HTTPS Provisioning

Starting with openUC and sipXecs 4.6.0 Update 3 HTTPS provisioning is possible with Polycom phones running firmware 4.0 and later.

Overview

In order for the phone and sipXecs to communicate securely, a certificate must be used. We distinguish two cases:

1. using self signed certificate - we'll discuss about using sipXecs default self signed certificate
2. using a certificate signed by a well known certificate authority.

In order to setup a phone to provision using HTTPS you must select Server Type: HTTPS under Admin Settings > Network > Provisioning Server.

Secure provisioning using sipXecs self signed certificate

> **Note**
>
> Please keep in mind that if you use a self signed certificate you will always need an "unsecure" step, that being uploading the certificate to the phone.

Follow the steps here: Installing the Root CA Server Certificate on the Polycom Phone to install the root CA on the phone. If you already have the phone running 4.0 firmware revision registered in sipXecs you can send profiles to the phone, and the certificate will be uploaded automatically to the phone. Then you may change the provisioning server type to use HTTPS. The phone will provision from then forward securely.

Auto-provisioning

In order to auto-provision a phone (for instance out of the box) using the self signed certificate you need to you need to upload the root CA on the phone first. You don't even need to register with sipXecs in order to do this, you just need to boot the phone in the same network with sipXecs and follow the above steps to upload the CA. Once the root CA is on the phone you may change the provisioning server type to use HTTPS. The phone will auto-provision securely.

Secure provisioning using a certificate signed by a well known CA

The best option to provision securely is to use a certificate signed by a well known CA. The phone has the most common root CAs installed from the factory and the phone will certify the server's certificate. So in this case there is no extra "unsecure" step to follow, and secure provisioning (including auto-provisioning) can be achieved out-of-the-box.

Trusted Certificate Authority List

The phone trusts the following certificate authorities by default:

- AAA Certificate Services by COMODO
- ABAecom (sub., Am. Bankers Assn.) Root CA
- Add Trust Class1 CA Root by COMODO
- Add Trust External CA Root by COMODO
- Add Trust Public CA Root by COMODO
- Add Trust Qualified CA Root by COMODO
- ANX Network CA by DST
- American Express CA
- American Express Global CA
- BelSign Object Publishing CA
- BelSign Secure Server CA
- COMODO CA Limited
- COMODO Certificate Authority
- Deutsche Telekom AG Root CA
- Digital Signature Trust Co. Global CA 1
- Digital Signature Trust Co. Global CA 2
- Digital Signature Trust Co. Global CA 3
- Digital Signature Trust Co. Global CA 4
- Entrust Worldwide by DST
- Entrust.net Premium 2048 Secure Server CA
- Entrust.net Secure Personal CA
- Entrust.net Secure Server CA
- Equifax Premium CA
- Equifax Secure CA
- Equifax Secure eBusiness CA 1
- Equifax Secure eBusiness CA 2
- Equifax Secure Global eBusiness CA 1
- GeoTrust Primary Certification Authority
- GeoTrust Global CA
- GeoTrust Global CA 2

- GeoTrust Universal CA
- GeoTrust Universal CA 2
- GTE CyberTrust Global Root
- GTE CyberTrust Japan Root CA
- GTE CyberTrust Japan Secure Server CA
- GTE CyberTrust Root 2
- GTE CyberTrust Root 3
- GTE CyberTrust Root 4
- GTE CyberTrust Root 5
- GTE CyberTrust Root CA
- GlobalSign Partners CA
- GlobalSign Primary Class 1 CA
- GlobalSign Primary Class 2 CA
- GlobalSign Primary Class 3 CA
- GlobalSign Root CA
- National Retail Federation by DST
- RSA 2048 v3
- Secure Certificate Services by COMODO
- TC TrustCenter, Germany, Class 1 CA
- TC TrustCenter, Germany, Class 2 CA
- TC TrustCenter, Germany, Class 3 CA
- TC TrustCenter, Germany, Class 4 CA
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA
- Thawte Universal CA Root
- Trusted Certificate Services by COMODO
- UTN-DATA Corp SGC by COMODO
- UTN-USER First-Client Authentication and Email by COMODO
- UTN-USER First-Hardware by COMODO
- UTN-USER First-Object by COMODO
- UPS Document Exchange by DST
- ValiCert Class 1 VA
- ValiCert Class 2 VA
- ValiCert Class 3 VA
- VeriSign Class 4 Primary CA
- Verisign Class 1 Public Primary Certification Authority
- Verisign Class 1 Public Primary Certification Authority - G2
- Verisign Class 1 Public Primary Certification Authority - G3
- Verisign Class 2 Public Primary Certification Authority
- Verisign Class 2 Public Primary Certification Authority - G2
- Verisign Class 2 Public Primary Certification Authority - G3
- Verisign Class 3 Public Primary Certification Authority
- Verisign Class 3 Public Primary Certification Authority - G2
- Verisign Class 3 Public Primary Certification Authority - G3
- Versign Class 3 Public Primary Certification Authority – G5
- Verisign Class 4 Public Primary Certification Authority - G2
- Verisign Class 4 Public Primary Certification Authority - G3
- Verisign/RSA Commercial CA
- Verisign/RSA Secure Server CA
- Windows Root Update by COMODO