Mitel Phone Manager Mobile Installation Guide

APRIL 2017

DOCUMENT RELEASE 5.0

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.

TRADEMARKS

MiVoice Office Application Suite
Release 5.0 - April, 2017

1 Mobile Client Requirements

Phone Manager Mobile is available for both iOS and Android platforms. The following section outlines the supported operating systems Phone Manager Mobile has been designed to support and the hardware variants it has been tested against.

> Phone Manager should run on devices not listed here as long as the operating system version is supported. However, not all features can be guaranteed to work on devices not in the list
>
> For unlisted devices support will be offered on a best endeavours basis.
>
> The client is not optimised for use on tablets.
>
> For use while travelling in the car we recommend using 'OfficeLink' as opposed to the softphone as this will generally give a call connection with a variety of mobile signals where a softphone data connection may not be reliably maintained.
>
> Bluetooth devices are not officially supported with this release, the level of functionality is solely based on the support of Bluetooth devices provided by the OS.
>
> Please refer to the release notes for up to date information.

iOS

Supported Operating systems

- iOS 9.x, 10.x

Supported Hardware

- iPhone 5 / 5s /5c
- iPhone 6 / 6s / 6 Plus / 6s Plus
- iPhone SE

Android

Supported Operating systems

- Nougat (7.x)
- MarshMallow (6.x)
- Lollipop (5.x)

Supported Hardware

- HTC One M8
- Motorola Droid Turbo / G3
- Nexus 5X
- Samsung Galaxy S5 / Galaxy S5 mini / Galaxy S6 / Galaxy S6 Edge / Galaxy S7
- Sony Xperia Z3 / Xperia Z3C

Network Performance for Softphone Calls

- Bandwidth (per call) - 32 kbit/s

- Latency - not exceeding 150 ms
- Jitter - not exceeding 50 ms

Network Data Utilisation for Softphone Calls

- A call would use a maximum of 32kbit/s which calculates into 4 Kbyte/s or 240 Kbytes per minute

2 Phone Manager Softphone

Phone Manager Desktop and Phone Manager Mobile both have Softphone capabilities that allow them to become an endpoint 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
- 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

MiVoice Office 250 Configuration

A SIP extension must be configured on the telephone system for each Phone Manager Softphone that will be connecting. Against each SIP extension's Phone Group configure the following settings (replace the examples in brackets with your own configuration):

- Maximum Number of Calls = 4
- Enable in-bound authentication = Yes
- Configure in-bound authentication username (e.g. 1880)
- Configure in-bound authentication password (e.g. m1t3l!)
- DTMF Payload = 101
- Camp-Ons Allowed = No
- Supports Ad Hoc Conferencing
- Use Registered Username (only required when connecting through an MBG)
- NAT Address Type = Native (when connecting through an MBG)

Repeat this process for each SIP extension required.

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 only, not Phone Manager Mobile)

* 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 set authentication against each SIP extension and ensure the password is complex. For example, *Mitel*Server1!.* If connecting externally through and MBG, a complex password is a requirement.

> ⚠ If a user is using a softphone on both Phone Manager Desktop & Phone Manager Mobile it is important to set them up two SIP Endpoints on the phone system

Mitel Communication Service Configuration

The MCS needs to be told about each SIP endpoint's authentication details and what IP address the Phone Manager Softphone should be connecting to. This information is programmed on the MCS so that a minimum

amount of work is required by the user when configuring Phone Manager.

SIP Device Authentication

Through it's OAI connection MCS will already know about any SIP extensions that have been created on the telephone system. Each SIP extension must have it's authentication details entered into MCS.

- On the MCS website, browse to "Configuration -> Site Settings -> Phone Systems -> <*PBX NAME*>".
- Locate the SIP extension to update and press Edit.

In the edit form that loads configure the Authorisation name and password for the SIP extension and press Confirm. Repeat this process for each SIP extension on the telephone system.

For more information click here.

> ⚠ Authorisation username and passwords are stored encrypted in the MCS database so that they can only be accessed by Phone Manager.

Node IP Addressing

When registering as a Softphone, Phone Manager needs to know the IP Address of the telephone system the SIP extension is on. This can be different from the OAI IP address the MCS already knows about in the following scenarios:

- OAI is being provided by a CT Gateway
- The telephone system has a PS1 installed with alternate IP addresses for OAI / SIP

For Phone Manager clients to register SIP softphones the following configuration must be completed:

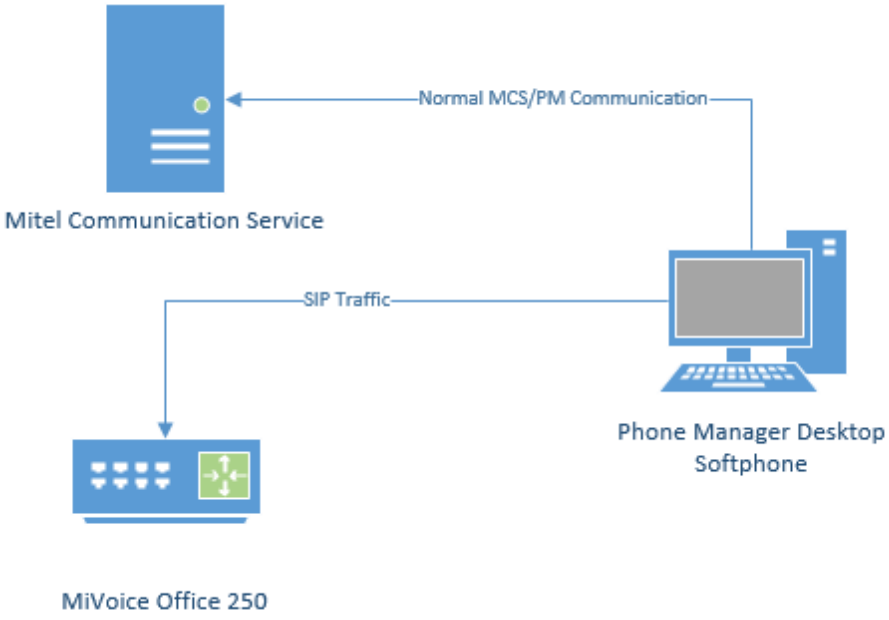
- On the MCS website, browse to "Configuration -> Site Settings -> Phone Systems -> <*PBX NAME*>"
- Locate the Nodes section at the bottom of the screen
- Edit each node and put in the Local & Remote IP address and port numbers for SIP (For remote, the IP address / Port will be those of the Router or MBG).

MCS now knows the authorisation details for the SIP extensions and the IP address / Port numbers it needs to connect to when registering the Softphone. It will pass this information to Phone Manager Desktop / Mobile when they are connecting as a Softphone.

For more information click here.

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:

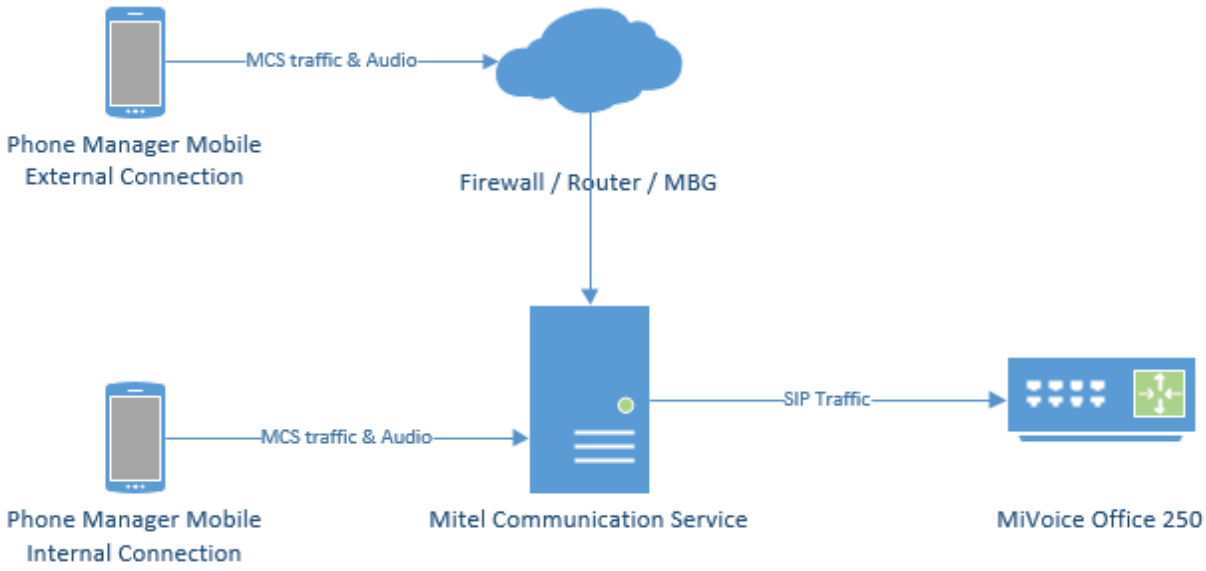
- Connecting Phone Manager Desktop using a MiVoice Border Gateway
- Connecting Phone Manager using a Router

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.

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:

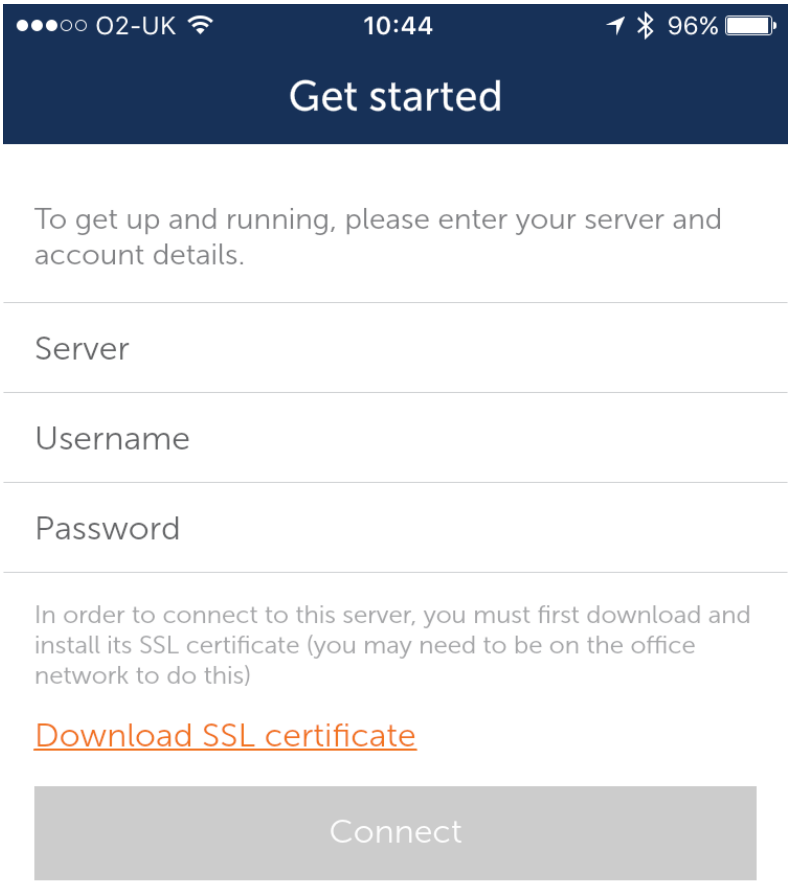
- Their username and password for accessing MCS. This may be their Domain user account (in format DOMAIN\username) or an MCS username and password.
- A valid network on their iOS device, Ideally they will be on the same network as the MCS Server.
- The IP address / Hostname of the MCS server. If connected 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.

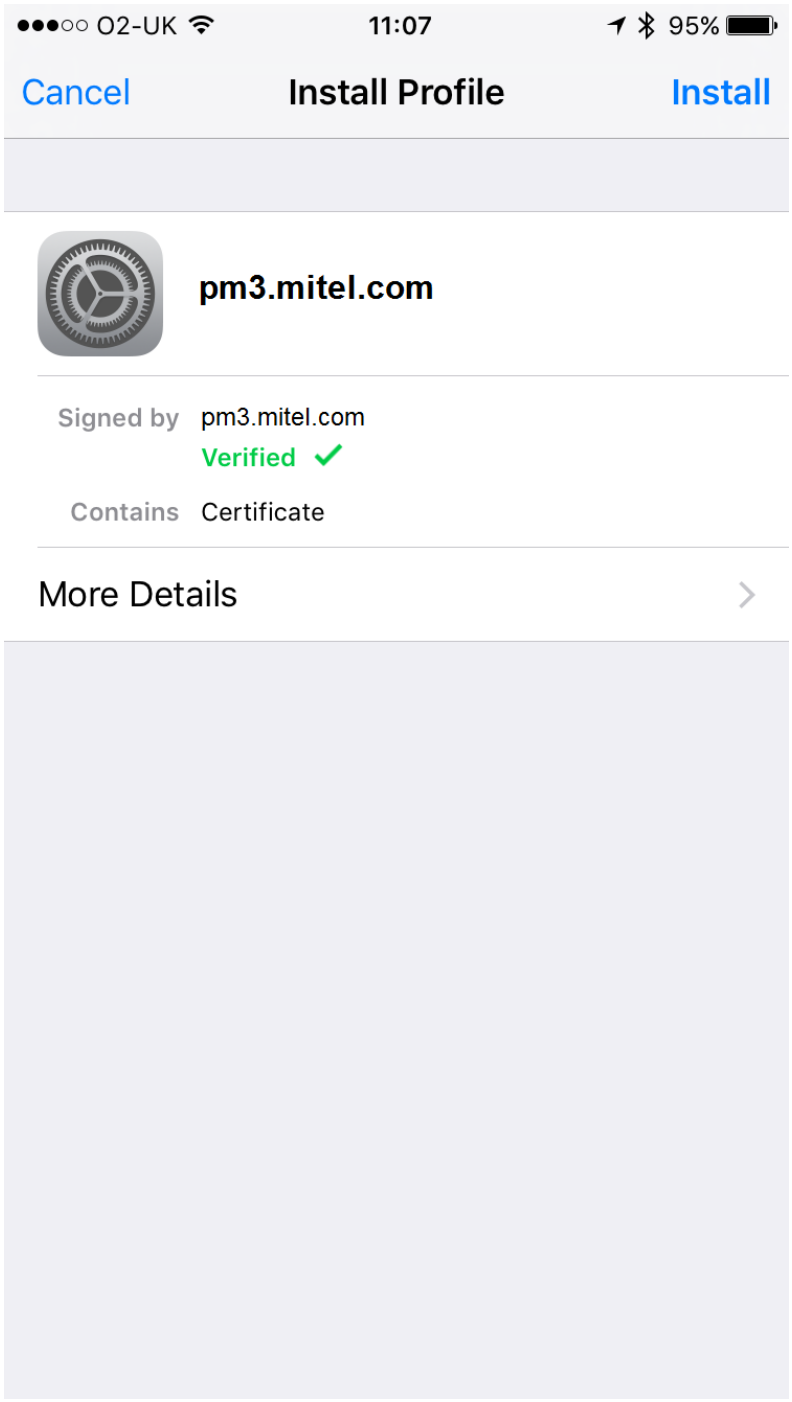
Installation Steps

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:

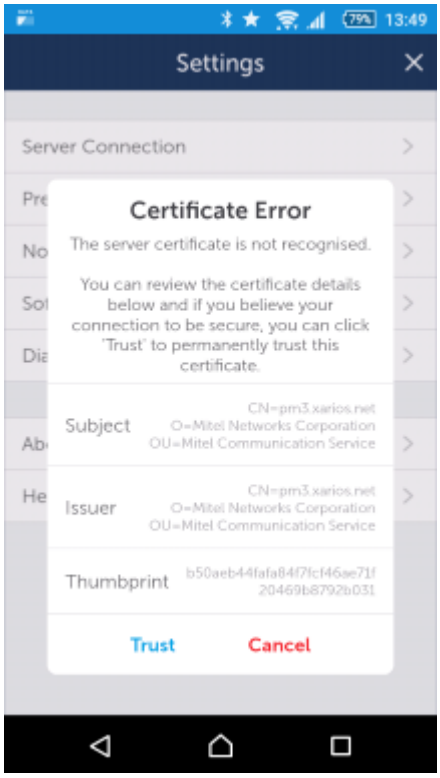
- Their username and password for accessing MCS. This may be their Domain user account (in format DOMAIN\username) or an MCS username and password.
- A valid network on their device, Ideally they will be on the same network as the MCS Server.
- The IP address / Hostname of the MCS server. If the user 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 Connections

Most installations will have some requirement to run Phone Manager (Desktop or Mobile) from outside the LAN. Operating remotely will require that Phone Manager 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
- 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 knows how to connect back to the system.

VPN

Using is 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 outside the local area network.

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.
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 will normally be used both on the internal network and remotely and will need to transition between the two without any reconfiguration by the end-user. It can be used remotely, connecting back to the Mitel Communication Service through a MiVoice Border Gateway (MBG) using Port Forwarding.

Phone Manager Desktop 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.

MiVoice Border Gateway Configuration

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 needed as local and remote address for the mobile client are configured in the server.

5 Using a Certificate Authority Certificate

To use a certificate generated from a third party or another certificate authority (CA) a certificate signing request (CSR) needs to be generated.

This CSR can then be provided to the CA who can then create the certificate to use.

From the Configuration -> Site -> Features -> Phone Manager -> Certificates section select the "MCS SSL client certificate" and click on Edit. Enter the requested information into the relevant fields.

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 'NAT 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.
State / region	Name of the state or province where your organisation is located. Do not 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 certificate (even a wildcard one) needs to include either in the Common name or the Alternative name **BOTH** of the configured 'Local IP Address/Hostname' and 'NAT IP Address/Hostname' addresses in the Client Locations Configuration of your MCS server.

Once complete click on the Download CSR file button. This will download a file called MCS_CertificateSigningRequest.csr that contains the CSR information, like that shown below.

-----BEGIN NEW CERTIFICATE REQUEST-----
MIID6TCCAtECAQAwUTEMMAoGA1UECwwDYXNkMQwwCgYDVQQKDANhc2QxCTAHBgNV
BAYTADEMMAoGA1UEBwwDYXNkMQwwCgYDVQQIDANhc2QxDDAKBgNVBAMMA2FzZDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOYYymhzefrUTuuLQxjZopBX
xOVZiazFt2TGyRVvL7kq2J1vQST5aHM0x3VbTssq/JgT6KIa99U8k0LDGKEHvOrs
HtR6Ym2y70nm5ou96kVP1a8t1B2zbJDM8W4fth1Ns3BqPqPNe7GuybwzKZEYcFG7
/jbzNf6aU9SeXHG7wFL5H/caZJqsgJ4WmlHfwBqwNgQJJLiVcL2PLVgIJWasX543
om4V5bSy7AcMy6DnJYlkFjijffWH8Y1aI19eTJCLEIstpBHYL1JecAP+0aBsKi7+
VOk+E+RRHuVT8w/oGCPcnM4r5XEKCUk4ccQwGAUGrnOkGfRfBUbltt7HuYjNtEsC
AwEAAaCCAVEwGgYKKwYBBAGCNw0CAzEMFgo2LjIuOTIwMC4yMFcGCSsGAQQBgjcV
FDFKMEgCAQUMF3hhci11ay1kZXYwMi5YYXJpb3MuTmV0DBdYQVJJT1NORVRcWEFS
LVVLLURFVjAyJAwRQ1MuV0NGU2VydmljZS5leGUwZgYKKwYBBAGCNw0CAjFYMFYC
AQIeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAdABYAG8AbgBnACAAQwByAHkAcAB0
AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgMBADByBgkqhkiG9w0B
CQ4xZTBjMA4GA1UdDwEB/wQEAwIE8DAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYB
BQUHAwIwEwYDVR0RBAwwCoIDYXNkggNhc2QwHQYDVR0OBBYEFId7bOuIH9Yoi7fA

IKSeqZrBuPLvMA0GCSqGSIb3DQEBBQUAA4IBAQBSFRCeUY/5HvGhcua8nEqq5lej
Z3pP+jkEgo2xCaJ7MXLQ+4uYCY0dBwzJ8I15+SrYSMmvbo8agRsvQeF5ntJTXIou
FBHul0rTCs7VUPyfwqzYc89Jg85PmDJklKoCzXHdJX/F7iH21BGtMhKpr41VXRug
KjG82ggWP5w0pfTadE9dGC5ga+MHfsWqS6SQsYbY6lyOfGMhc7d4DbgXWYpcV54N
eFwBTQPURSH6aw/N0k3kiXzKC82BtuyKtKiwk5E3309we17K0KuSRcDxSKS+pUGQ
ccvhR3x5++RX496X+nGU9VZ19V/csITUFL3OZAecRMBGCvxrm9iGjJjCkVNx
-----END NEW CERTIFICATE REQUEST-----

Follow the relevant process from the CA that is being used to create the certificate. The certificate needs to be Base64 encoded.

Once the certificate has been received, this then needs to be uploaded back into the server. From the 'Configuration -> Site -> Features -> Phone Manager -> Certificates' section select the "MCS SSL client certificate" and click on Edit. As you have already completed the information when you create the CSR - just select the 'Next' button and using the 'Choose files' button, select the certificate file then click on 'Save'

The new certificate will take effect.

> If you change the certificate your Android mobile clients will get a popup on connection to trust the new certificate

If you use a certificate from a trusted CA then you no longer need to have a copy of the server certificate installed on the client

6 Index

mitel.com