

Mitel Phone Manager Mobile Installation Guide

MAY 2020

DOCUMENT RELEASE 5.2

INSTALLATION GUIDE



Table of Contents

1.	Mobile Client Requirements	3
2.	Phone Manager Softphone	4-8
3.	Mobile Client Installation	9
4.	Remote/Teleworker Connections	10
4.1.	Connecting Through Firewalls	11
4.2.	MiVoice Border Gateway with Phone Manager Mobile	12
5.	SSL Certificate	13-15
6.	Index	16

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

Windows and Microsoft are trademarks of Microsoft Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

MiVoice Office Application Suite
Release 5.2 - May, 2020

®,™ Trademark of Mitel Networks Corporation
© Copyright 2020 Mitel Networks Corporation All rights reserved

1 Mobile Client Requirements

Phone Manager Mobile is available for both iOS and Android platforms.

We target making the App work on iPhone, Samsung Galaxy and Google Pixel devices.

As the Mobile client is released on a different schedule to Application Suite refer to the on-line Mobile Help for current Mobile version requirements on the following link

https://edocs.MitelAppSuite.com/pmmlatest/#Requirements_Mobile.html

2 Phone Manager Softphone

Phone Manager Desktop and Phone Manager Mobile both have Softphone capabilities that allow them to become an extension off the telephone system. They connect to the telephone system as a SIP extension. Both products use OAI features to add additional capabilities on top of the SIP features.

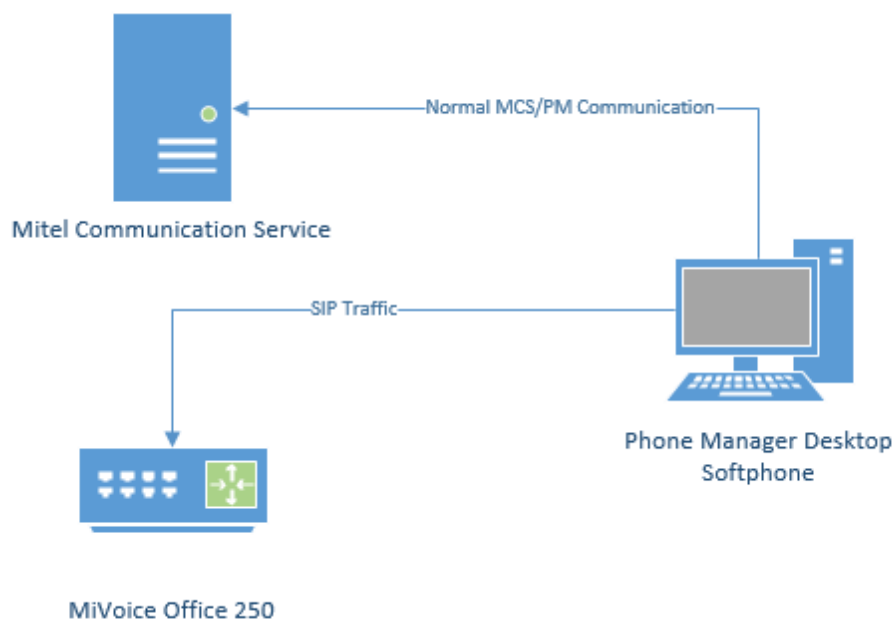
Requirements

The following requirements apply to any use of the Phone Manager Softphone:

- MiVoice Office 250 6.1 or higher (Release 6.3 SP1 or higher is recommended for automatic configuration of authentication details)
- Cat F licenses for each SIP extension on the telephone system Phone Manager will be connecting to
- Phone Manager Softphone Licenses for each Phone Manager Softphone that will be used

Phone Manager Desktop with Softphone

When Phone Manager Desktop connects as a softphone, the SIP traffic goes directly between the Phone Manager Client and the node on which the SIP extension is configured.



For information on connecting Phone Manager Desktop from outside the LAN, refer to the appropriate guide:

- Connecting Phone Manager Desktop using a [MiVoice Border Gateway](#)
- Connecting Phone Manager using a [Router](#)

Connecting from a Different Subnet

If the Phone Manager Desktop client is located on a different subnet to that of the MiVO 250 it is registering it with, the Auto NAT detection of Phone Manager Desktop can get confused and will use the client PC's public address to connect, not the local address. In this scenario, the softphone will get one way audio.

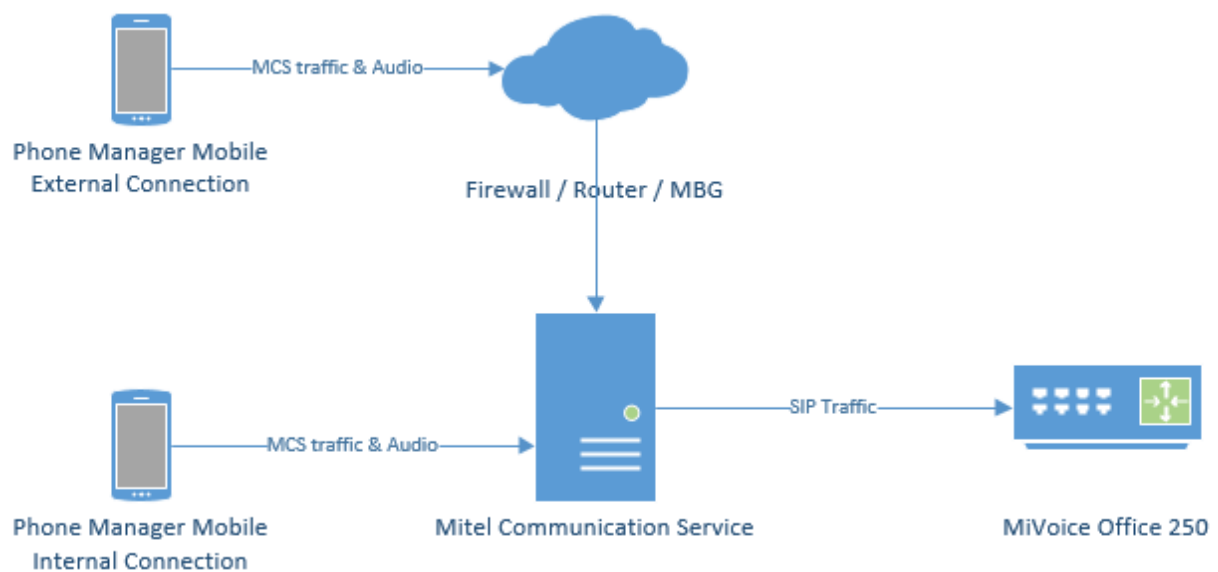
To work around this issue, Auto NAT Detection needs to be disabled on Phone Manager Desktop.

Phone Manager Mobile with Softphone

When using the Softphone features of Phone Manager Mobile the Mitel Communication Service acts as a proxy. The MCS SIP Proxy service manages all SIP extension registration and traffic on the behalf of the Phone Manager Mobile Softphone so that all SIP traffic is kept on the internal network and does not have to be exposed externally.

⚠ If the MCS SIP Proxy is restarted all the Phone Manager Mobile clients with a softphone need to reconnect the app to receive call notifications as they will no longer be registered. The easiest way to do this is by restarting the app on the mobile.

All audio connections for the Phone Manager Mobile Softphone are to the MCS SIP Proxy:



The MCS SIP Proxy requires G.711 to be configured against the SIP Endpoint on the telephone system as the audio encoding for making calls.

For information on connecting Phone Manager Mobile from outside the LAN, refer to the appropriate guide:

- Connecting Phone Manager Mobile using a [MiVoice Border Gateway](#)
- Connecting Phone Manager using a [Router](#)

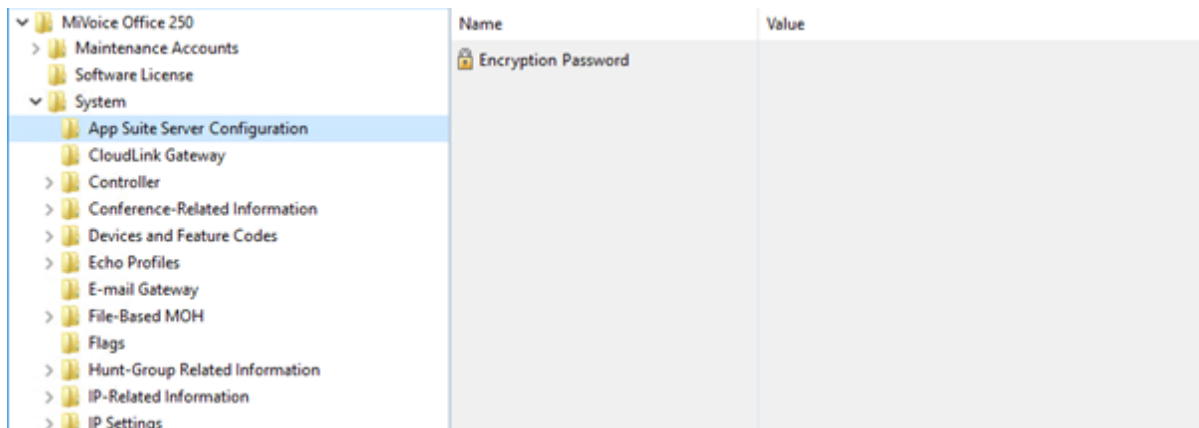
⚠ The SIP Proxy service must be on the same network as the PBX with no NAT in between the two.

The Softphone support within Phone Manager and the SIP connectivity of 6900 phones require some configuration to be performed within the PBX and with MiVoice Office Application Suite.

The configuration below applies to 6900 phones, SIP Hot Desk Devices, Phone Manager Desktop Softphone AND Phone Manager Mobile Softphone unless explicitly stated otherwise.

When using release 6.3 SP1 or higher of the MiVoice Office 250, MCS has the ability to query all SIP Authorization Credentials from the telephone system to use with Phone Manager Softphones and 6900 phones. This integration simplifies the process of installing Softphones/6900 phones and minimizes the risk of mis-configuration.

To support this feature, a new configuration section within MiVO 250 Database Programming has been created:




Encryption Password

On each node in the MiVO 250 network, an Encryption Password needs to be configured which will allow MCS to query and decrypt the SIP authorization credentials.

If the password is not configured, MCS will not be able to query the credentials from the PBX and they will have to be configured manually. See the [Device Configuration](#) section for more information.

Once the encryption password has been configured on the telephone system(s), it must also be configured in the [Nodes](#) section of the MCS configuration website.

 In addition to using requiring 6.3 SP1 or higher, CT Gateway release 5.0.64 or higher is also required for the SIP authorization credential query to work.

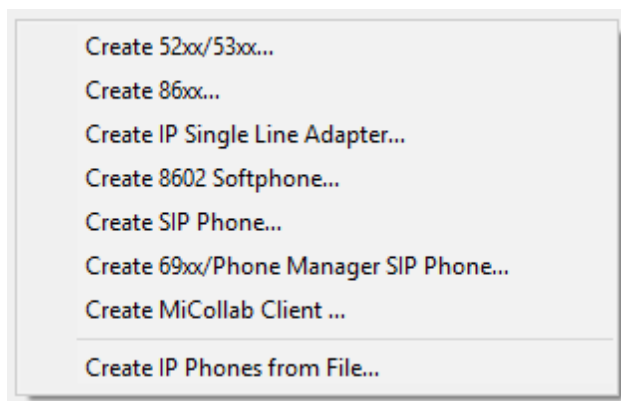
The MCS server needs to provide each 6900 phone and Phone Manager Softphone with the IP address of a SIP server to register with (the MiVoice Office 250). The IP address required will depend on which MiVoice Office 250 node the SIP extension is configured on and whether the phone is local or a teleworker.

For each node on the MiVoice Office 250 network that MCS is connected to, it is important to configure the IP address/port number to be used for SIP registrations.


For information on configuring the IP address(es)/Ports for each node, please refer to the [Node Configuration](#) section.

69xx SIP Phone


From release MiVO 250 6.3 onwards, a new SIP phone type called '69xx/Phone Manager SIP Phone' (renamed from '69xx SIP Phone' in 6.3 SP2) is available for creating SIP extensions on the telephone system for use with Phone Manager softphones & 6900 phones.




When SIP extensions are created using this type, the SIP Phone Groups created will automatically be configured with the required settings and will have a default inbound authentication applied with a randomly assigned password.

 If a user is using a 6900 handset and a softphone (on either or both of Phone Manager Desktop & Phone

Manager Mobile) it is important to set them up with separate SIP Endpoints on the phone system.

 For release prior to 6.3, the generic SIP Phone type should be used for Phone Manager Softphones. Please review the Phone Group settings under [Manual SIP Configuration](#) to check the required configuration.

 Remember that when connecting any SIP device to the MiVoice Office 250, the 'SIP UDP Listening Port' must be enabled in the 'Advanced IP Settings' section. Currently a reboot of the phone system is required after enabling this.

If 6.3 SP1 is not installed on the MiVoice Office 250 or for some reason the configuration of a SIP device needs to be performed manually, the details of all the settings required for a 69xx or Phone Manager Softphone are shown below.

SIP Phone Group


For each SIP Phone Group for SIP phones that are to be used as either Phone Manager Softphones, 6900 phones or SIP Hot Desk phones, the following configuration needs to be performed:

- Maximum Number of Calls = 3
- Enable in-bound authentication = Yes
- Configure in-bound authentication username = Extension number
- DTMF Payload = 101
- Camp-Ons Allowed = Yes
- Supports Ad Hoc Conferencing = Yes
- Use Registered Username (only required when connecting through an MBG)
- NAT Address Type = Native (even when connecting through an MBG)

Remember to repeat this process for each SIP extension.

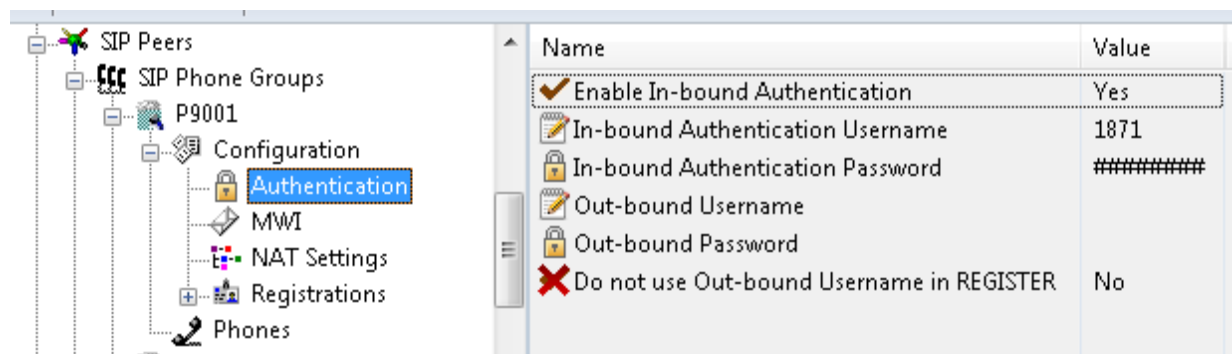
Manual Authentication Configuration

If a version prior to 6.3 SP1 is being used, the Inbound Authentication Credentials will need to be configured on both the telephone system and the MCS server.

 If release 6.3 SP1 or higher is being used, check the App Suite Server Configuration section below.

When using a SIP Softphone it is critical that authentication is used to help prevent unauthorized access to the PBX. To configure authentication a username and password need to be set on the PBX for the relevant extension and on device configuration of the Communication Service.

To configure the authentication on the PBX follow Mitel's recommendations by enabling In-bound Authentication and setting a complex username and password combination on the associated *Sip Phone Group* for the extension.



This same username and password combination would then need to be set on the [device configuration](#) on the

Communication Service for this extension.

For information on configuring Teleworker phones, please refer to the [Remote Connections](#) engineering guidelines.

It is recommended that a complex password is used when configuring the authentication, such as Mitel*Server1!. If using the MBG for external connections, a complex password is a requirement and the authorization name must be the extension number.

Authorization username and passwords are stored encrypted in the MCS database.

Any changes made to the Authorization configuration of an extension within MCS or to the Node IP Addressing will be sent immediately to any 6900 handsets currently connected.

Call Configuration

In addition, the following changes need to be made to the SIP extension's Call Configuration:

- Audio Frame/IP Packet = 2
- DTMF Encoding = RFC 2833 DTMF
- Speech Encoding G.711* or G.729** (G.729 for Phone Manager Desktop Softphone or 6900 only, not Phone Manager Mobile Softphone)

* On some sites, a delay in answering calls has been noticed when using a-law. If you are experiencing this, switch to use mu-law.

** Using G.729 can affect the performance of the telephone system.

It is important to connect only one softphone to each extension number on the telephone systems. Registering more than one SIP extension with the same credentials at the same time is not supported by the telephone system and will cause problems.

If using the desktop and mobile versions of Phone Manager Softphone for a single user then ensure that each application uses different extension numbers.

Remember to configure the [IP Address](#) for each node on the system so Phone Manager knows where to send SIP traffic to.

3 Mobile Client Installation

Phone Manager Mobile is a software application provided for Android and iOS mobile devices. Phone Manager Mobile must be installed by end users via the relevant application store (Apple App Store or Google Play Store). The application is free at the point of installation but will require a [license](#) on the MCS to connect and operate.


Server Side Configuration

MCS & PBX Configuration

Before users start installing Phone Manager Mobile, ensure the following configuration has been completed on the server:

- Users have been given permission to use Phone Manager Mobile on their [Client Profile](#)
- Users have been configured to use [Presence Profiles](#) on their [Client Profile](#)
- Users have a Dynamic Extension Express (DEE) account on the MiVoice Office 250
- Users have their DEE main extension programmed as the Primary Extension on their [MCS user account](#)

For more information about why these configuration steps are needed please review the [Phone Manager Mobile](#) section.

 If using Phone Manager Mobile Office Link features then an OfficeLink Assistant Extension needs creating on the telephone system. Also, any user wanting to make use of the feature needs to have at least one external number in their DEE configuration.

Network Configuration

Phone Manager Mobile clients must be able to connect to the MCS server from inside and outside the local area network so that users have seamless operation and do not need to keep changing their connection details. Phone Manager Mobile will automatically switch between Local and Remote location details. To allow Phone Manager to connect remotely one of the [documented](#) methods needs to be implemented on the customer's network. Once configured, the [Remote Location](#) and [Node](#) information needs to be updated with the external DNS or IP Addresses.

MCS Certificate Configuration

By default the MCS server uses a Self-Signed certificate for Phone Manager Desktop connections. These can be used for Phone Manager Mobile connections as well. In the case of iOS installations the end-user will need to manually install the certificate.

It is possible to purchase and install a certificate from a trusted certificate authority. For more information on this please refer to the [engineering](#) guidelines at the end of this document.

Mobile Client Installation

To install the Phone Manager Mobile client application please follow one of the platform specific guides in the on-line Mobile Help:

- [iOS Installation](#)
- [Android Installation](#)

4 Remote/Teleworker Connections

Most installations will have some requirement to run Phone Manager (Desktop or Mobile) or 69xx phones from outside the LAN. Operating remotely will require that IP traffic is routed from outside of the network to inside the network in a secure manner.

There are three different ways to route external traffic to the Mitel Communication Service / MiVoice Office 250:

- VPN (Recommended for Phone Manager Desktop remote connections)
- Port Forwarding (not recommended for remote 69xx phones)
- Proxy through a MiVoice Border Gateway

Once one of the chosen methods has been implemented, the Remote [Location](#) and Remote [Node](#) IP addresses / hostnames need to be updated so that Phone Manager/69xx phones know how to connect back to the system.

VPN

Using a virtual private network (VPN) is the simplest way of connecting Phone Manager to the MCS / telephone system from outside the local area network. Once a VPN tunnel is in place between the host client (Mobile phone or desktop PC) and the network then Phone Manager will be able to connect as normal with no configuration changes required by the end-user.

VPN is the best way of connecting Phone Manager Desktop from an external computer, especially when using Phone Manager Softphone.

Port Forwarding

Another method of connecting Phone Manager from outside the network is to use port forwarding. Port forwarding involves configuring the customer's existing firewall to forward traffic on the necessary ports through to the MCS / telephone system.

For more information on Port Forwarding please click [here](#).

MiVoice Border Gateway


Mitel provide a dedicated proxy solution for connecting software and devices from outside the local area network. This is the supported method for remote 69xx phones.

For more information on the MiVoice Border Gateway please click [here](#).

4.1 Connecting Through Firewalls

Port Forwarding

One method to connect Phone Manager from outside the local network is to use Port Forwarding. This involves reconfiguring the customer's firewall or router to forward traffic on specified ports through to the either the Mitel Communication Service or the MiVoice Office 250 telephone system.

 **WARNING** - Port Forwarding is a security risk when opening up SIP ports on the telephone system to the outside world. Mitel does not recommend using Port Forwarding for external Softphone connections.

Port Forwarding for Remote Phone Manager Desktop Connections

Configure the ports shown below to be forwarded to the IP address of the MCS server:

Port	Target	Description
TCP 8187 & 8186	MiVoice Office Application Suite	Used to communicate to the MCS server to provide configuration, user data, chat etc.
TCP 8188	MiVoice Office Application Suite	Integration Services, only required if client access to the server-side API is required
TCP 2001	MiVoice Office Application Suite	Used to provide telephony status and real-time data.
TCP 8200 & 8204	MiVoice Office Application Suite	Used to provide Personal Wallboard real-time data.

Port Forwarding for Remote Phone Manager Mobile Connections

Configure the ports shown below to be forwarded to the IP address of the MiVoice Office Application Suite server:


Port	Target	Direction	Description
TCP 8185	MiVoice Office Application Suite	Inbound	Used to communicate to the MCS server to provide configuration, user data, chat etc.
TCP 8190	MiVoice Office Application Suite	Inbound	Softphone Audio

4.2 MiVoice Border Gateway with Phone Manager Mobile

Phone Manager Mobile Port Forwarding on MBG

Phone Manager Mobile uses the following TCP/UDP ports to operate:

Port	Target	Description
TCP 8185	MiVO App Suite Server	Used to communicate to the MCS server to provide configuration, user data, chat etc.
TCP 8190*	MiVO App Suite Server	Softphone Audio

 * Only required when the Softphone is running. Phone Manager Mobile does not require Teleworker licenses or configuration on the MBG.

Configuring Port Forwarding for Phone Manager Mobile


Complete the following configuration on the MBG:


- On the 'MBG Security -> Port Forwarding' page, create the port forwarding rules for TCP 8185 with the Destination Host IP Address pointing to the IP address of the MCS host.

If using a Softphone then configure the following port forwarding:

- On the 'MBG Security -> Port Forwarding' page, create the port forwarding rules for TCP 8190 with the Destination Host IP Address pointing to the IP address of the MCS host.

Protocol	Source Port(s)	Destination Host IP Address	Destination Port(s)	SNAT	Action
TCP	8185	172.19.5.46	8185	Yes	Remove
TCP	8190	172.19.5.46	8190	Yes	Remove

 SNAT must be enabled on all the port forwarding rules added.

 For more information on configuring Remote Softphone connections, see [here](#).

Phone Manager Mobile Configuration

No specific configuration is needed on the Phone Manager Mobile client software. Ensure local and remote addresses for the mobile client to connect to have been configured on the server in the [Client Locations](#) section.

A trusted [certificate](#) is also recommended for Phone Manager Mobile connections.

5 SSL Certificate


The SSL certificate configuration section provides access to control the certificate used by Client Applications (Phone Manager Desktop/Mobile, Call Recorder Client) and the web site for HTTPS if required. By default, a self-signed certificate is created by the MCS when it is installed. This is used by clients to communicate back to the MCS. This means the data sent between Phone Manager and MCS is encrypted. Alternatively a certificate may be purchased from a trusted certificate authority and installed on the MCS. When doing this, the DNS name used for the server/certificate must be accessible both internally and externally by the Phone Manager clients.

Optionally, when adding a certificate from a trusted authority, it can also be applied to the website and real-time services so that access to the configuration, Real-Time Dashboard/Wallboard and Call Recorder are all over HTTPS.

Certificate Properties

The properties of the certificate currently in use by the system are displayed on the page.

- Status -> Self-Signed or Trusted
- Certificate Expiry -> The date the certificate will expire
- Hostnames -> The hostnames the certificate is currently supporting
- Usage -> Indicates whether the certificate is just being used for client applications or the website as well

 The hostnames used for the certificate need to match those configured in the [Client Locations](#) section. If using a self-signed certificate, the certificate will be regenerated automatically anytime these addresses get updated.

Requesting/Using a Trusted Certificate

To improve security and simplify Phone Manager Mobile client installations, a trusted certificate can be purchased and applied to the server.

Pressing the 'Start Certificate Request' button will start the process of creating a certificate request file. This must be populated with the following information:

Common name	The fully-qualified external domain name of the MCS server. This should be the Client Location Remote 'NAT IP Address/Hostname' address configured on your MCS server If you are requesting a Wildcard certificate, add an asterisk (*) to the left of the common name where you want the wildcard, for example *.<mydomain>.com.
Alternative names	Enter any alternative hostnames or IP addresses that may be used to connect to the server, for example the internal DNS name. This must include the Client Location Local 'IP Address/Hostname' address configured on your MCS server
Organization	The legally-registered name for your business. If you are enrolling as an individual, enter the certificate requestor's name.
Organization unit	If applicable, enter the DBA (doing business as) name.
State / region	Name of the state or province where your organization is located. Do not abbreviate.
	Name of the city where your organization is registered/located. Do not

City / locality	abbreviate.
Country	The country where your organization is legally registered.


The 'Common Name' and 'Alternative Names' fields should match those that the clients are using to connect to the server. They will be pre-populated with the information from the [Client Locations](#) section.


Once the fields have been correctly populated, press the 'Download CSR file' button to generate the certificate request. You will be prompted for a location to store the file.

This CSR should be submitted to a certificate authority to request a certificate. Once the certificate has been obtained, it can be uploaded to the system using the 'Complete Certificate Request' button.

Any certificate uploaded will be used for client application connections. Optionally it can also be used for website connections by checking the relevant box.

For more information on enabling HTTPS on the website, please refer to the [Enabling HTTPS](#) section.

 A restart of the system is required for certificate changes to take effect.

 If using a trusted certificate, it must be updated any time the local or remote addresses in the [Client Locations](#) section are updated.

Unbinding

To revert back to a self-signed certificate and remove a certificate that has been applied to the solution, press the 'Unbind from website' option at the bottom of the current certificate's information:

If you have a CA-signed certificate you can also bind it to the website to allow website traffic to be encrypted.

Status	OK
Certificate Expiry	07/04/2021 13:39:52
Host Names	qa-uk-lab37.qa.test
Usage	Client applications Website connections Unbind from website

[View Certificate](#)
[Start Certificate Request](#)
[Complete Certificate Request](#)

Using this option will unbind the certificate from the website and update the bindings in IIS, disabling the enforced SSL usage on the website.

To stop the certificate being used for Phone Manager Client connections, follow these steps:

- Open MMC.exe
- Add the Certificates snap-in for the **Local Computer**
- In the snap-in, expand 'Personal -> Certificates'
- Find the certificate with the friendly name "MCS - Phone Manager client connections", edit this and change the friendly name to something else (put OLD at the end etc)
- Restart the MCS services
- New self-signed certificates will be generated

6 Index

Connecting Through Firewalls, 11

Mitel Back Page, 17

Mitel Phone Manager Mobile - Installation Guide, 0

MiVoice Border Gateway with Phone Manager Mobile, 12

Mobile Client Installation, 9

Mobile Client Requirements, 3

Notice, 2

Phone Manager Softphone, 4-8

Remote/Teleworker Connections, 10

SSL Certificate, 13-15



mitel.com

© Copyright 2020, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation.
Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.