

Certificates

- [System Certificates](#)
- [Chrome and Self Signed Certificates](#)
 - [On a Windows PC](#)
 - [On a Mac](#)
 - [On a Fedora Workstation](#)

System Certificates

Sipxcom works with two types of certificates:

1. Web certificate needed for system GUI and Unite Web -User portal
2. Sip certificate needed for TLS communication between Proxy and Phones

open communication.

USERS DEVICES FEATURES SYSTEM DIAGNOSTICS

CERTIFICATES

Web Certificate

SIP Certificate

Certificate Authorities

Certificate File: ssl-web.crt [Show certificate](#)

Encryption strength: 2048 bit

Rebuild Certificate: **Rebuild**

Rebuild private key is using 2048 bit encryption

You only need to rebuild the certificate if the private key has been compromised, the certificate is about to expire as its contents are somehow invalid.

Certificate & Key File Certificate & Key Text

Certificate File: **Browse...** No file selected.

Key File (Optional): **Browse...** No file selected.

Certificate Chain File: **Browse...** No file selected.

CA Certificate File: **Browse...** No file selected.

Import

Certificate Signing Request

Country: US (Default: US)

State: AnyState (Default: AnyState)

Import a certificate based on a CSP. Or a certificate & key generated from a third party authority. Be sure to add authority to 'Certificate Authorities' page.

Certificate Signing Request (CSR)

Upon installation of your system a default self-signed certificate was installed to secure Web access. This certificate causes browsers to show a security warning message. If you would like to remove this warning you have to install a trusted certificate available from Certificate Authority such as VeriSign, Entrust, Comodo, GlobalSign etc.

This page allows you to create the necessary Certificate Signing Request (CSR) needed by Certificate Authority and then install the new certificate.

Generate a new Certificate Signing Request (CSR) by filling the fields with the appropriate information.

1. To upload a (trusted) web certificate you need to generate a Certificate Signing Request that will be sent to a Certificate Authority. You can do this either by using internal CSR generation mechanism from Sipxcom or by using a different machine. If you are using a different machine you need to make sure that you will have your "private key" stored in a safe place and that you are using complete FQDN or you can ask for a wild-card certificate that should match your domain (go to step C.).

A.generate CSR:

Email: root@test.miahi (Default: root@test.miahi)

Generate CSR

Generates a CSR for the installed certificate

```
-----BEGIN CERTIFICATE REQUEST-----
MIDPJCAlYCAQAwgZcxCAJBgIVBAYTAITMREwDwyDVQIDAH
BbnITdGF0ZTEQ
MA4GA1UEBwwHQW55VG93bjETMBEGA1UECgwKdGVzdC5taWF
oaTEQMA4GA1UECwwH
c2lwWGVjczEcmBoGA1UEAwwTdWxkNDPpc28udGVzdC5taWFOaT
EeMBwGCScqGSIb3
DQEJAPYPCm9vdEB0ZXN0Lm1pYWhpMIBiJANBgkqhkiG9w0BAQE
FAAOCAQ8AMIIB
CgKCAQEAlVsoChVMPbWyoUedDms30Pbx3CGiWuUeVaqG7bR
bMQ3LT5oyJBxQyK
IjRNOxKuOUJg/ekj8E1qQ5bBp7BWNd89V
IjHUXG8m9FS3DYTAJONVMLbj8IHnH
ZyE267WubtrGcli
/dnhP+GXC10Xe9P91v24cx44OAzNScWcBwz5dJpCDBLsvfH
f5VYC8B2YBKVE
/586+sSkUJ4BsPS4yTT490lx5W a6acHpWafUjlnkurDJN/
gIFd1f84qRFAR4sJPDkriUNN+z3aapS2eGJ7ZKLWEU
/eIzQYA9xp65CrBOCEW
1jZPSqA2z4AinLUH0Z82HcmWUwwIDAQABoGEWwYJKoZlHvc
NAQK0MvIwUDAt
BgNVHQ4EGAQWBBR5FmW6YqYGngEH12vzsn3lqLXZjALBgNVH
RMEBAQCMAAAWAD
VfOPBBkEFzAvghh1YzE0NGIzby50ZXN0Lm1pYWhpMA0GCScqGSI
b3DQEBBQUAA4IB
```

B Sent your csr file to a trusted authority to sign it.

C. If you receive any intermediary certificate from your CA you need to uploaded it here, if not you can skip this step:

Certificate Chain File No file selected.

D. If you used a different machine to issue your csr then you MUST import your private key (skip if you used sipxcom internal mechanism):

Certificate File No file selected.
 Key File (Optional) No file selected.

E. Import your signed certificate:

Certificate & Key File No file selected.

After you reconnect to system GUI you should see in your browser information about your newly signed(or not signed) certificate.

You can check the time of creation and content of ssl-web.crt and ssl-web.key from this path /etc/http/conf.d/ssl/ to make sure it matches your newly uploaded certificate and key (if needed).

Troubleshooting:

If something goes wrong don't panic you can always access your system GUI from HTTP by using the below method:

- a.service iptables stop
- b.connect to http://Your_IP:12000/sipxconfig/app
- c. Re-try adding the certificate or simply "Rebuild" sipxcom self signed certificate

Still having problems? then take a look at /var/log/sipxpbx/sipxconfig.log and /var/log/httpd also a service httpd restart may be needed.

Usually a key mismatch is the common problem, you can see this is in /var/log/httpd/ssl_error.log - depending on your certificate provider you will be able to re-key the certificate with the current ssl-web.key or you will need to submit a new CSR.

Very important: keep your initial ssl-web.key safe (copy to another machine). This is the key used when CSR was issued and if you hit Rebuild it will be overwritten.

2. Sip Certificate and how to upload CA to a polycom phone.

As mentioned earlier SIP Certificate is needed if you are planning to use TLS signaling between Phones and proxy.

Self signed sip certificate issued by sipxcom can be used simply by setting transport to TLS from Devices--> Line ---> Registration page.

Registration server

Primary registration server

address (Default: test.miahi)
Primary Registration Server: IP address or host name of a SIP server that accepts registrations.

port (Default: 0)
0, empty, 1 to 65535

transport (Default: UDPOOnly)
DNSNaptr, TCPpreferred or UDPOOnly. If empty or DNSNaptr and if Address is a hostname and Port is 0 or empty, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If Address is an IP address, or a port is given, then UDP is used. If set to TCPpreferred: TCP is the preferred transport, UDP is used if TCP fails. If set to UDPOOnly: Only UDP will be used.

Since polycom phones are auto-provisioned they will acquire Certificate Authority corresponding to sipxcom file from the beginning.

If you are planning to use a signed sip certificate or a self signed certificate (as always don't forget to save your private key) you will need to upload the both under System--> Certificate --> Sip Certificate page

CERTIFICATES

Web Certificate

SIP Certificate

Certificate Authorities

Certificate File ssl.crt
[Show certificate](#)

Certificate is used for secure communications to other systems in a specific context like SIP or system is valid for two years before it needs to be rebuilt. Show certificate description for expiration

Encryption strength 2048 bit

Installed private key is using 2048 bit encryption

Rebuild Certificate Rebuild

You only need to rebuild the certificate if the private key has been compromised, the certificate somehow invalid.

Certificate & Key File Certificate & Key Text

Certificate File Browse... No file selected.

Key File (Optional) Browse... No file selected.

Import

In order for clients (in this case phones) to trust a certificate they need to have a valid CA file for the issues of the sip certificate they will receive. Since the new certificate is not created by sipxcom you will need to upload CA file to phones.

if you are using a softphone like zoiper you can do this by simply reaching to the menu that will let you upload CA.

The screenshot shows a SIP account configuration interface. On the left, a sidebar displays 'SIP' and a checked status for '2048@ezuce.com'. The main panel has tabs for 'General', 'Extra', 'Codec', and 'Advanced', with 'Advanced' selected. Under 'Advanced account options', there are several settings: 'Registration expiry' is set to 3600; 'Keep alive time-out' is set to 'Disable' with a '30' input field; 'Enable ZRTP' is a checkbox; 'Use BLF' is a checkbox; 'Subscribe presence' and 'Publish presence' are checked checkboxes; 'Send KPML' is a checkbox; 'Use DTMF RFC-2833' is a dropdown menu; 'Use rport' is a checkbox; 'Use TLS transport' is a dropdown menu; 'Use rport media' is a checkbox; 'TLS with no SRTP' is a dropdown menu; 'Force RFC-3264' is a checkbox; 'Use default STUN' is a dropdown menu. Below this is the 'TLS client certificate' section, which includes a 'Certificate file' input field with a browse button and a 'Use certificate as:' dropdown menu set to 'Use certificate'.

If you are using a provisioned phone like polycom with firmware => 4.x you can create a custom config file with the following content

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
<sec
sec.TLS.customCaCert.2="—BEGIN CERTIFICATE---
```

```
YOUR CERTIFICATE AUTHORITY FILE
-----END CERTIFICATE-----"
sec.TLS.profile.2.deviceCert="Application2"
sec.TLS.profileSelection.SIP="ApplicationProfile2"
sec.TLS.profile.2.caCert.application2="0"
sec.TLS.profile.2.caCert.application3="0"
sec.TLS.profile.2.caCert.application4="0"
sec.TLS.profile.2.caCert.application5="0"
sec.TLS.profile.2.caCert.application6="0"
sec.TLS.profile.2.caCert.defaultList="0"
sec.TLS.profile.2.caCert.platform1="0"
sec.TLS.profile.2.caCert.platform2="0"
/>
</polycomConfig>
```

Then go to Devices--> Devices Files--> Unmanaged TFTP and upload this custom file

Last go to Devices --> MAC--> Custom Configuration--> Select File name(exactly as the name of the cfg file uploaded at previous step) ---> Send profiles

Chrome and Self Signed Certificates

Chrome likes to complain about self signed certificates. To resolve this either, upload a valid web certificate or:

On a Windows PC

On a Mac

1. In the address bar, click the red lock with the X. This will bring up an information screen. In the 'Connection' tab, click the link that says "Certificate Information".
2. Click and drag the image of the certificate to your desktop.
3. Double-click on the certificate on your desktop will bring up the Keychain Access utility. Enter your password to enter the application.
4. Click on the lock icon in the program to unlock it.
5. Find the certificate in the System keychain. Double click on it.
6. Expand 'Trust'
7. Find 'When using this certificate' entry select "Always Trust" from the drop down selector.

Close Keychain Access and restart Chrome, and the self-signed certificate should be recognized now by the browser. (it still won't be green in the address bar, but the browser won't keep prompting you)

On a Fedora Workstation



Incomplete

This page needs your help to finish.