# Mitel Phone Manager Mobile Installation Guide

⋈ Mitel

# Table of Contents

**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.

# 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.mitelcommunicationservice.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.
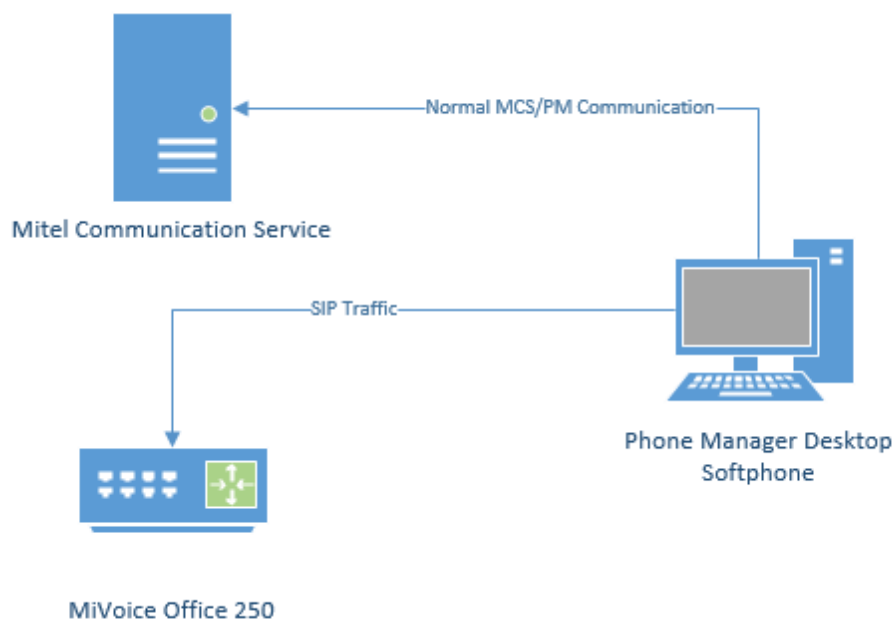


For information on connecting Phone Manager Desktop from outside the LAN, refer to the appropriate guide:

- 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:
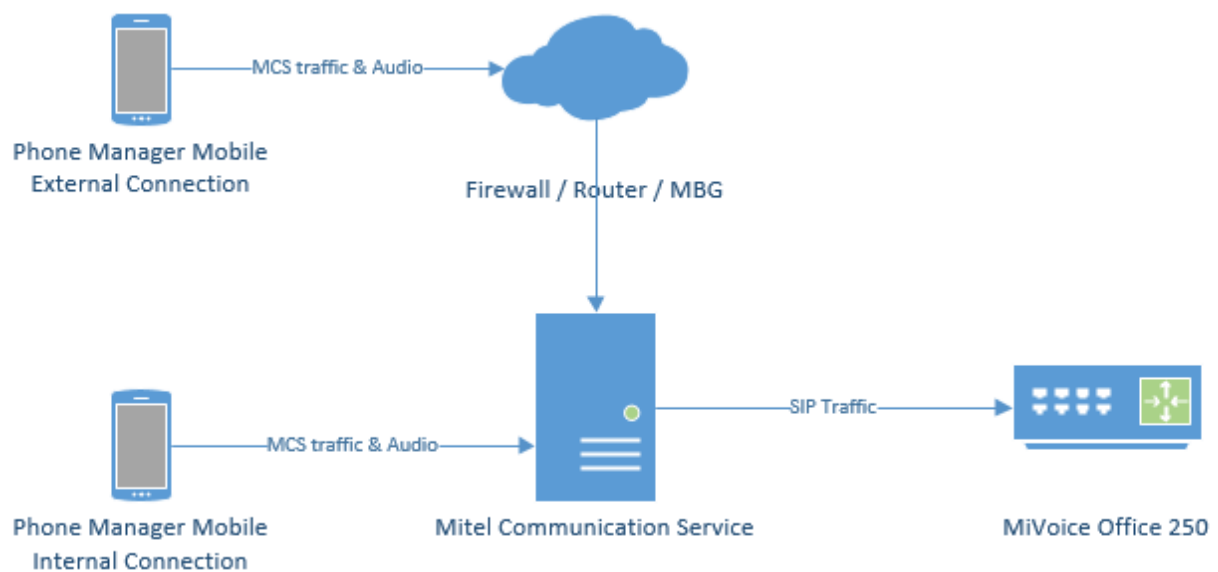


The MCS SIP Proxy requires G.711 to be configured against the SIP Endpoint on the telephone system as the audio encoding for making calls.

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 Authorisation 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 minimises the risk of mis-configuration.

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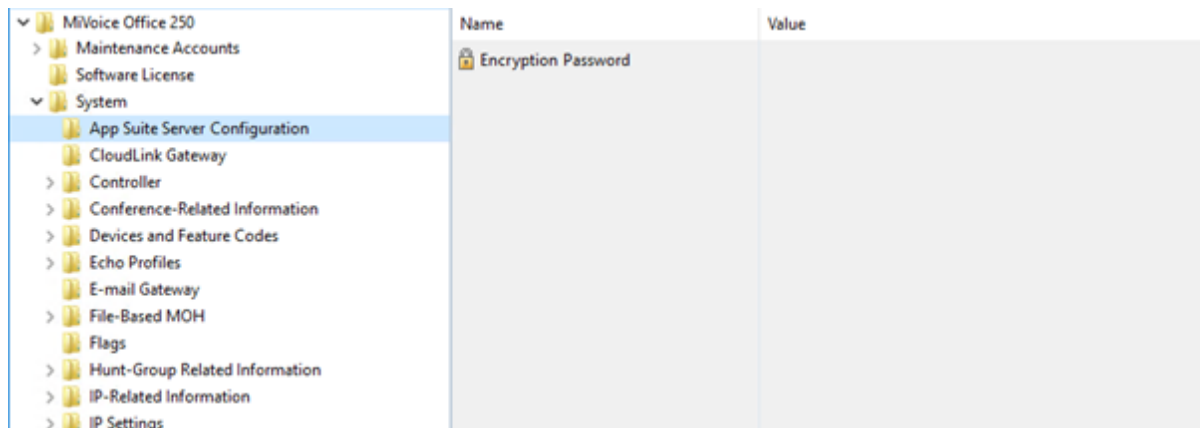
**Encryption Password**

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 authorisation 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 as 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 authorisation credential query to work.

**Node Configuration for SIP**

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.
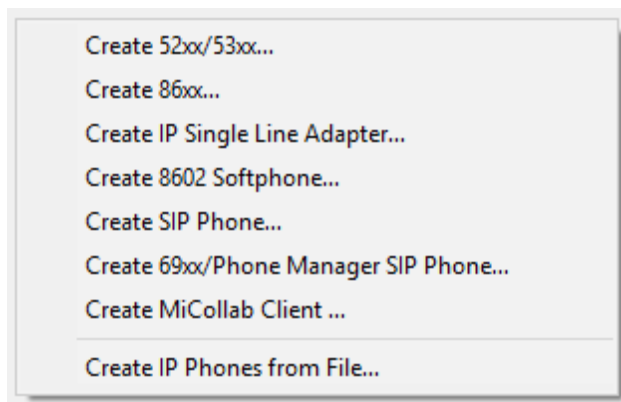


When SIP extensions are created using this type, the SIP Phone Groups created will automatically be configured with the required settings and will have a default inbound authentication applied with a randomly

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.

# 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

The following server-side configuration steps need to be completed before Phone Manager Mobile clients can start to be deployed:

**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:

- iOS Installation

- Android Installation

# 3.1 Mobile iOS Installation

## iOS Installation

This section outlines the steps involved in getting Phone Manager Mobile installed on one of the supported iOS devices.

### Installation Requirements

End-users will need the following information in their possession before they start the mobile client installation:

- Their username and password for accessing MCS. This may be their Domain user account (in format DOMAIN\username) or an MCS username and password.
- A valid network on their iOS device, Ideally they will be on the same network as the MCS Server.
- The IP address / Hostname of the MCS server. If connected to the corporate LAN then they will need the external IP Address / DNS name that has been configured for the remote Phone Manager Mobile connections.

### Installation Steps

The following steps need to be followed to successfully complete a Phone Manager Mobile installation on an iOS device:

- Locate and install the Mitel Phone Manager Mobile application from the App Store on the iOS device. The application is free at the point of installation to the end-user. The application logo is shown below:



- Launch the application
- The end-user license agreement will be displayed, this must be accepted before continuing.
- The user will then be presented with the 'Get Started' screen. The server connection details (IP address / hostname) and the user's username and password need to be entered at this point. If using a self-signed certificate on the MCS server the user will need to install the certificate at this time.
- Installing the certificate:
  - If the user is on the same network as the MCS server then they can click the 'download SSL Certificate' link from the 'Get Started' screen.
  - If the user is remote then they will need to be emailed the certificate as an attachment. This can be done from the Mobile Clients Page on the MCS server. Clicking on the attachment will bring up the same certificate installation page as clicking on the download link.

●●●○○ O2-UK 📶      10:44      ➤ ✳ 96% ▭

## Get started

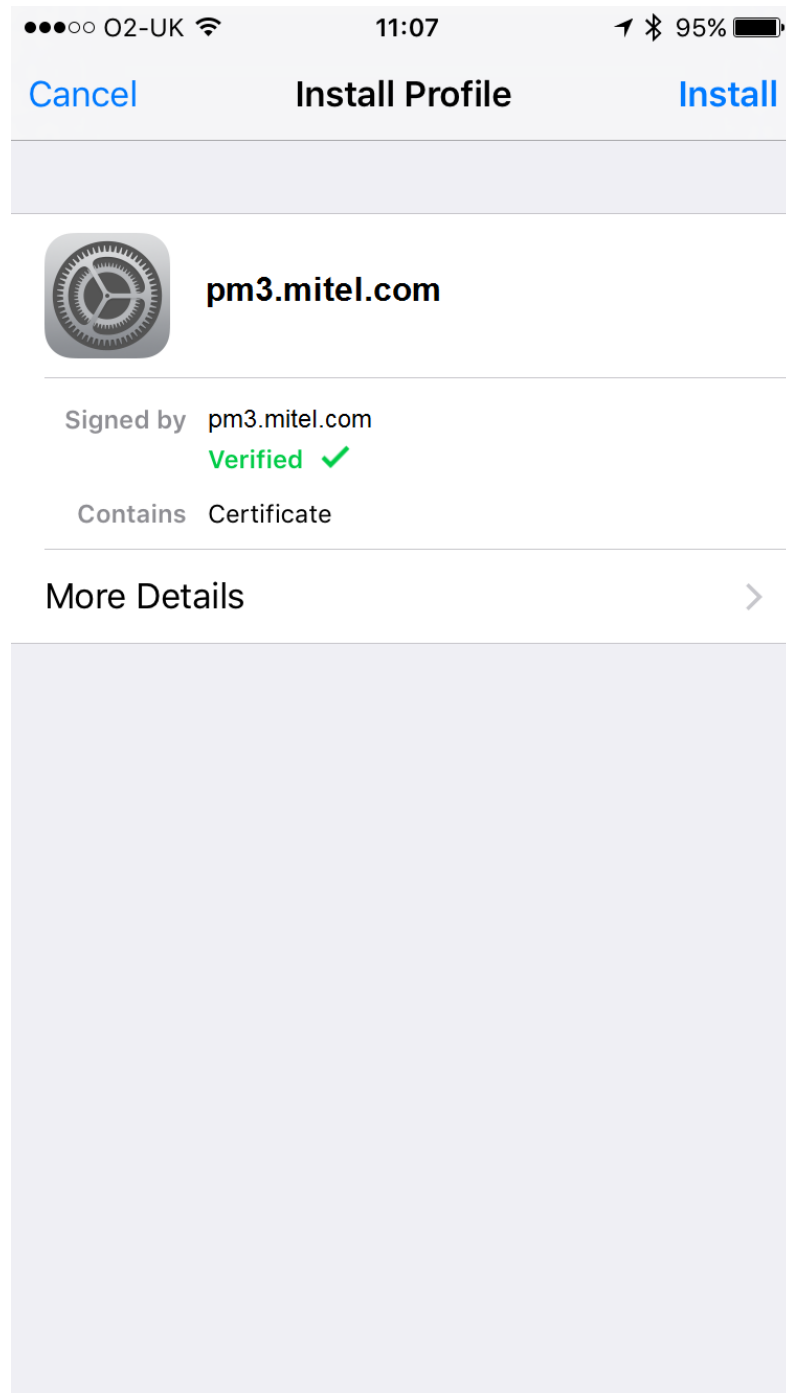To get up and running, please enter your server and account details.

Server

Username

Password

In order to connect to this server, you must first download and install its SSL certificate (you may need to be on the office network to do this)

Download SSL certificate

Connect

- Pressing 'Install' in the top corner will store the certificate on the local device.
- Press the 'Connect' button to complete the configuration

If the configuration is successful the application will load and the user will be presented with main Phone Manager UI.

### Troubleshooting

If the user has problems:

- They have not installed the self-signed certificate

- They have entered their domain username in the format 'username@domain' or have entered their email address instead of 'DOMAIN\Username'
- The user does not have a Primary Extension programmed against their User Account on MCS
- The user's client profile does not give them permission to use Phone Manager Mobile
- The user's client profile is not configured to use Presence Profiles
- The user has entered an incorrect server address or username/password (if they are remote they will need to enter the remote server connection details on the 'Get Started' page).

**iOS 10.3 Onwards**

From iOS 10.3, Apple have increased the security on self-signed certificates. If you are having problems on iOS 10.3, please follow these steps:

On the iPhone, Navigate to 'Settings -> General -> about'. At the bottom of this list is an entry labelled 'Certificate Trust Settings'. In this section there are toggle controls for the installed certificates. Locate the certificate for the MCS server and enable it.

# 3.2  Mobile Android Installation

## Android Installation

This section outlines the steps involved in getting Phone Manager Mobile installed on one of the supported Android devices.

### Installation Requirements

End-users will need to have the following information in their possession before they start the mobile client installation:

- Their username and password for accessing MCS. This may be their Domain user account (in format DOMAIN\username) or an MCS username and password.
- A valid network on their device, Ideally they will be on the same network as the MCS Server.
- The IP address / Hostname of the MCS server. If the user is installing this remotely i.e. not connected to the corporate LAN then they will need the external IP Address / DNS name that has been configured for the remote Phone Manager Mobile connections.

### Installation Steps

The following steps need to be followed to successfully complete a Phone Manager Mobile installation on an Android device:

- Locate and install the Mitel Phone Manager Mobile application from the Play Store on the Android device. The application is free at the point of installation to the end-user. The application logo is shown below:



- Launch the application.
- The end-user license agreement will be displayed, this must be accepted before continuing.
- The user will then be presented with the 'Get Started' screen. The server connection details (IP address / hostname) and the user's username and password need to be entered at this point.
- Press the 'Connect' button to complete the configuration.
- The first time you connect to the server you will receive a 'Certificate Error' popup (similar to that shown below) - this will allow you to confirm the Subject and Issuer is your server and then press 'Trust' to trust the certificate. Once trusted it will not re-appear unless the MCS server certificate has changed.
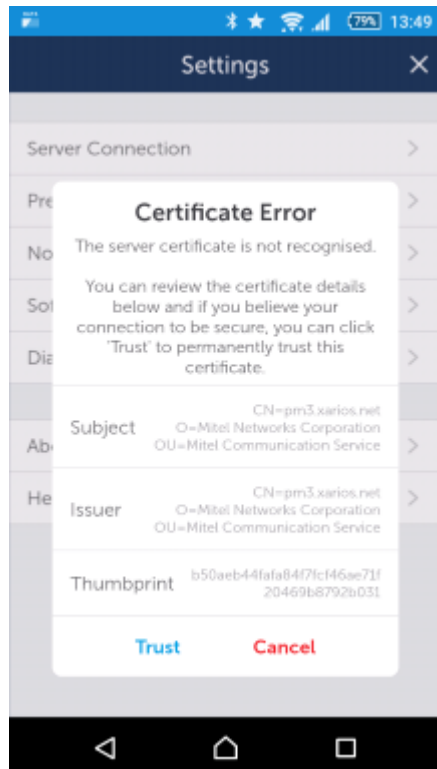
If the configuration is successful the application will load and the user will be presented with main Phone Manager UI.

## Troubleshooting

If the user has problems connecting:

- They have entered their domain username in the format 'username@domain' or have entered their email address instead of 'DOMAIN\Username'
- The user does not have a Primary Extension programmed against their User Account on MCS
- The user's client profile does not give them permission to use Phone Manager Mobile
- The user's client profile is not configured to use Presence Profiles
- The user has entered an incorrect server address or username/password (if they are remote they will need to enter the remote server connection details on the 'Get Started' page.

# 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 recommend 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 | Direction | Description |
|---|---|---|---|
| TCP 8187 & 8186 | MCS Server | Inbound | Used to communicate to the MCS server to provide configuration, user data, chat etc. |
| TCP 8188 | MCS Server | Inbound | Integration Services, only required if client access to the server-side API is required |
| TCP 2001 | MCS Server | Inbound | Used to provide telephony status and real-time data. |
| TCP 8204 | MCS Server | Inbound | Used to provide Personal Wallboard real-time data. |
| UDP 5060* | MiVoice Office 250 | Inbound/Outbound | SIP connectivity to the telephone system, used by the Phone Manager Desktop Softphone. |

* Only required when the Softphone is running

### Port Forwarding for Remote Phone Manager Mobile Connections

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

| Port | Target | Direction | Description |
|---|---|---|---|
| TCP 8185 | MCS Server | Inbound | Used to communicate to the MCS server to provide configuration, user data, chat etc. |
| TCP 8190 | MCS Server | 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 | Direction | Description |
| --- | --- | --- | --- |
| TCP 8185 | MCS Server | Inbound | Used to communicate to the MCS server to provide configuration, user data, chat etc. |
| TCP 8190* | MCS Server | Inbound | Softphone Audio |

*\* Only required when the Softphone is running. Phone Manager Mobile does note require Teleworker licences 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.

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. <br><br> This should be the Client Location Remote 'NAT IP Address/Hostname' address configured on your MCS server <br><br> 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. <br><br> This must include the Client Location Local 'IP Address/Hostname' address configured on your MCS server |
| **Organisation** | The legally-registered name for your business. If you are enrolling as an individual, enter the certificate requestor's name. |
| **Organisation unit** | If applicable, enter the DBA (doing business as) name. |
| | Name of the state or province where your organisation is located. Do not |

| State / region | abbreviate. |
| --- | --- |
| City / locality | Name of the city where your organisation is registered/located. Do not abbreviate. |
| Country | The country where your organisation 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.

# 6 Index

Powering connections