Application Note - AN16036

MT App Note 16036 (AN 16036)
May, 2018

Mitel MiVoice Connect Security Certificates

Description: This Application Note describes the use of security certificates in Mitel MiVoice Connect.

Environment:
Mitel MiVoice Connect

Target Audience:
Mitel Partners
Mitel Partner Sales Engineers
Mitel Sales Engineers
Mitel MiVoice Connect customers

Security certificates are a component of a Windows Server system which enables an encrypted connection between the server and a client application. Using security certificates with MiVoice Connect provides a secure and encrypted path for data to flow between the end user's Connect system and the Connect desktop application.

This Application Note describes how security certificates are used in the Mitel MiVoice Connect system, and how they are created and installed.

Note that the use of SSL security certificates also applies to the MiCloud Connect system. This functionality is controlled by the Mitel host systems and is automatically installed with the Mitel Connect desktop application.

Contents

Introduction

The topic of computer systems security and cryptography is large and complicated. This document does not intend to thoroughly address all aspects of digital security and security certificates. This document gives some of the basic concepts of security certificates and how they are used with the Mitel MiVoice Connect system.

Administrators are encouraged to consult computer security professionals for more complete information regarding these topics, and the ramifications and risks with the Mitel Connect system.

What is a Security Certificate?

Security certificates are data files that which contain information about the organization that owns the certificate and special “keys” that are used for encryption. The certificate is digitally signed by the issuer of the certificate. This information is used by application systems to validate and then create an encrypted data connection.

When security certificates are installed on a server, it enables the system to communicate securely. The Secure Sockets Layer (SSL) protocol is used for many applications, such as Mitel Connect. SSL certificates contain a domain name, subdomain name, or hostname, and an organizational identity (i.e. company name) and location. This information, along with the certificate key and digital signature provided by the Certificate Authority, is used to establish the secure connection.

Certificates ensure that data communications between systems and clients are secure within the company network (behind the corporate firewall) and are also secure over the public Internet. All data communications are trustworthy, encrypted, and secure.

When SSL certificates are utilized, network traffic changes from HTTP application protocol to HTTPS. Various applications and browsers will indicate when a secure connection has been established. The Mitel Connect desktop client displays a “lock” icon when a secure connection has been established.

Security certificates can be obtained either by purchase from an authorized public certificate vendor, or can be generated by the organization itself. A public certificate vendor (such as Symantac, GoDaddy, GlobalSign, DigiCert, etc.) is also called a Certificate Authority. Trusted security certificates can be purchased from a Certificate Authority and then used with the client / server system.

A security certificate that is generated and provided by the organization itself is called a “self-signed” certificate. There is no cost associated with self-signed certificates, which is what makes them attractive. However self-signed certificates are also not “trusted” by an authorized independent Certificate Authority. **Mitel Connect does not support self-signed certificates for secure connections.** See Support of Self-signed Certificates below for information on using self-signed certificates with Mitel Connect.

Support of Self-signed Certificates

Mitel Connect provides data encryption for all end-user communication, including all protocols for the Mitel 400-series phones and the Connect desktop client. To ensure secure client access (HTTPS) and avoid warning messages, **a custom security certificate, purchased from a public certificate vendor, must be installed**. This is the only method that ensures that the Connect client is secure.

The Connect client falls back to HTTP if certificates are not installed. Secure connections require that trusted certificates are installed on all platforms where the client connects. If a secure connection is not a desired, the default certificates that are created during installation can be used. These certificates are signed by the UC Certificate Authority.

Consult the “Setting Up Security Parameters” chapter of the *MiVoice Connect System Administration Guide* for more information.

Obtaining a purchased Security Certificate

In order to purchase a security certificate from a Certificate Authority, a Certificate Signing Request (CSR) must be generated. The CSR is a small data file which contains coded information about the company or organization. For MiVoice Connect, a CSR is created using Director. See Generating the Certificate Signing Request (CSR) below.

Once the CSR has been created, the desired type of certificate must be determined. Most Certificate Authority vendors offer many certificate options. In general, certificates can cover a single domain, or multiple domains and subdomains. The cost and options vary per vendor. The organization administrator must determine scope of the desired validation for the certificate.

Domain Validation

This is the lowest cost security certificate. The certificate validates the one domain only. The certificate is obtained by simply verifying ownership of the domain. These certificates are issued almost immediately.

Organization Validation

Organization certificate require slightly more verification, at additional cost, resulting in more credibility. For websites, an organizational SSL certificate will display the browser padlock and use HTTPS.

Extended Validation

An Extended Validation certificate is the latest type of SSL technology and is incorporated into many high security browsers. Browsers will display a green address bar, the legally incorporated company name, the browser padlock, and use HTTPS. For application systems such as Mitel Connect, an Extended Validation certificate provides additional credibility.

Wildcard Validation

Wildcard certificates allow a single certificate to be used on an unlimited number of subdomains and across an unlimited number of servers. The cost of the certificate typically covers additional subdomains or servers that are added in the future. Wildcard certificates are frequently used for application systems such as Mitel Connect.

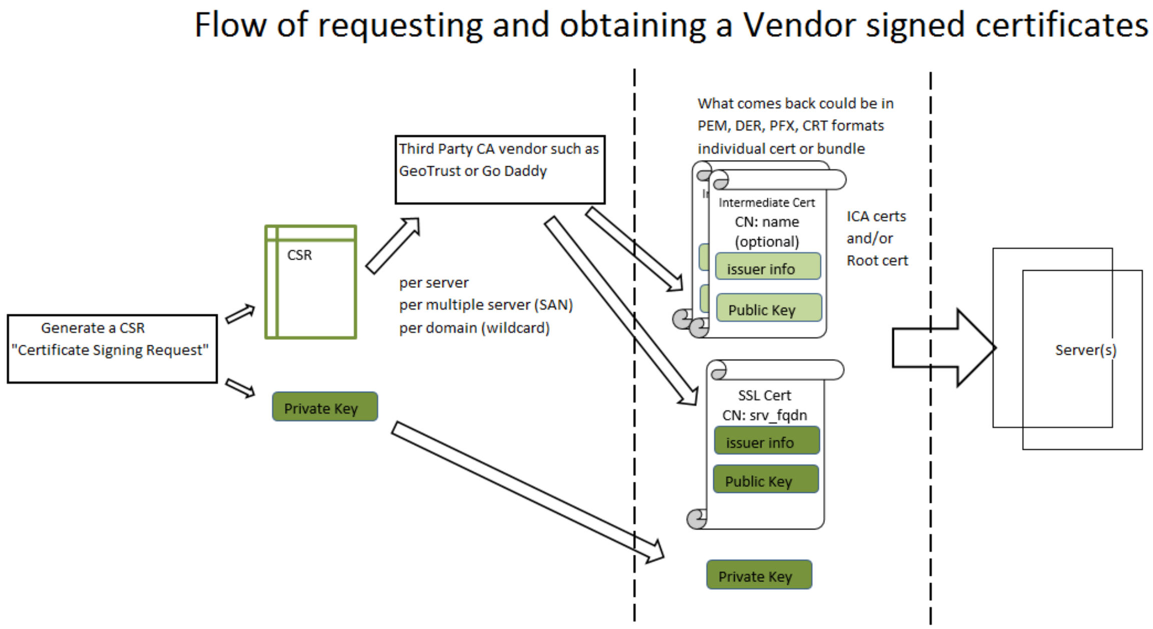

Flow of requesting and obtaining a Vendor signed certificates
Generate a CSR
"Certificate Signing Request"
CSR
Private Key
Third Party CA vendor such as GeoTrust or Go Daddy
per server
per multiple server (SAN)
per domain (wildcard)
What comes back could be in PEM, DER, PFX, CRT formats individual cert or bundle
Intermediate Cert
CN: name
(optional)
issuer info
Public Key
ICA certs
and/or
Root cert
SSL Cert
CN: srv_fqdn
issuer info
Public Key
Private Key
Server(s)

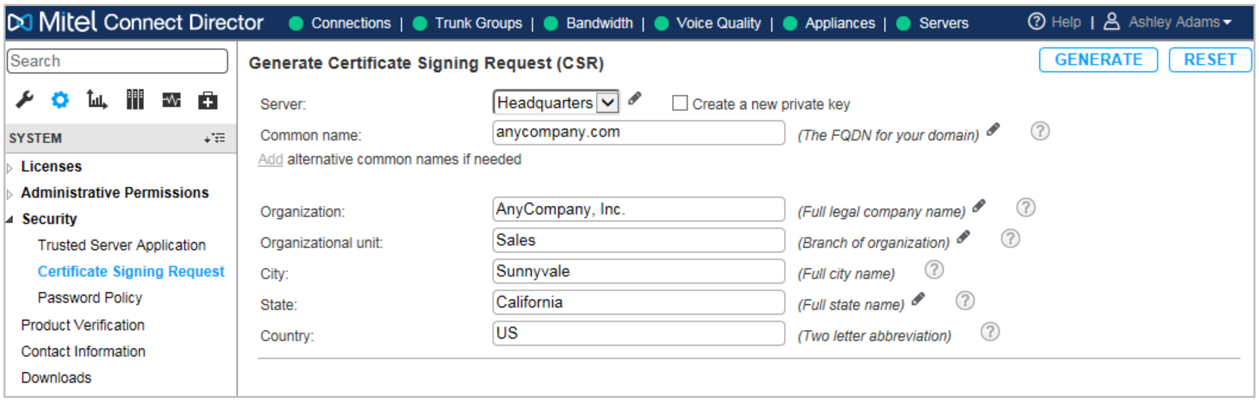
Figure 1 - Process flow for obtaining a security certificate

Generating the Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is submitted when purchasing a security certificate from a Certificate Authority vendor. For MiVoice Connect, the CSR is generated using Director.

In Director, navigate to System > Security > Certificate Signing Request. Complete all fields on the page.

For complete information on the contents of each field and the full procedure for generating the CSR, consult the “Generating a Certificate Signing Request” section of the *MiVoice Connect System Administration Guide*.


Mitel Connect Director
Connections | Trunk Groups | Bandwidth | Voice Quality | Appliances | Servers
Help | Ashley Adams
Search
SYSTEM
Licenses
Administrative Permissions
Security
Trusted Server Application
Certificate Signing Request
Password Policy
Product Verification
Contact Information
Downloads
GENERATE
RESET

Generate Certificate Signing Request (CSR)

Server: Headquarters ☐ Create a new private key

Common name: anycompany.com (The FQDN for your domain)

Add alternative common names if needed

Organization: AnyCompany, Inc. (Full legal company name)

Organizational unit: Sales (Branch of organization)

City: Sunnyvale (Full city name)

State: California (Full state name)

Country: US (Two letter abbreviation)

Figure 2 - Process flow for obtaining a security certificate

Create a “staging” folder (for example, <drive>:\CertStaging), and save the following text files:

- Copy and paste the generated CSR into a text file (for example, server01.csr), and save the file in the staging folder.
- If generated, copy and paste the generated private key into a text file (for example, server01.key), and save the file in the staging folder. Retain the private key for local use. Do not share it with the vendor.

Send the Certificate Signing Request file to the desired Certificate Authority vendor to purchase the SSL certificate. Usually this file is uploaded to the vendor when the order is placed.

When the SSL certificate files are received from the CA vendor, they will be “imported” to the HQ server and any DVS appliances, along with the private key file saved earlier.

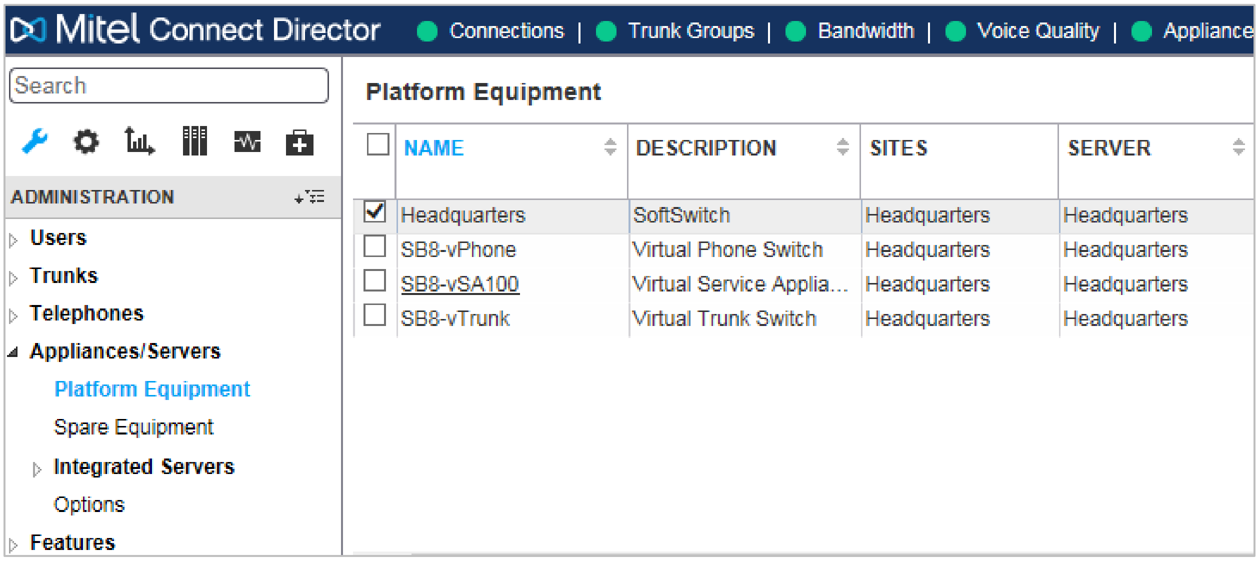
Installing / Importing the Certificate

After the receiving the purchased SSL certificate(s), and any intermediate CA certificates, the files are saved and then “imported” to the Connect HQ server and any DVS appliance. This process is performed using Connect Director.

The following are general guidelines for importing the certificates. For the most complete and up to date installation procedures, please consult the “Importing a Certificate for Headquarters and DVSs” section of the *MiVoice Connect System Administration Guide*.

Save the received SSL certificates to the “staging” folder that was created when the CSR was generated (see above).

In Connect Director, navigate to Administration > Appliances/Servers > Platform Equipment. Click the device where the certificate is to be installed. The device details are displayed.

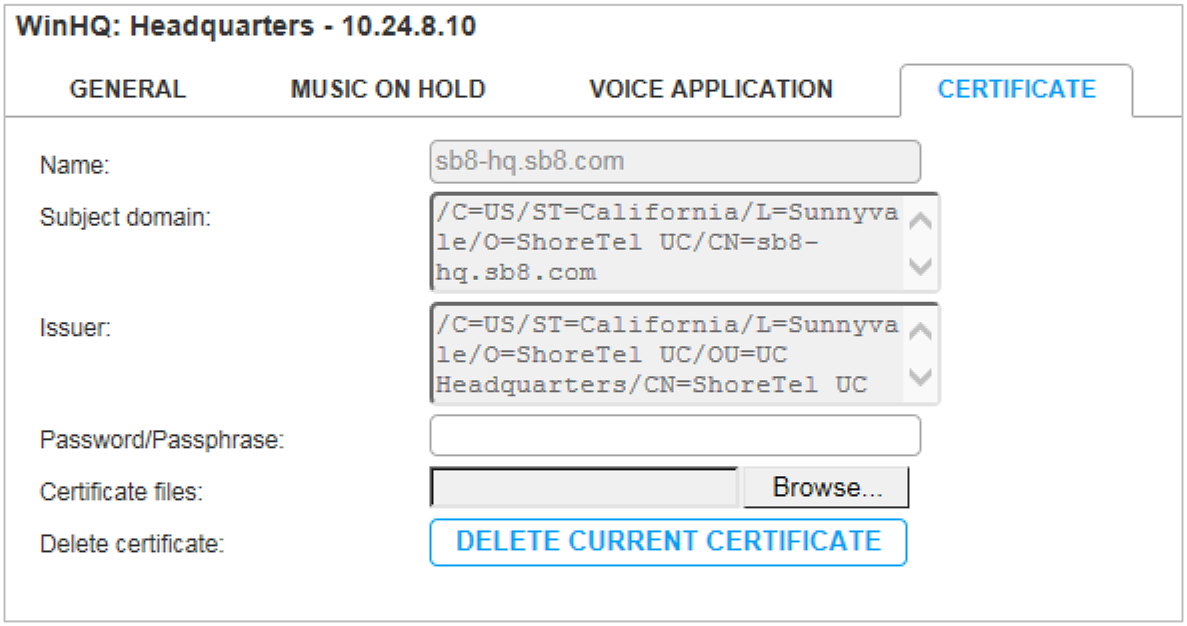


Platform Equipment

□	NAME	DESCRIPTION	SITES	SERVER
☑	Headquarters	SoftSwitch	Headquarters	Headquarters
□	SB8-vPhone	Virtual Phone Switch	Headquarters	Headquarters
□	SB8-vSA100	Virtual Service Applia...	Headquarters	Headquarters
□	SB8-vTrunk	Virtual Trunk Switch	Headquarters	Headquarters

Figure 3 - Platform Equipment

Click the “Certificate” tab on the details pane. The details for the currently installed Mitel self-signed certificate (or any previously imported certificate) are displayed. The name of the currently installed certificate (FQDN name) should be identical to the Common name of the certificate to be imported.



WinHQ: Headquarters - 10.24.8.10

Name: sb8-hq.sb8.com

Subject domain: /C=US/ST=California/L=Sunnyvale/O=ShoreTel UC/CN=sb8-hq.sb8.com

Issuer: /C=US/ST=California/L=Sunnyvale/O=ShoreTel UC/OU=UC Headquarters/CN=ShoreTel UC

Password/Passphrase:

Certificate files:

Delete certificate:

Figure 4 - Certificate details

Delete the currently installed certificate before importing the new certificate. Click “Delete Current Certificate”.

Enter the new certificate’s password, if supplied.

Import the certificate and any other relevant files by clicking “Choose Files” or “Browse”. Navigate to the previously created staging folder. Select all the files provided by the Certificate Authority vendor, including the SSL certificate, any intermediate CA certificates, and the private key file if one was created when the CSR was generated.

Connect Director validates the uploaded files. After the import is complete, refresh the browser to view the new “Issuer” information.

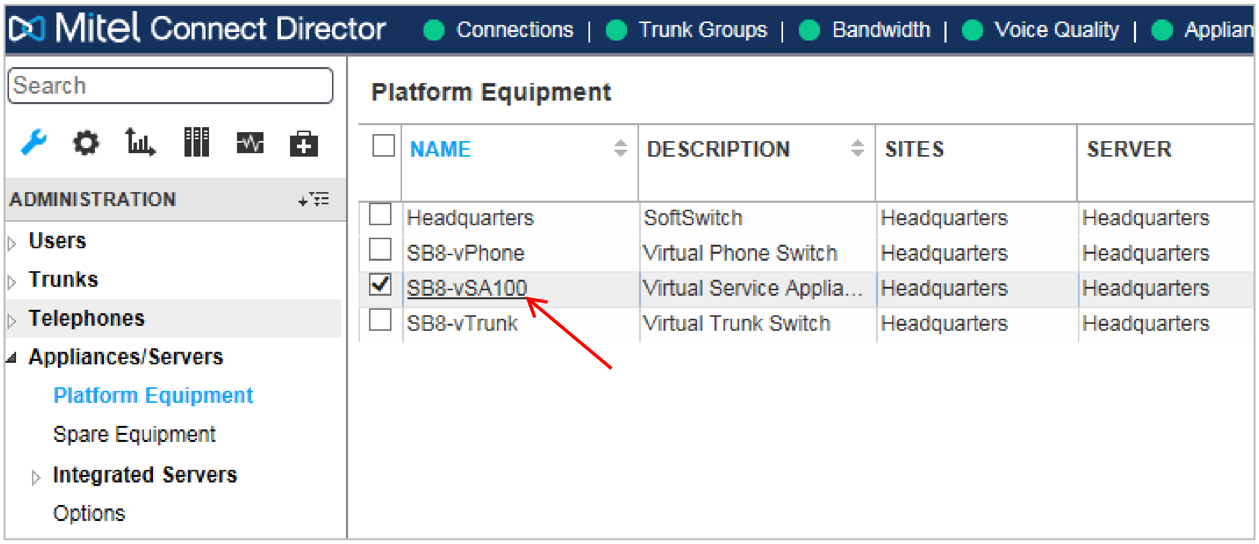
Click “Save” to install the certificate on the HQ server or appliance.

Once the security certificate has been received and installed, the Mitel Connect desktop application will indicate the status of the secure connection by displaying a “locked” padlock icon. An “unlocked” icon indicates that the connection is not secure and that there may be problems with the certificate.

Certificates for the SA-100/400 Service Appliance

In order to provide secure communications throughout the Mitel Connect platform, security certificates must be used on the main HQ server, and on all DVS appliances, including the SA-100/400 Service Appliance. The SSL certificates are similar to those installed on the HQ server; however the CSR must be generated and installed separately.

The SA-100/400 Service Appliance has a separate administration web page, which can be accessed from Connect Director. In Director, navigate to Administration > Appliances/Servers > Platform Equipment. Click the underlined link of the name of the SA-100 device.

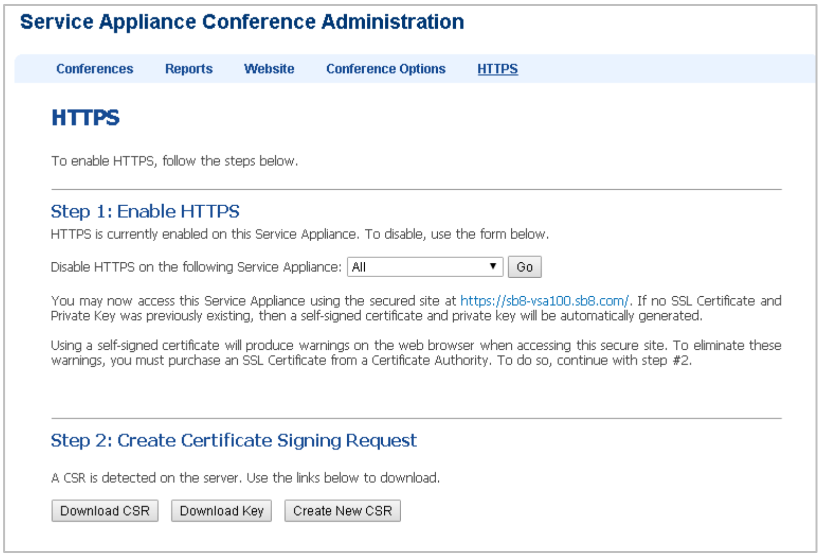


Platform Equipment

☐	NAME	DESCRIPTION	SITES	SERVER
☐	Headquarters	SoftSwitch	Headquarters	Headquarters
☐	SB8-vPhone	Virtual Phone Switch	Headquarters	Headquarters
☑	SB8-vSA100	Virtual Service Applia...	Headquarters	Headquarters
☐	SB8-vTrunk	Virtual Trunk Switch	Headquarters	Headquarters

Figure 5 - SA-100 device administration URL

The SA-100 administration web page will open. Click the “HTTPS” tab.



Service Appliance Conference Administration

HTTPS

To enable HTTPS, follow the steps below.

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 ▾ Go

You may now access this Service Appliance using the secured site at https://sb8-vsa100.sb8.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.

Step 2: Create Certificate Signing Request

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

Download CSR | Download Key | Create New CSR

Figure 6 - SA-100 - HTTPS administration page

From the HTTPS page, a CSR can be generated and installed.

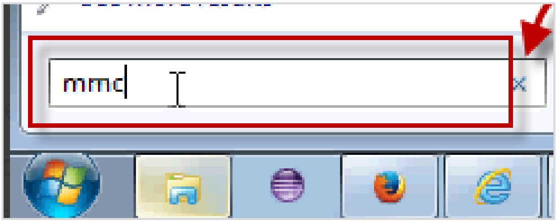
For complete information on certificate generation and installation, please consult the *Mitel Connect Conferencing and Instant Messaging Planning and Installation Guide* and App Note 16033 - *Security Certificates w/ SA100-SA400*.

Installing Security Certificates on End User Systems

Depending on the type of Security Certificate that is installed, especially when self-signed certificates are used, a similar certificate must be installed on the end user's computer system in order for the Connect desktop application to establish a secure HTTPS connection. This process is generally not needed if an SSL certificate is obtained from a trusted Certificate Authority.

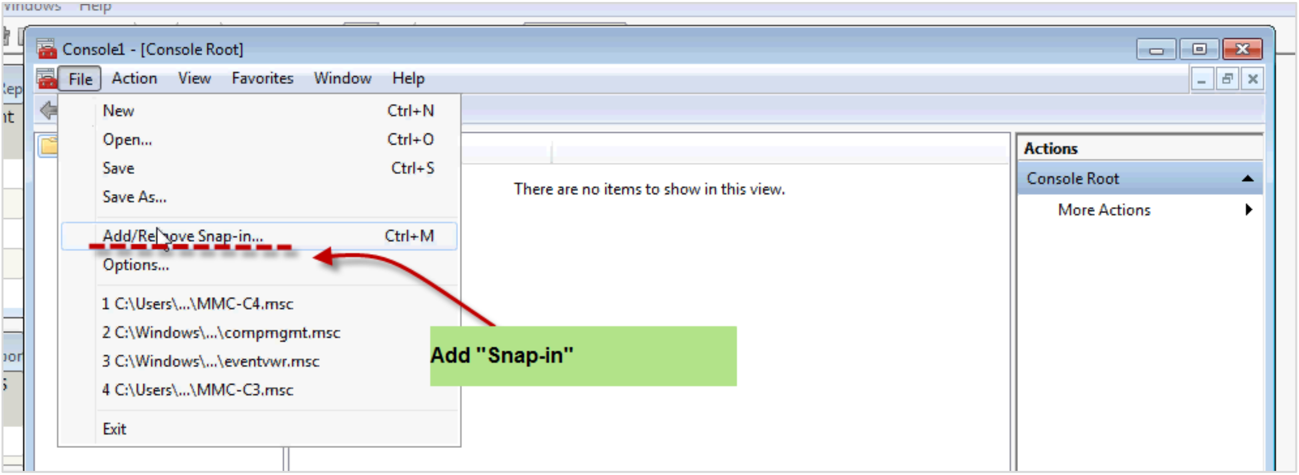
The following example is for installing a certificate on a Windows PC. Installation on a Mac system is similar.

Run the Microsoft Management Console applet by going to the start button or search and type in "MMC"



mmc

Click on "File", and then click "Add/Remove Snap-in".

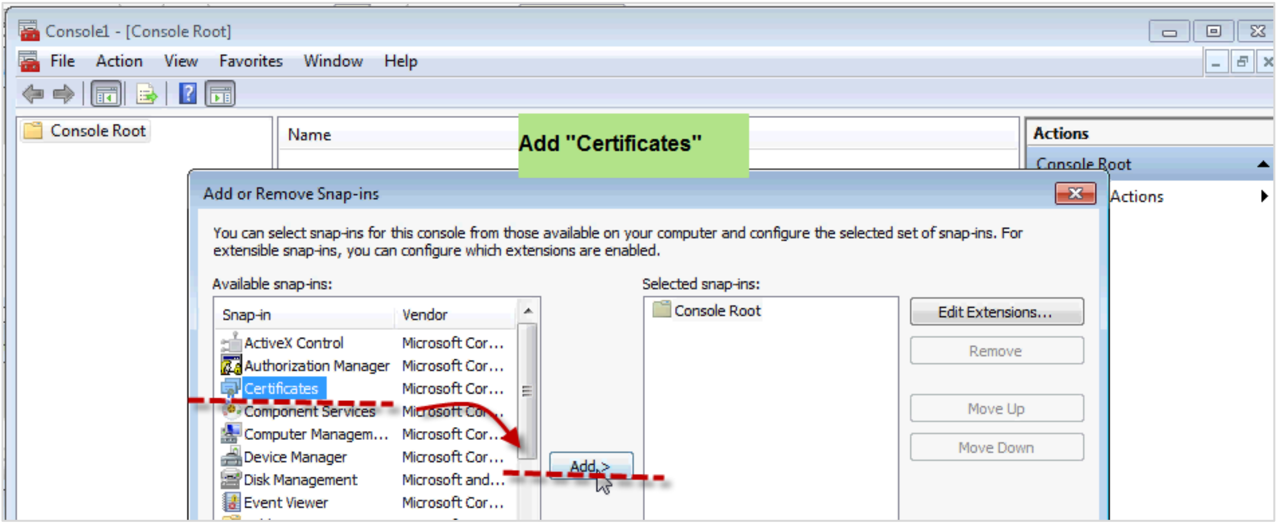


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Users\...\MMC-C4.msc
2 C:\Windows\...\compmgmt.msc
3 C:\Windows\...\eventvwr.msc
4 C:\Users\...\MMC-C3.msc
Exit
Actions
Console Root
More Actions

There are no items to show in this view.

Add "Snap-in"

Click “Certificates”, and then click “Add”.



Add "Certificates"

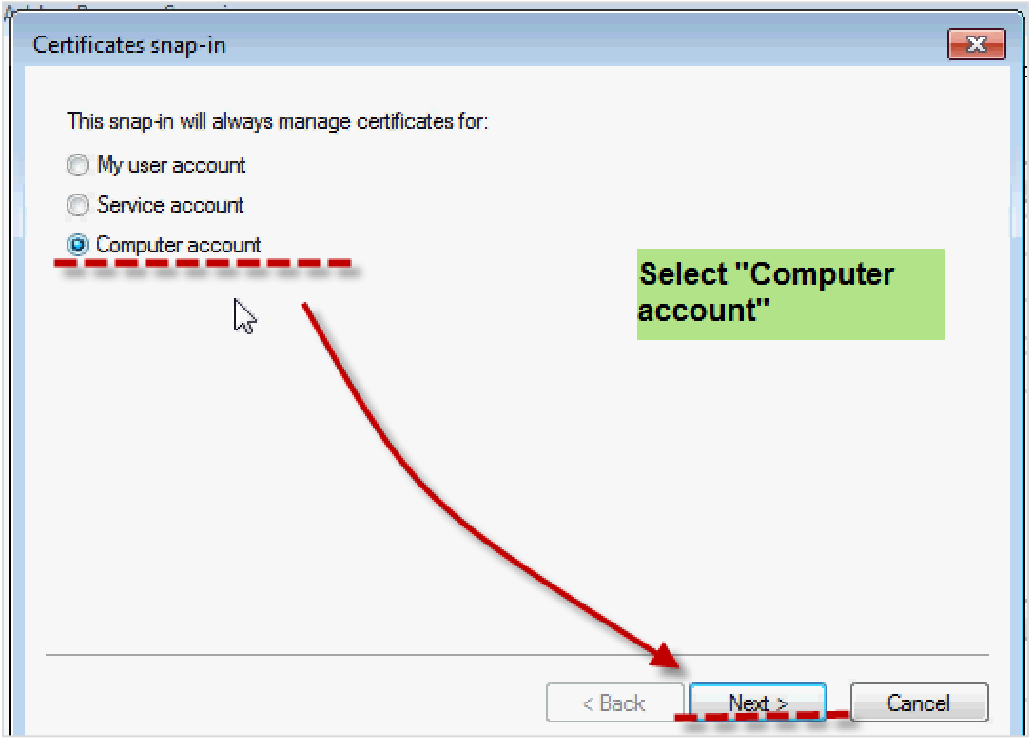
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...

Selected snap-ins:

If prompted, click “Computer Account”, and then click “Next”.

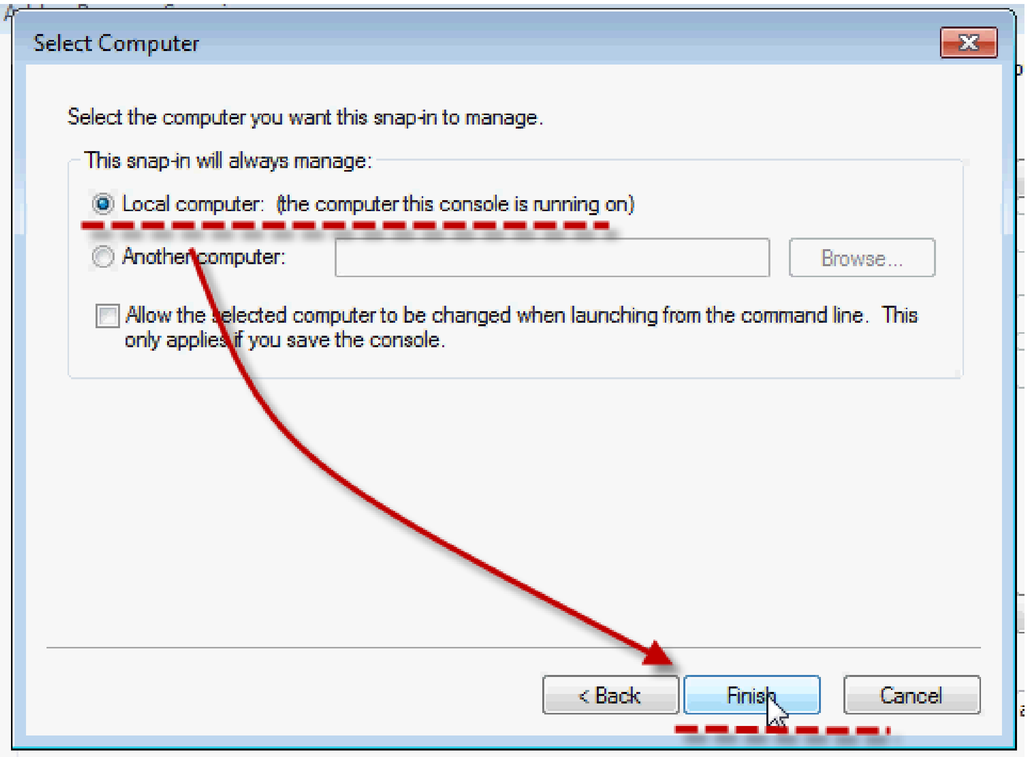


This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Select "Computer account"

Click “Local Computer” and then click “Finish”.



Select Computer

Select the computer you want this snap-in to manage.

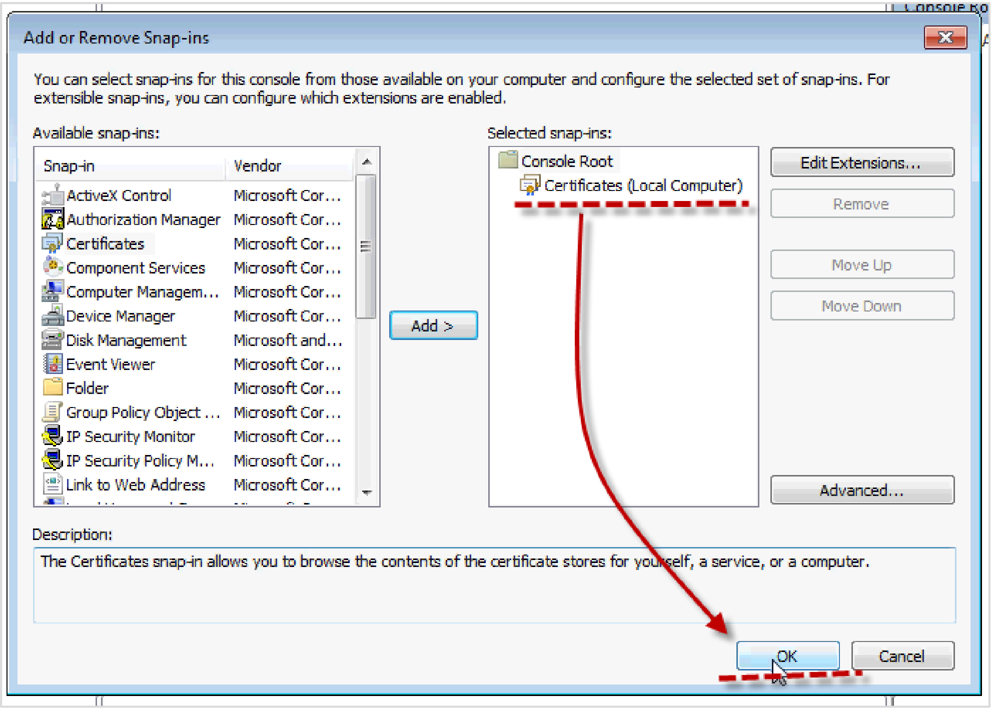
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Click “OK”.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

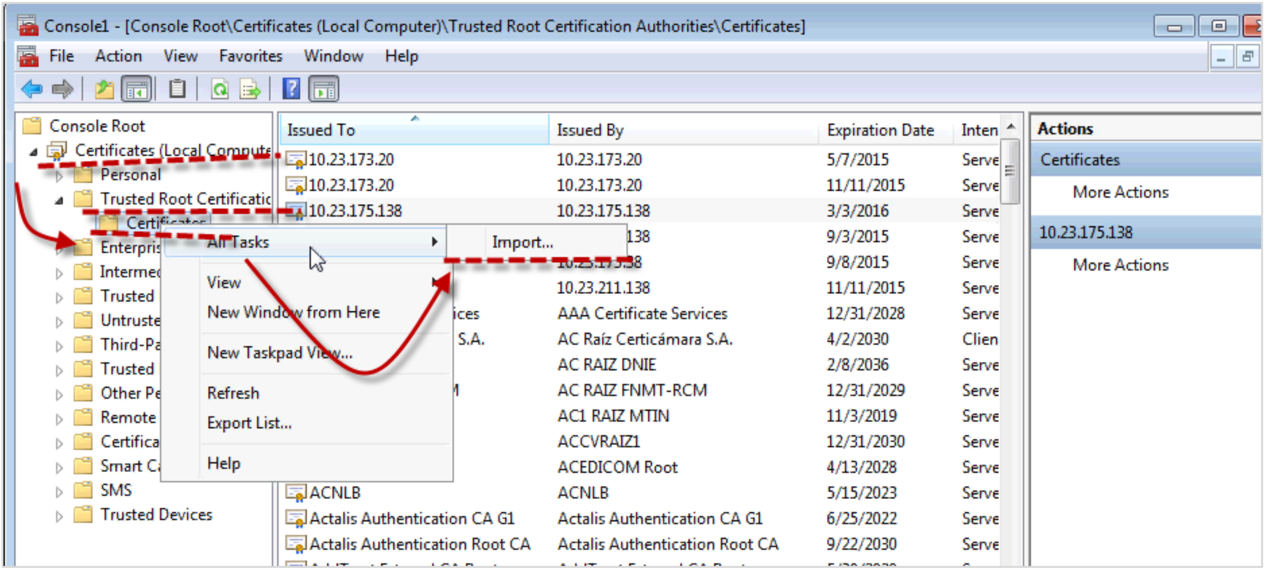
Console Root
Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Click and expand “Certificates (Local Computer)”.

Right-click on “Trusted Root Certification Authorities”, then select “All Tasks”, and then “Import”.



Issued To	Issued By	Expiration Date	Inten
10.23.173.20	10.23.173.20	5/7/2015	Serve
10.23.173.20	10.23.173.20	11/11/2015	Serve
10.23.175.138	10.23.175.138	3/3/2016	Serve
	138	9/3/2015	Serve
	10.23.173.38	9/8/2015	Serve
	10.23.211.138	11/11/2015	Serve
ices	AAA Certificate Services	12/31/2028	Serve
S.A.	AC Raíz Certicámara S.A.	4/2/2030	Clien
	AC RAIZ DNIE	2/8/2036	Serve
M	AC RAIZ FNMT-RCM	12/31/2029	Serve
	AC1 RAIZ MTIN	11/3/2019	Serve
	ACCVRAIZ1	12/31/2030	Serve
	ACEDICOM Root	4/13/2028	Serve
ACNLB	ACNLB	5/15/2023	Serve
Actalis Authentication CA G1	Actalis Authentication CA G1	6/25/2022	Serve
Actalis Authentication Root CA	Actalis Authentication Root CA	9/22/2030	Serve

Follow the Certificate Import Wizard to install the certificate. It may be necessary to restart the client PC to load the certificates into the environment.

Additional Resources

- MiVoice Connect System Administration Guide
- MiVoice Connect Build Notice
- MiVoice Connect Release Notes
- Mitel Connect Planning and Installation Guide
- Mitel Connect Conferencing and Instant Messaging Planning and Installation Guide

Version	Date	Contributor	Content
1.0	May, 2016	S. Lopez	Original App Note
1.1	September, 2017	S. Lopez	Rebranded to Mitel
2.0	May, 2018	W. Toigo	Revised and enhanced content and format, added disclaimer for self-signed certificates, replaced screen shots with Mitel branded images.