Application Note – AN17038

MT AppNote 17038 (AN 17038)
September 2017

Best Practices for Security Certificates w/ Connect

Description: This Application Note describes the process and best practices for using SSL certificates with Mitel Connect OnSite Systems

Environment: Mitel IP-PBX versions Connect

Contents

Introduction

This guide is intended for professional services engineers or technical personnel responsible for system installation and administration. This guide describes the procedure of utilizing SSL security certificates with the Unified Communications Mitel Connect systems.

Security Certificate

Security certificates are data files that bind a cryptographic key to a company's details. When installed on a server, it allows for secure communications between the client application via the https protocol (over port 443) and the designated server.

An organization will usually purchase certificates for all servers individually or by way of a wildcard certificate to use on their entire domain of servers. A wildcard certificate will cover all 'sub-domains' and servers for that domain. This type of certificate may be the preferred method if the Mitel UC solution is comprised of numerous servers.

Certificates on HQ Server

The certificate authority (CA) in the Mitel Connect Director HQ server is used to sign certificates for Mitel Connect. Encryption is provided for all end-user communication, including all protocols to and from the Mitel 400-series phones (except for a few downloaded configuration files), and all protocols to and from the Mitel Connect client.

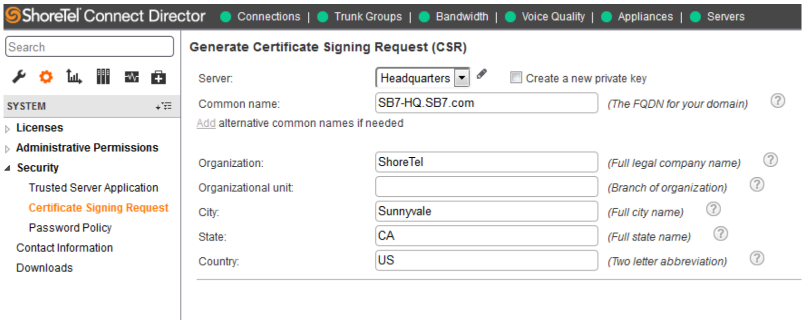
To ensure secure (HTTPS) client access and avoid warning messages, you must install a custom certificate purchased from a public certificate vendor. This is the only method for ensuring that the Mitel Connect client is secure. The Mitel Connect client falls back to HTTP if certificates are not installed to enable HTTPS. Connecting securely requires trusted certificates to be deployed on all platforms where the client connects. If ensuring secure client access is not a requirement, you can opt to use the default certificates signed by the Mitel UC Certificate Authority that are created during installation.

A certificate signing request (CSR) can be generated from the Mitel Director web interface.

1. In Director, go to **System** – **Security** – **Certificate Signing Request**.
2. Select Headquarter from the drop-down list for **Server**.
3. The FQDN should automatically populate from the given name in the Platform Equipment page. If not change the name to reflect proper host name.
4. Click **Add alternative common names** if needed.
5. Organization, city, state and country should auto-fill from Platform Equipment configuration page.

   Note: State name needs to be the full name, <u>not</u> the two-letter abbreviation. (eg. California)

6. Click **Generate** button at top right when done. This will prompt the saving of a CSR file to the local computer.
7. Submit the CSR to your preferred SSL certificate vendor.


ShoreTel Connect Director
Connections | Trunk Groups | Bandwidth | Voice Quality | Appliances | Servers
Search
SYSTEM
Licenses
Administrative Permissions
Security
Trusted Server Application
Certificate Signing Request
Password Policy
Contact Information
Downloads

Generate Certificate Signing Request (CSR)

Server: Headquarters ☐ Create a new private key

Common name: SB7-HQ.SB7.com (The FQDN for your domain)

Add alternative common names if needed

Organization: ShoreTel (Full legal company name)

Organizational unit: (Branch of organization)

City: Sunnyvale (Full city name)

State: CA (Full state name)

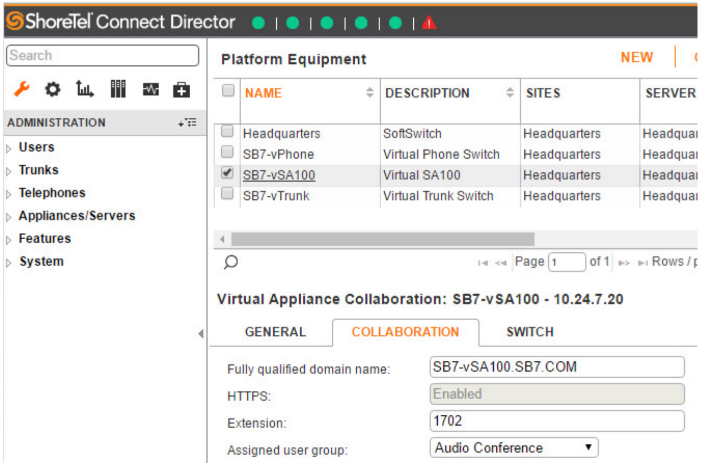
Country: US (Two letter abbreviation)

To install certificates, you use the Certificates tab on the Platform Equipment page in Mitel Connect Director. This process assumes that you have purchased a signed certificate from a trusted Certificate Authority vendor.

1. After purchasing a signed certificate from a CA vendor, store all the files received from the vendor, which should include the SSL certificate and the intermediate CA certificates, into a staging folder that you access for the upload. (Note that vendors might return files in various formats and file types and might return a password along with the files.)
2. Verify that there is a certificate currently installed.
3. Launch Mitel Connect Director.
4. On the navigation pane, click Administration > Appliances/Servers > Platform Equipment.
5. On the list pane, click the name of the device on which you want to install the certificate.
6. Click the Certificate tab on the details pane.
7. If provided by the vendor, in the Certificate password field enter the password for the certificate.
8. Browse to the certificate files and then click the Save button in the upper right of the window.

Create a CSR on a Mitel Service Appliance

Service Appliances do need to have the CSR filled out if you are going to be using the Fully Qualified Domain Name (FQDN) of the conferencing server in the Mitel Connect Director settings pages. (See pic below) The Collaboration tab is used for setting the FQDN of the appliance. You will notice from the pic that the Name field is underlined. If you mouse click on the underlined name field, then it will open another browser tab with the admin page of that Service Appliance.



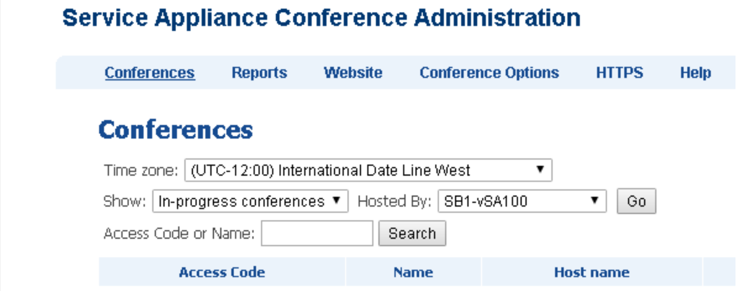
Platform Equipment

☐	NAME	DESCRIPTION	SITES	SERVER
☐	Headquarters	SoftSwitch	Headquarters	Headquai
☐	SB7-vPhone	Virtual Phone Switch	Headquarters	Headquai
☑	SB7-vSA100	Virtual SA100	Headquarters	Headquai
☐	SB7-vTrunk	Virtual Trunk Switch	Headquarters	Headquai

Virtual Appliance Collaboration: SB7-vSA100 - 10.24.7.20

Fully qualified domain name: SB7-vSA100.SB7.COM
HTTPS: Enabled
Extension: 1702
Assigned user group: Audio Conference

Once you have opened the **Service Appliance Conference Administration** page you can click on the **HTTPS** menu option to change to that settings page.

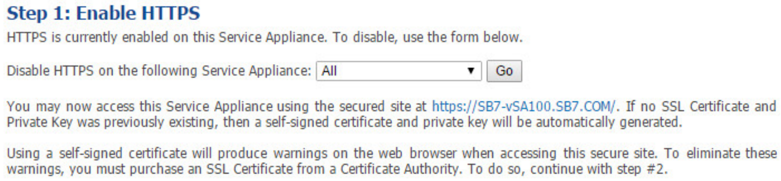


Service Appliance Conference Administration

Conferences

Time zone: (UTC-12:00) International Date Line West
Show: In-progress conferences
Hosted By: SB1-vSA100
Access Code or Name:

Access Code	Name	Host name



Step 1: Enable HTTPS

HTTPS is currently enabled on this Service Appliance. To disable, use the form below.

Disable HTTPS on the following Service Appliance: All

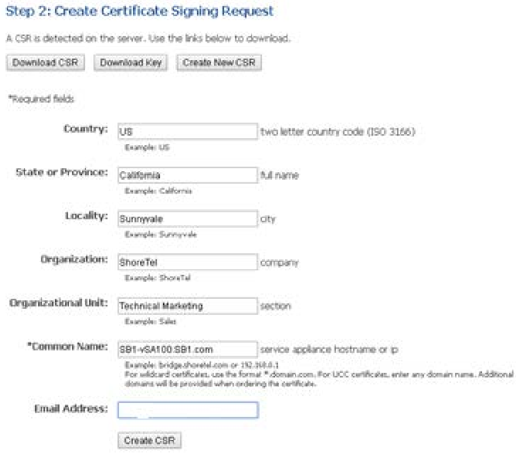
You may now access this Service Appliance using the secured site at https://SB7-vSA100.SB7.COM/. If no SSL Certificate and Private Key was previously existing, then a self-signed certificate and private key will be automatically generated.

Using a self-signed certificate will produce warnings on the web browser when accessing this secure site. To eliminate these warnings, you must purchase an SSL Certificate from a Certificate Authority. To do so, continue with step #2.

As you can see, this page has dynamic content inline that tells you currently this device is configured for

HTTPS and it is enabled. There is a drop-down list box for options of controlling one or more appliances and a **Go** button. If your appliance is still in HTTP mode it will be represented here as such and you will have the option of enabling it. You can also see the FQDN of the appliance in question as depicted here as https://SB7-vSA100.SB7.COM in blue text.

Step 2: Create Certificate Signing Request is electronic form that will generate a digital file known as the CSR. This file can be used to request a certificate from a recognized root authority. This is also a mandatory step if you plan on using a self-signed certificate and wish to reference your appliance via a FQDN. Failing to fill out and save this CSR request will result in your Connect Client reporting that it is not connecting securely with your Conferencing Server. Additionally, if you try and import the certificate into your client machine it will reference as *IM Appliance* instead of the FQDN of your service appliance.



Step 2: Create Certificate Signing Request

A CSR is detected on the server. Use the links below to download.

*Required fields

Country: US two letter country code (ISO 3166)
Example: US

State or Province: California full name
Example: California

Locality: Sunnyvale city
Example: Sunnyvale

Organization: ShoreTel company
Example: ShoreTel

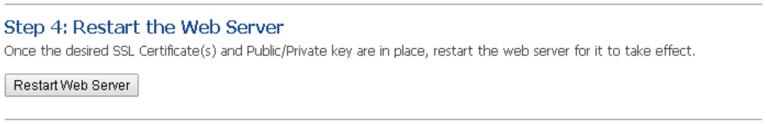
Organizational Unit: Technical Marketing section
Example: Sales

*Common Name: SB1-vSA100.SB1.com service appliance hostname or ip
Example: bridge.shoretel.com or 192.168.0.1
For wildcard certificates, use the format *.domain.com. For UCC certificates, enter any domain name. Additional domains will be provided when ordering the certificate.

Email Address:

Fill out the information requested and be sure to spell out the state name (do not use two letter abbreviations). Click the **Create CSR** button and it will prompt to save the file.

Skip to **Step 4: Restart the Web Server** and click the button.



Step 4: Restart the Web Server

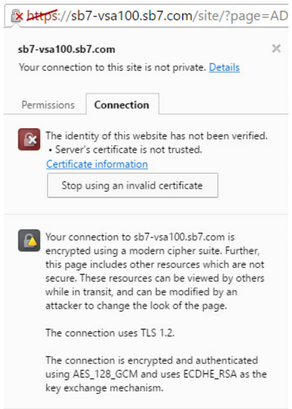
Once the desired SSL Certificate(s) and Public/Private key are in place, restart the web server for it to take effect.

Wait approximately 2 minutes for web server to come fully online and proceed.

Exporting the Certificate

Next, generate a copy of the certificate that you can upload to the client PC certificate stores. Open Connect Director and log in with an administrative permissions account. Click on **Administration** (wrench icon) in the navigation pane and go to **Appliances/Servers** and **Platform Equipment**. Click on the underlined name field of the appliance to open the UCB admin webpage.

If you click on the lock, more information can be obtained, as well as a method for extracting the proper certificate to gain secure communications. A tabbed sub window will open and the **Connection** tab will inform you of the status of the connection to the server.



~~https~~://sb7-vsa100.sb7.com/site/?page=AD

sb7-vsa100.sb7.com

Your connection to this site is not private. Details

The identity of this website has not been verified.
• Server's certificate is not trusted.
Certificate information

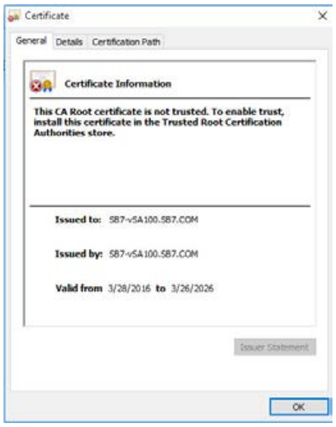
Your connection to sb7-vsa100.sb7.com is encrypted using a modern cipher suite. Further, this page includes other resources which are not secure. These resources can be viewed by others while in transit, and can be modified by an attacker to change the look of the page.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

As you can see from this example the connection is not secure and the server's certificate is not trusted. Click on the **Certificate information** link in blue and another window will open providing the additional information regarding this certificate.

The General tab will show the FQDN name you have entered in the CSR previously.



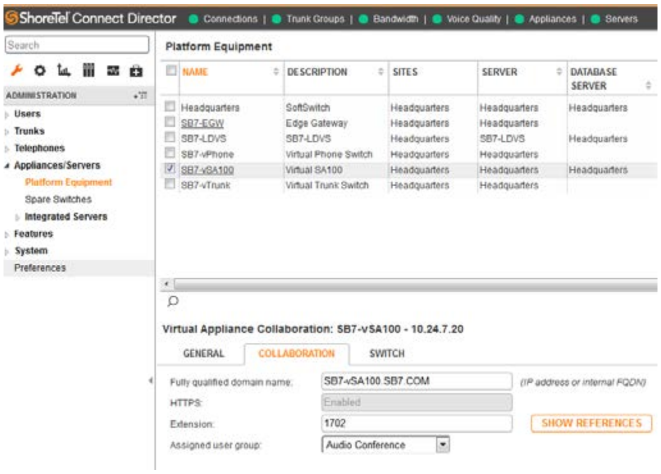
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: SB7-vSA100.SB7.COM

Issued by: SB7-vSA100.SB7.COM

Valid from 3/28/2016 **to** 3/26/2026



Platform Equipment

□	NAME	DESCRIPTION	SITES	SERVER	DATABASE SERVER
□	Headquarters	SoftSwitch	Headquarters	Headquarters	Headquarters
□	SB7-EGW	Edge Gateway	Headquarters	Headquarters	
□	SB7-LDVS	SB7-LDVS	Headquarters	SB7-LDVS	Headquarters
□	SB7-vPhone	Virtual Phone Switch	Headquarters	Headquarters	
☑	SB7-vSA100	Virtual SA100	Headquarters	Headquarters	Headquarters
□	SB7-vTrunk	Virtual Trunk Switch	Headquarters	Headquarters	

Virtual Appliance Collaboration: SB7-vSA100 - 10.24.7.20

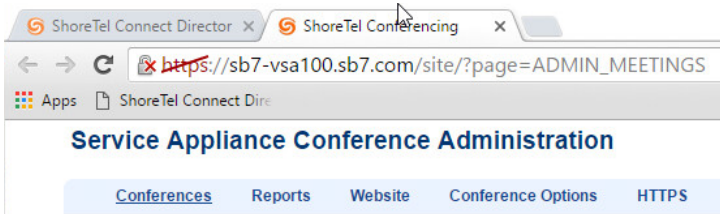
Fully qualified domain name: SB7-vSA100.SB7.COM (IP address or internal FQDN)

HTTPS: Enabled

Extension: 1702

Assigned user group: Audio Conference

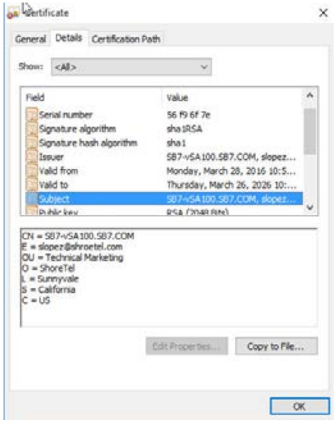
When the admin web page opens you will see that the connection has security issues via the lock being grey with a red x and slash thru the https:// in the address bar.



~~https~~://sb7-vsa100.sb7.com/site/?page=ADMIN_MEETINGS

Service Appliance Conference Administration

Click on the Details tab and if you select **Subject** you can see that the information that was entered into the CSR is present.

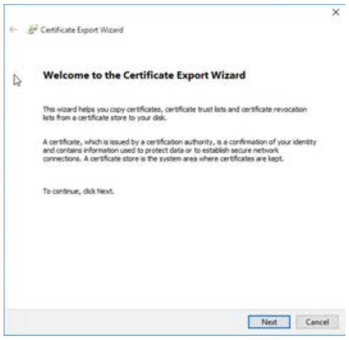


Show: <All>

Field	Value
Serial number	56 f9 6f 7e
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	S87-vSA100.S87.COM, slopez...
Valid from	Monday, March 28, 2016 10:5...
Valid to	Thursday, March 26, 2026 10:...
Subject	S87-vSA100.S87.COM, slopez...
Public key	RSA (2048 Bits)

CN = S87-vSA100.S87.COM
E = slopez@shroetel.com
OU = Technical Marketing
O = ShoreTel
L = Sunnyvale
S = California
C = US

Now click the **Copy to File…** button. A dialog will open Welcoming you to the Certificate Export Wizard, Click **Next**.



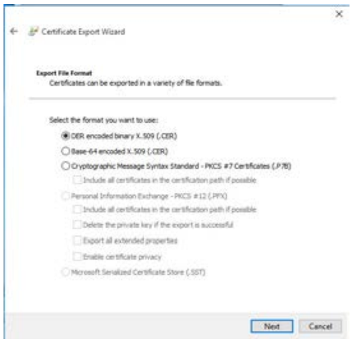
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Leave the default selection of *DER encoded binary x.509 (.cer)* and click **Next**.

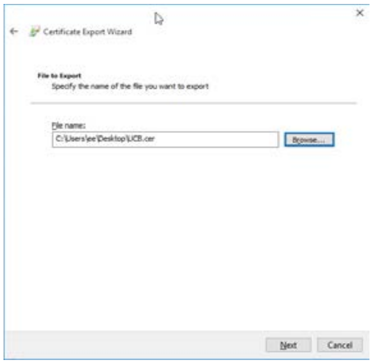


Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

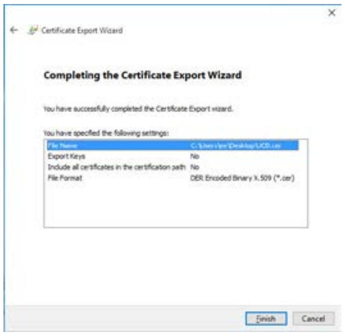
Browse and save the file you name and be sure to note the location presented in the **File Name:** box. Click **Next**.



File to Export
Specify the name of the file you want to export

File name: C:\Users\ee\Desktop\UCB.cer

Click **Finish** button on following screen.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\[illegible]\Desktop\UCD.cer
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

Certificates on Edge Gateway Router

Certificate Configuration

The Mitel Connect Edge Gateway solution uses the following certificates to secure communications between the Mitel Connect Edge Gateway and devices running Mitel Connect:

- Edge Gateway Certificate—Certificate used to access the administration portal of the Mitel Connect Edge Gateway.
- RAST Certificates—Certificate used to authenticate the secured connection between Remote IP phones and Mitel Connect Edge Gateway.
- Reverse Proxy Certificate—Certificate used to securely access the Mitel services via Reverse Proxy.
- TURN Certificate—Certificate used to securely use the TURN service from the Mitel Connect Edge Gateway.

You can generate certificates on the Mitel Connect Edge Gateway, import self-signed certificates, or individual/wildcard certificates from other certificate authorities.

Generating a Certificate

Use the Mitel Connect Edge Gateway administration portal to perform the following procedures. There are four certificates that establish secure sessions with the Mitel Connect Edge Gateway. In addition, these certificates establish mutually authenticated secure remote connections when the clients are outside of the enterprise.

The Mitel Connect Edge Gateway presents different certificates when a client initiates a

connection from local or remote interfaces.

1. Launch Mitel Connect Director.
2. Click Administration > Appliances/Servers > Platform Equipment.
3. Click the Name of the Edge Gateway from the list pane to launch the Mitel Connect Edge Gateway administration portal.
4. Select Configuration > System > Certificate.
5. Select Edge Gateway, RAST, Reverse Proxy, or TURN as needed.
6. Click Generate. The Generate Certificate page opens.
7. In the Country Name field, type the two-letter country code for the country where the Mitel Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located.
8. In the State or Province field, type the state or province where the Mitel Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located.
9. In the Locality field, type the locality where the Mitel Connect Edge Gateway, RAST, Reverse Proxy, or TURN is located. Typically, this is the name of a city.
10. In the Organization field, type the name of the organization. Typically, this is the name of the company.
11. In the Organization Unit field, type the name of the organization unit (for example, enter the name of a department within the organization).
12. In the Common Name field, type the domain name for the Mitel Connect Edge Gateway, RAST, Reverse Proxy, or TURN.
13. In the Key Length (bits) field, select the required key length from the drop-down list.
14. In the Subject Alternative Names field, select the alternative names for the Mitel Connect Edge Gateway, RAST, Reverse Proxy, or TURN.
15. In the Other Alternative Names field, select Alternative IP Address or DNS from the drop-down list. Enter the IP Address or domain name and click Add.

16. Click Generate. It displays a confirmation message to restart the Edge Gateway.
17. To generate the certificate, click OK.
18. Click Close to close the certificate window.
19. A restart prompt displays. Do one of the following:
    - Click **OK** to restart the service and activate the newly generated certificate.
    - If you do not want to restart, click **Cancel**. The newly generated certificate will be activated on next restart.

Certificates on Mobility Router

Certificate Authority

The certificate authority (CA) in the Mitel Connect Mobility Router is used to sign certificates
generated by the Mitel Connect Mobility Router. The Mitel Connect Mobility Router generates
and signs a client certificate for every client that is provisioned. The Mitel Connect Mobility Router
can also generate and sign the Mitel Connect Mobility Router certificates if you choose to use a
generated certificate instead of an imported certificate.

You must either generate or import a CA because there is no preinstalled factory-default CA. Without a
generated or imported CA, users cannot be provisioned, and Mitel Connect Mobility Router
certificates cannot be generated.

Generating a Certificate Authority

To generate a certificate authority:

1. Click **Configuration > System > Certificate > Certificate Authority**. The **Certificate Authority** page displays.
2. Click **Generate**. The **Generate Certificate** page displays.
3. In the **Country Name** field, type the two-letter country code for the country where the Mitel Connect Mobility Router is located. The default is US.
4. In the **State or Province**, field, type the state or province where the Mitel Connect Mobility Router is located.
5. In the **Locality** field, type the locality where the Mitel Connect Mobility Router is located.

Typically, this is the name of a city.

6. In the **Organization** field, type the name of the organization. Typically, this is the name of the company.
7. In the **Organization Unit** field, type the name of the organization unit (or example, enter the name of a department within the organization).
8. In the **Common Name** field, type the domain name for the Mitel Connect Mobility Router. The default value is the domain name on the Express Setup page and can be changed as needed.
9. Click **Generate**. A warning message displays:

    GENERATING CLIENT CERTIFICATE AUTHORITY CERTIFICATE INVALIDATES PROVISIONING STATUS
    OF EXISTING CLIENT APPLICATIONS. ALL PROVISIONED CLIENTS WILL STOP WORKING UNTIL
    THEY ARE RE-PROVISIONED. GENERATE THE CERTIFICATE?

10. To generate the certificate, click OK.
11. Click Close to close the certificate window.
12. A restart prompt displays. Do one of the following:
    - Click **OK** to restart the Mitel mobility service and activate the newly generated certificate.
    - □If you do not want to restart the Mitel Connect Mobility Router, click **Cancel**. The newly generated certificate will be activated on next restart.

Importing a Certificate Authority

You can import a Certificate Authority (CA) certificate to the Mitel Connect Mobility Router.

To import a certificate authority:

1. Click **Configuration > System > Certificate > Certificate Authority**. The **Certificate Authority** page displays.
2. Click **Import**. The **Import Certificate** page displays.
3. Paste the certificate and private text key into the text box on the **Import Certificate** page.
4. Click **Import**. A warning message displays as follows:

```
Warning: Importing Certificate Authority certificate invalidates provisioning status
of existing client applications. All provisioned clients will stop working until
```

```
they are re-provisioned. Press OK if you want to import the certificate. Press
Cancel otherwise.
```

If the certificate is valid, a Restart prompt displays. If the certificate is not valid, an Error prompt displays. In the case of an error, generate a valid certificate or obtain a new certificate to paste in the field.

5. Restart the Mitel mobility service and activate the newly generated certificate, click **OK**.

The Last Generated Date field updates to the current date and time. Verify the certificate was created correctly by checking the status line at the top of the certificate.

Mitel Connect Mobility Router Certificates

There are four Mitel Connect Mobility Router certificates which establish secure sessions during client provisioning and create HTTPS sessions to the Mitel Connect Mobility Router. In addition, these certificates establish mutually authenticated secure remote connections when the clients are outside of the enterprise.

The Mitel Connect Mobility Router presents different certificates when a client initiates a connection from local or remote interfaces.

Generate a Mitel Connect Mobility Router virtual certificate only if you are creating a redundancy cluster to provide stateful high availability for the Mitel mobility solution. This is the certificate used by the virtual IP address that manages the redundancy cluster. When the Mitel Connect Mobility Router runs in redundancy mode, both nodes must use the same virtual certificates.

The following local, remote, and virtual certificates are supported:

- **Local Access**—internal connections over the LAN interface in a standalone configuration inside the enterprise.
- **Remote Access**—connections using Secure Remote Access with Mitel Connects in standalone configuration.
- **Local Access (Virtual)**—internal connections over the LAN interface in cluster configurations inside the enterprise, and synced across all cluster nodes.
- **Remote Access (Virtual)**—connections using Secure Remote Access with Mitel Connects in cluster configurations.

Locally Generated Certificates

You can create a locally generated certificate on the Mitel Connect Mobility Router. This is a convenient option for enterprises that have not already purchased a certificate. The certificate is signed by the certificate authority on the Mitel Connect Mobility Router.

Certificate Signing Request

Administrators can generate a Certificate Signing Request (CSR) for all Mitel Connect Mobility Router Certificates. The Mitel Connect Mobility Router stores only one set of CSRs and corresponding private keys per type of certificate, and automatically syncs them to the standby node, if applicable.

Generating a Mitel Connect Mobility Router Certificate

The Mitel Connect Mobility Router Certificate page displays the date and time that the last certificate was generated.

1. Click **Configuration > System > Certificate > Mobility Router**.
   a. If you are running a Mitel Connect Mobility Router in a standalone environment, select **Standalone** to generate a Local Access or Remote Access certificate
   or
   b. If you are running a Mitel Connect Mobility Router in a clustered configuration, select **Clustered** to generate a Local Access or Remote Access certificate.
2. Click **Generate**. If the remote access configuration does not match the certificate, a warning message displays as follows:
   ```
   Warning: Certificate Subject CN <> does not match Remote Access configuration <>.
   ```
3. In the Country Name field, type the two-letter country code for the country where the Mitel Connect Mobility Router is located. The default is US.

4. In the State or Province, field, type the state or province where the Mitel Connect Mobility Router is located.
5. In the **Locality** field, type the locality where the Mitel Connect Mobility Router is located. Typically, this is the name of a city.
6. In the **Organization** field, type the name of the organization. Typically, this is the name of the company.
7. In the **Organization Unit** field, type the name of the organization unit (for example, enter the name of a department within the organization).
8. In the **Common Name** field, type the FQDN, hostname or IP Address for the Mitel Connect Mobility Router.
9. Select the strength of the private key from the **Key Length** pulldown menu. The longer the number, the stronger the security of the key. The default is 1024.
10. Select any combination of the default **Alternative Names** displayed, or add your own by entering it in the **Other Alternative Names** field. (Click **Add** if entering an address in this field.) These additional addresses will be added to the locally generated certificate or CSR, and display in the **Subject Alternative Names** field as they are selected.
11. Click **Generate** to generate a certificate signed by the certificate authority installed on the Mitel Connect Mobility Router, or click Generate CSR to generate a certificate signing request (CSR) to be sent to a third-party certificate signing authority.
12. If generating a CSR in the previous step, submit the CSR to a trusted certificate signing authority and save the RSA private key.
13. If a restart prompt displays, do one of the following:
    - Click **OK** to restart the Mitel mobility service and activate the newly generated certificate.
    - If you do not want to restart the server, click **Cancel**. The newly generated certificate will not take effect until the next restart.
14. Refresh the browser to regain access, then log in.

Importing a Certificate to the Mitel Connect Mobility Router

You can also import a purchased or self-signed certificate for any of the four Mitel Connect Mobility Router certificates. For example, if you purchased a certificate from VeriSign, that certificate can be imported and used by the Mitel Connect Mobility Router.

1. Click **Configuration > System > Certificate > Mobility Router.**
   a. If you are running a Mitel Connect Mobility Router in a standalone environment, select **Standalone** or
   b. If you are running a Mitel Connect Mobility Router in a clustered configuration, select **Clustered**.
2. Click **Import**. The Import Certificate window displays.
3. **Paste** the Mitel Connect Mobility Router certificate issued by the trusted certificate authority, RSA private key, and the intermediate and root certificates you may have received from the certificate signing authority. Be sure to include both “BEGIN” and “END” statements for all information in the following order:
    - Mitel Connect Mobility Router signed certificate
    - RSA private key
    - Any certificate chain/bundle that may have been included from the certificate authority.

Questions and Answers

Q: Will the Connect client display as secure ‘Locked’?

A: Yes. The lock on the Connect client will be enabled and green as long as the certificate name and details matches the URL FQDN.

Q: Can we use the same wildcard certificate that we use for our business to secure our Mitel Connect VoIP communications?

A: Yes. The use of wildcard certificates is supported.

Q: Can we avoid the cost of certificates by creating self-signed certificates on all Mitel servers?

A: This is not recommended for a production system. In the case of a lab environment then a self-signed certificate can be used.

Conclusion

Mitel Connect OnSite security features are an integral part of the UC solution structure. Secure IP communications are no longer a 'feature' but are now a necessity. Third party SSL certificates are strongly suggested for all Mitel UC communications. It is not recommended to use self-signed certificates in a production environment.

Additional Resources

For more information about security in Mitel Connect, see the "Security" chapter of the Mitel Connect System Administration Guide. Excerpts were taken from the Mitel Connect Mobility Router and Mitel Connect Edge Gateway Admin guides for reference.
You might find the following resources helpful for working with certificates:

Mitel Connect System Administration Guide
https://support.shoretel.com/kb/view.php?id=kA41A000000LiMqSAK

Digicert's page for creating a certificate signing request:
https://www.digicert.com/csr-creation.htm

The XCA tool for managing certificates:
http://sourceforge.net/projects/xca/

Version	Date	Contributor	Content
1.0	June 2017	S. LOPEZ	Original App Note
1.1	September 2017	S. LOPEZ	Revised for branding