Mitel Phone Manager Mobile Installation Guide

APRIL 2018

DOCUMENT RELEASE 5.1

INSTALLATION GUIDE

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.

MiVoice Office Application Suite
Release 5.1 - April, 2018

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 may 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 endeavors basis.
>
> The client is not optimized for use on tablets.
>
> For use while traveling 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, 11.x

Supported Hardware

- iPhone 5 / 5s /5c
- iPhone 6 / 6s / 6 Plus / 6s Plus
- iPhone 7 / 7 Plus
- iPhone SE

Android

Supported Operating systems

- Oreo (8.x)
- Nougat (7.x)
- MarshMallow (6.x)
- Lollipop (5.x)

Supported Hardware

- HTC One M8
- Motorola Droid Turbo / G3 / G5 plus
- 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 Utilization 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 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.

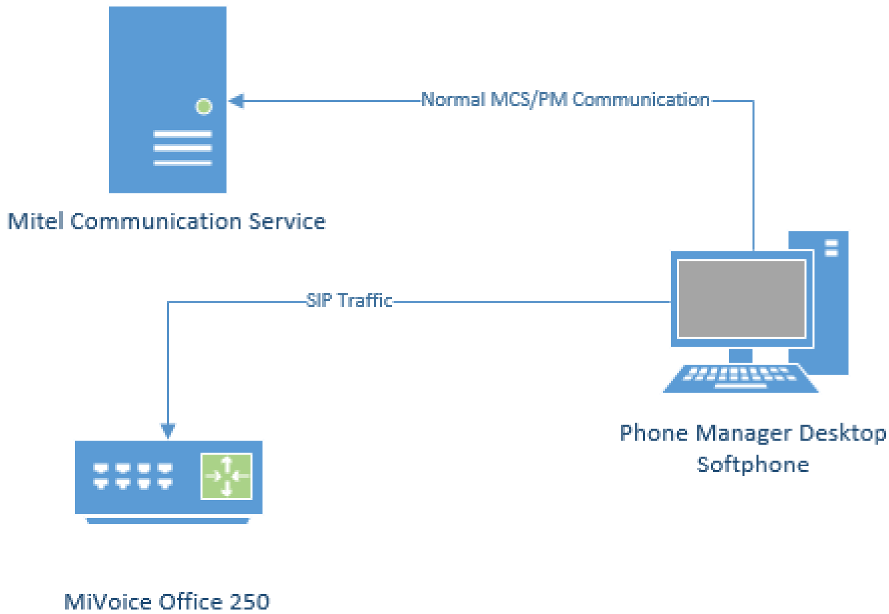
Requirements

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

- MiVoice Office 250 6.1 or higher (Release 6.3 PR1 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.

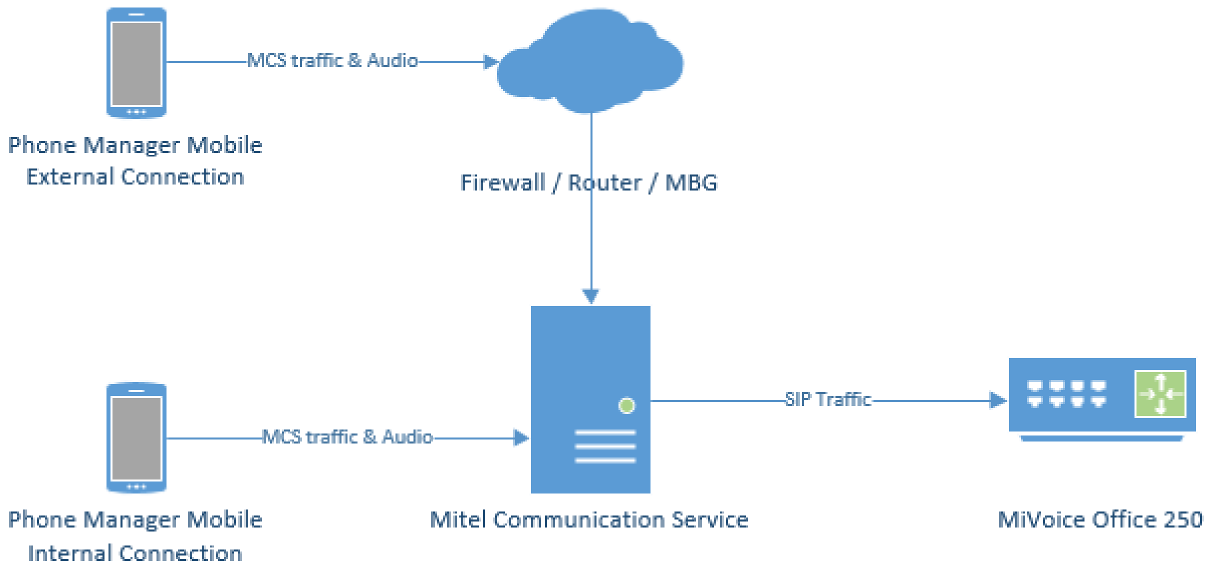
To work around this issue, Auto NAT Detection needs to be disabled on Phone Manager Desktop.

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 . The sections below outline the changes that are required for the SIP Extension's Phone Group and Call Configuration.

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

Node Configuration

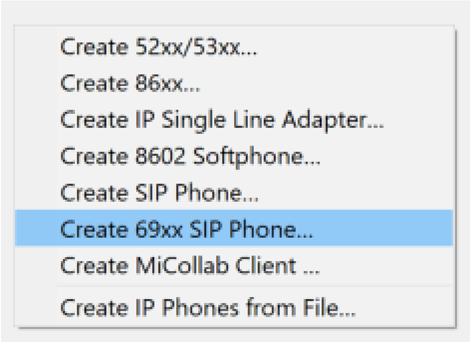
The MCS server needs to provide each 6900 phone and Phone Manager Softphone with the IP address of a SIP server to register with. The IP address required will depend on which MiVoice Office 250 node the SIP extension is configured on and whether the phone is local or a teleworker.

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

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

69xx SIP Phone

From release MVO 250 6.3 onwards, a new SIP phone type called '69xx SIP Phone' 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.

> For release prior to 6.3, the normal SIP Phone type should be used for Phone Manager Softphones. Please review the Phone Group settings below to check the required configuration.

> 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.

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 = 4
- 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.

Authentication

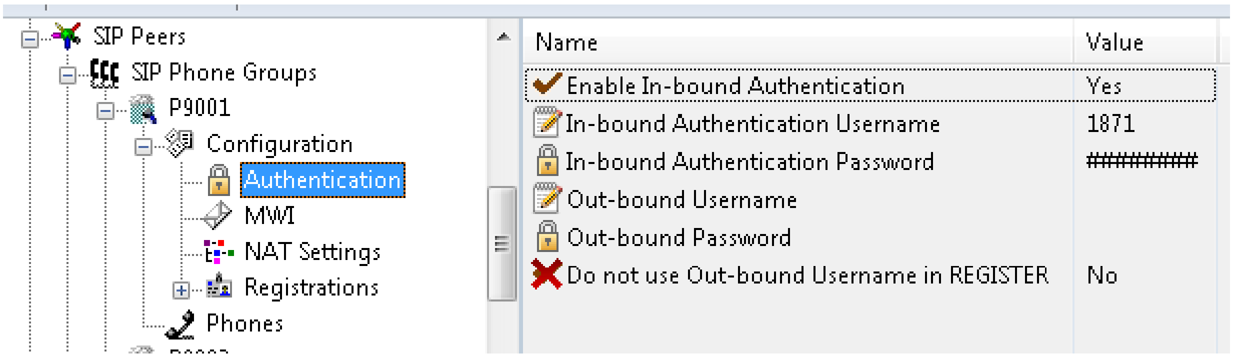
If a version prior to 6.3 SP1 is being used, the Inbound Authentication Credentials will need to be configured on both the telephone system and the MCS server.

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

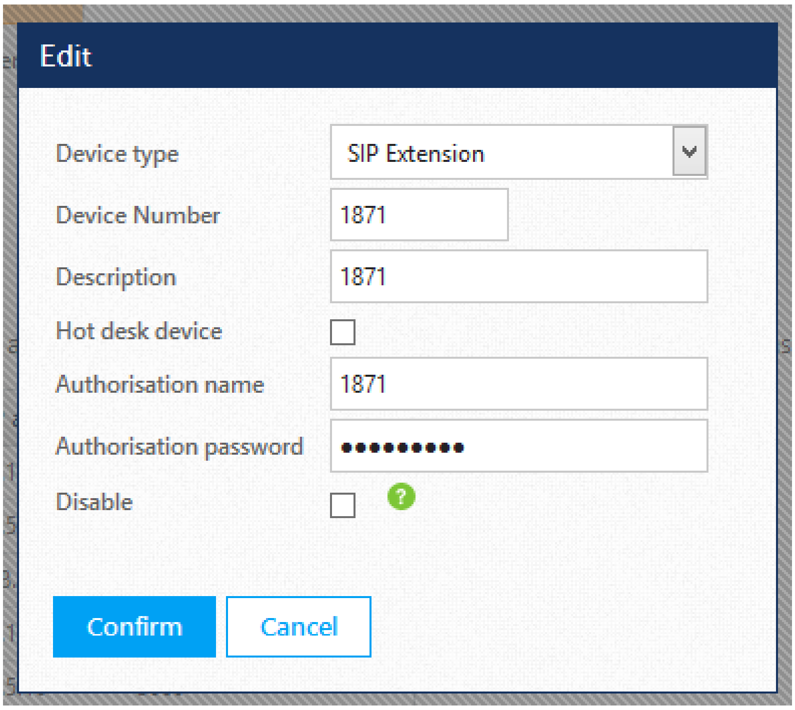
When using a SIP Softphone it is critical that authentication is used to help prevent unauthorized access to the PBX. To configure authentication a username and password need to be set on the PBX for the relevant extension and on device configuration of the Communication Service.

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.



> 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.

> 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.

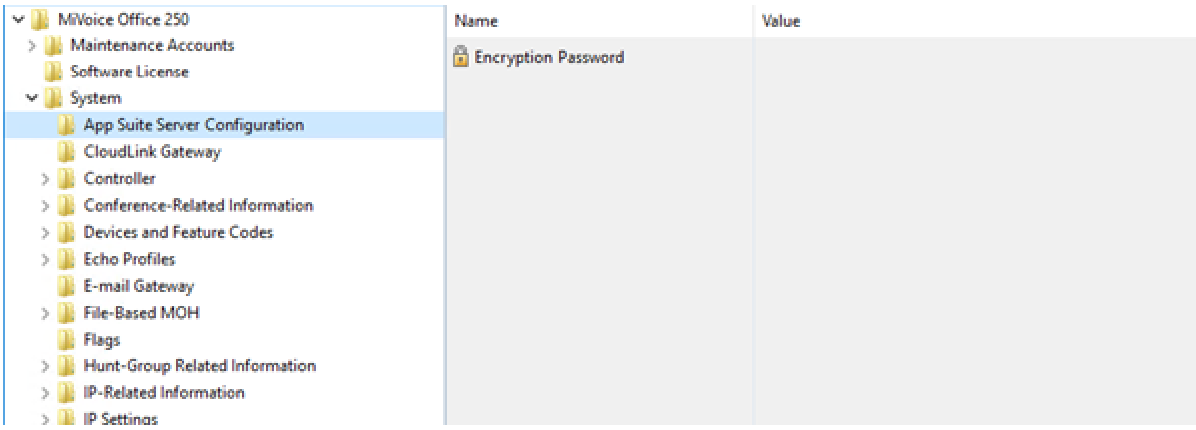
> It is important to connect only one softphone to each extension number on the telephone systems. Registering more that one SIP extension with the same credentials at the same time is not supported by the telephone system and will cause problems.
>
> If using the desktop and mobile versions of Phone 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.

App Suite Server Configuration

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 MVO 250 Database Programming has been created:



Encryption Password

On each node in the MVO 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 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 5.0.62 or higher is also required for the SIP authorization credential query to work.

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:

- 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:

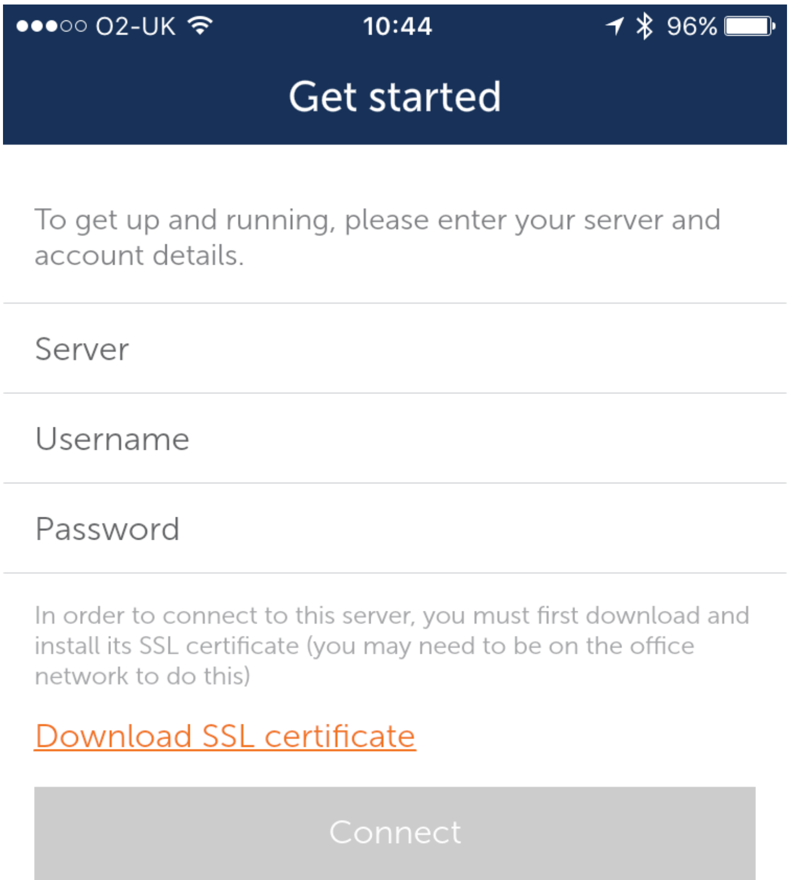
- Their username and password for accessing MCS. This may be their Domain user account (in format DOMAIN\username) or an MCS username and password.
- A valid network on their iOS device, Ideally they will be on the same network as the MCS Server.
- The IP address / Hostname of the MCS server. If connected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

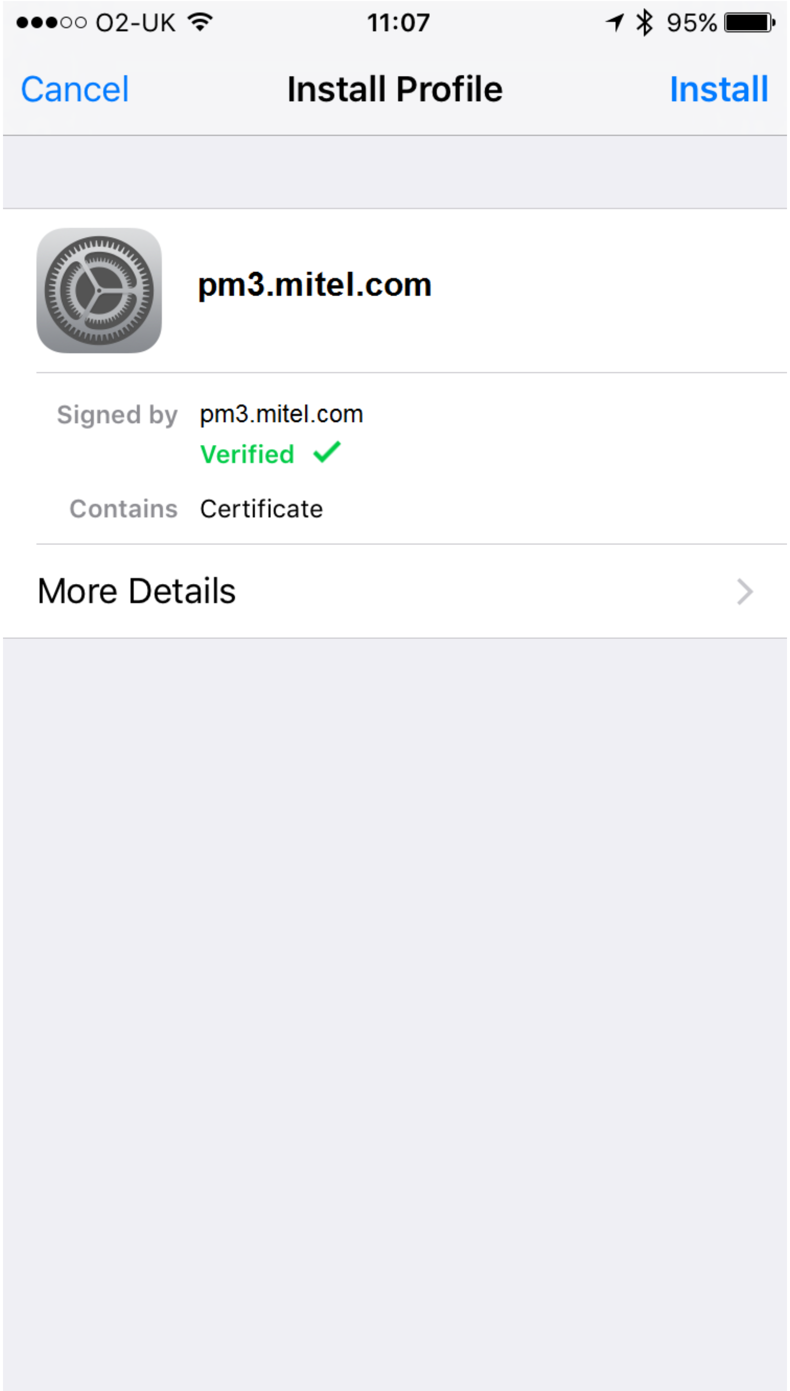
Installation Steps

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 connecting:

- 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 labeled '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:

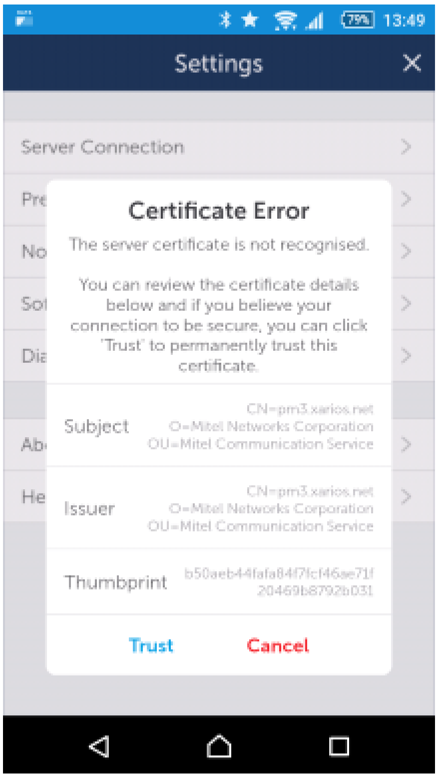
- Their username and password for accessing MCS. This may be their Domain user account (in format DOMAIN\username) or an MCS username and password.
- A valid network on their device, Ideally they will be on the same network as the MCS Server.
- The IP address / Hostname of the MCS server. If the user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

The use of port forwarding is not recommended when using the Phone Manager Desktop Softphone. A VPN or MBG connection should be used instead.

The use of port forwarding is recommended when using Phone Manager Mobile Softphone due to there being no need to forward SIP traffic through. The only SIP traffic is between the MCS server and the 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. This MBG can be used in conjunction with Phone Manager clients and softphones but is not a requirement.

The MBG provides additional security over Port Forwarding when using Phone Manager Desktop Clients/Softphones.

The MBG does not provide any additional security over Port forwarding when using Phone Manager Mobile/Softphone.

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	Outbound	Used to communicate to the MCS server to provide configuration, user data, chat etc.
TCP 8190*	MCS Server	Outbound	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 ⚙ -> 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
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.
City / locality	Name of the city where your organization is registered/located. Do not abbreviate.
Country	The country where your organization 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 -> 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

Powering connections

mitel.com