jeweiligen Hersteller gehörig authentisieren.

Welche Methode zum Einsatz kommt, legen Sie über die Konfiguration des Web- und des DHCP-Servers auf der Telefonanlage fest.



Hinweis:

Aktivieren Sie stets nur eine oder keine der beiden Verschlüsselungsmethoden.

Web-Server konfigurieren

Um die Verschlüsselung zu (de)aktivieren, erstellen Sie eine symbolische Verknüpfung auf dem Web-Server. Ziel und Speicherort der Verknüpfung hängen dabei vom Hersteller der angeschlossenen Telefone und der gewünschten Verschlüsselungsmethode ab:

Hersteller	Verknüpfungsziel
Snom	/etc/nginx/locations.d/50-prov-snom.conf
Yealink	/etc/nginx/locations.d/52-prov-tiptel-yealink.conf
Gigaset	/etc/nginx/locations.d/51-prov-gigaset.conf
Methode	Speicherort
unverschlüsselt	/etc/nginx/http.d/
verschlüsselt ohne Prüfung des Gerätezertifikats	/etc/nginx/https.d/
verschlüsselt mit Prüfung des Gerätezertifikats	/etc/nginx/https-alt.d/
Nur für Snom und Yealink verfügbar.	

Gehen Sie wie folgt vor:

1. Greifen Sie über Secure Shell (SSH) auf den UCware Server zu.
2. Deaktivieren Sie die aktuelle Verschlüsselungsmethode, indem Sie alle zugehörigen Verknüpfungen löschen:

```
sudo rm /etc/nginx/http*.d/5*-prov-*.conf
```

3. Aktivieren Sie die neue Methode, indem Sie eine Verknüpfung mit dem zugehörigen Ziel im zugehörigen Verzeichnis erstellen:

```
sudo ln -s [Verknüpfungsziel] [Speicherort]
```

4. Wiederholen Sie Schritt 3 für alle gewünschten Geräte-Hersteller.
5. Starten Sie den Web-Server neu:

```
sudo systemctl restart nginx
```

DHCP-Server konfigurieren



Hinweis:

Die folgenden Schritte gelten für den integrierten DHCP-Server der Telefonanlage. Wenn Sie den Dienst anderweitig hosten,



weicht die Vorgehensweise ab.

Nachdem Sie die gewünschte Verschlüsselungsmethode aktiviert haben, konfigurieren Sie den DHCP-Server. Dazu passen Sie das Protokoll und den Port für die Provisionierung entsprechend an:

Methode	Protokoll	Port
unverschlüsselt	http	80
verschlüsselt ohne Prüfung des Gerätezertifikats	https	443
verschlüsselt mit Prüfung des Gerätezertifikats	https	8443

Nur für Snom und Yealink verfügbar.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Datei `/etc/dhcp/dhcpd.conf` mit einem Texteditor, z. B. Nano:

```
sudo nano /etc/dhcp/dhcpd.conf
```

2. Scrollen Sie zum Bereich des gewünschten Herstellers.



Hinweis:

Für Tisch- und DECT-Telefone von Snom erfolgt die Konfiguration getrennt in den Bereichen **Snom** (für Tischtelefone) und **Snom IPDECT**.

```
#####  
# Snom  
#####  
class "Snom" {  
    match if (  
        (substring(hardware, 1, 3) = 00:04:13)  
        and not (substring(pick-first-value(option vendor-class-iden$  
and not ( (substring(pick-first-value(option vendor-class-identifizier$  
));  
# store vendor-class-identifier in the lease:  
set vendor-class-identifier = pick-first-value(option vendor-class-iden$  
  
# DHCP options 66/67  
option tftp-server-name "http://172.17.2.1:80";  
option bootfile-name "ucware/prov/snom/settings.php?mac={mac}";  
  
    default-lease-time 2764800; # 32 days  
    max-lease-time 3024000; # 35 days  
}
```

3. Passen Sie in der Zeile `option tftp-server-name [...]` das Protokoll und den Port gemäß der aktiven Verschlüsselungsmethode an.
4. Für die Provisionierung über HTTPS ersetzen Sie zusätzlich die IP-Adresse des UCware Servers durch den **Fully-Qualified Domain Name**.
5. Wiederholen Sie die Schritte 2 bis 4 bei Bedarf für weitere Hersteller bzw. Geräte-Typen.
6. Speichern Sie die Änderungen.

UCware Daemon konfigurieren

Im nächsten Schritt konfigurieren Sie den UCware Daemon.

Gehen Sie dazu wie folgt vor:

1. Öffnen Sie die Datei `/opt/ucwared/ucwared.conf` mit einem Texteditor:

```
sudo nano /etc/dhcp/dhcpd.conf
```

2. Ersetzen bzw. ergänzen Sie im Bereich **[provisioning]** die folgenden Zeilen gemäß der gewählten Verschlüsselungsmethode:

```
protocol = [http oder https]
host = [Fully-Qualified Domain Name]
port = [80, 443 oder 8443]
```

3. Speichern Sie die Änderungen.

Key-Value-Store konfigurieren

Abschließend konfigurieren Sie den Key-Value Store um die gewählte Verschlüsselungsmethode im Key-Value-Store des UCware Servers.

Gehen Sie dazu wie folgt vor:

1. Rufen Sie im Admin-Client die Detailseite  **System > Key-Value-Store** auf.
2. Passen Sie die Werte der folgenden Schlüssel gemäß der gewählten Verschlüsselungsmethode an:

Schlüssel	Wert
PROV_SCHEME	[http oder https]
PROV_HOST	[Fully-Qualified Domain Name]
PROV_PORT	[80, 443 oder 8443]



3. Übernehmen Sie die Einstellungen mit

Neues Zertifikat hochladen

Nach einer



Hinweis:
Eigene Zertifikate müssen im PEM-Format vorliegen.

Um ein anderes Zertifikat zu verwenden, laden Sie dieses und den zugehörigen Schlüssel im Admin-Client unter  **System > SSL-Zertifikat** hoch.



</WRAP>

From:
<https://wiki.ucware.com/> - **UCware-Dokumentation**

Permanent link:
https://wiki.ucware.com/adhandbuch/provisionierung/provisionierung_ssl?rev=1643099551

Last update: **18.03.2023 14:47**