Mitel Communication Service & Phone Manager Desktop 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 Introduction

About this Document

This document is designed for administrators who need to install or upgrade the Mitel Communication Service and Phone Manager applications in association with Mitel MiVoice Office 250.

Chapter 1 provides a brief introduction and overview of the Communication Service and Phone Manager products.

Chapter 2 describes installation procedures for the Communication Service software.

Chapter 3 describes installation procedures for the Phone Manager Client software.

Chapter 4 includes engineering guidelines on configuring Phone Manager Softphone and Remote Connections

Introduction

Mitel Communication Service is a Microsoft Windows © software application that connects to the MiVoice Office 250 PBX Open Architecture Interface (OAI) and, as well as providing various features, is the server for the Phone Manager UC and CTI client software application.

The software maintains a Microsoft SQL© database and can be configured using a browser and automatically maintains sync with the PBX as DB Programming changes are made.

The objective was to design a server application that is simple to install and configure and maintains a low cost of ownership for the end user.

About the Communication Service & Phone Manager

The Mitel Communication Service is a server-based software application that provides the following features:

- Supports Phone Manager Desktop and Mobile UC clients
- Manages user's device status using Presence Profiles
- Provides dialer features through MiContact Center Office Campaign Manager
- Provides call logging and reporting features through MiVoice Office Call Reporter
- Provides call recording features through MiVoice Office Call Recorder
- Group Messaging
- Agent Hot Desking
- Alarm Notification

The applications are specifically designed for the MiVoice Office 250 to improve desktop interaction with the telephone system for the user.

Communication Service

The Communication Service runs as a combination of a website, a desktop administration tool, a SQL Server database and seven windows services.

1. Website:
    - Provides an administrative interface for configuring the application features and settings
    - Provides status information and historical event tracking for the solution
2. Desktop Administration Tool:
    - Provides a way to edit the SQL connection details
    - Provides a way to check and perform manual DB updates
3. SQL Server:
    - Stores all configuration information
    - Stores historical call and Chat history for users

4. MCS Watchdog Service:
    - Controls automatic database updates post installation
    - Controls the status of all other services
5. MCS CTI Host Service:
    - Proxies connections for Phone Manager Clients and the Logger Service to the MiVoice Office 250
    - Implements Agent Hot Desking, Group Messaging & Alarm Notification features
6. MCS Logger Service:
    - Logs all internal and external calls made by all devices on the system to the SQL database
    - Handles the recording of telephone calls via RAC and IP/SIP Extension Side port mirroring.
7. MCS DB Service:
    - Manages database archiving and database backups
8. MCS WCF Service:
    - Provides configuration information from the database to all services and the website
9. MCS Gateway Service:
    - Provides integration service support
10. MCS Campaign Manager Processor:
    - Manages the imports, exports and reports for the Campaign Manager
11. MCS SIP Proxy
    - Manages SIP registrations for Phone Manager Mobile Softphones
12. MCS Reporting
    - Processes all reports run through the website or through schedules.
13. MCS Call Archiver
    - Processes all call recording archive routines to local and network shares.

> Direct connections to the MCS SQL database are not supported. The database structure will change with version upgrades. Customers accessing the database directly will not be supported.

Phone Manager Desktop

Mitel Phone Manager is a windows desktop client application that provides complete control of your MiVoice Office 250 Extension. The application is designed to give users easy access to the core MiVoice Office 250 features and enhance them by providing:

- Real-time status visibility of other users on the system
- Control of personal presence including control of Dynamic Extension Express
- Access to global and personal directories
- Chat between Phone Manager users
- Access to personal and group voicemail boxes
- Integration to Microsoft Outlook and other third party applications
- Access to call history
- Softphone mode that allows Phone Manager to be an extension on the MiVoice Office 250 system

Phone Manager is available in four different license levels; Standard*, Outlook, Professional & Team Leader. Each license level offers an increase in features over the previous level

> * Phone Manager Standard is not currently available to purchase

Phone Manager Mobile

Mitel Phone Manager Mobile for iOS and Android provides the following features:

- Snap-shot status visibility of other users on the system
- Control of personal presence including control of Dynamic Extension Express
- Access to global and personal directories
- Chat between Phone Manager users
- Access to call history
- Softphone mode that allows Phone Manager to be an extension on the MiVoice Office 250 system.

Licensing

The Communication Service is licensed via a software key. The key contains all licenses required for the server application and the Phone Manager Client applications.

To license the software an internet connection is required. The license can either be applied online through the software or offline via file transfer if the server running the Communication Service does not have access to the internet.

For more information please review the Initial Configuration section.

> Offline activations can be completed using a file transfer to the Mitel Communication Service website www.mitelcommunicationservice.com

2 Installation

System Requirements

The server(s) must meet the minimum requirements described here.

Operating Systems

- Windows 7 Pro/Enterprise/Ultimate 64-bit
- Windows 8.1 Pro 64-bit
- Windows 10 Pro/Enterprise 64-bit
- Windows Server 2008 R2 Standard/Enterprise/Datacenter 64-bit
- Windows Server 2012 R2 Standard/Datacenter 64-bit
- Windows Server 2016 Standard/Datacenter 64-bit

> From release 5.0, Mitel Communication Service is supported on 64-bit operating systems only.

> Windows Server Core installations are not supported.
> Windows Server Small Business/Foundation/Essential versions are not supported.

Hardware Requirements

The minimum required hardware is dependent on the call rate, the number of Phone Manager clients that will be connected and the Application Suite features in use.

Select the size of system which will cover all of the systems limits.

System Limits	Hardware Requirements
Small: • 1,200 calls per hour • 50 Phone Manager Desktop Clients • 50 Phone Manager Mobile Clients (up to 5 softphone calls in progress) • 8 Concurrent Call Recordings	• CPU: 1 x Intel dual core Core i3 @ 3.3 GHz • RAM: 4GB • HDD: 100GB + 1GB for each million call records • HDD: 1TB for each 175,000 hours of call audio data (Only applies when using MiVoice Office Call Recorder) • SQL Server: Express
Medium: • 2,400 calls per hour • 100 Phone Manager Desktop Clients • 100 Phone Manager Mobile Clients (up to 10 softphone calls in progress) • 60 Concurrent Call Recordings	• CPU: 1 x Intel quad core Xeon @ 3.1 GHz • RAM: 8GB • HDD: 100GB + 1GB for each million call records • HDD: 1TB for each 175,000 hours of call audio data (Only applies when using MiVoice Office Call Recorder) • SQL Server: Express • NIC: 1Gb
Large: • 4,200 calls per hour • 500 Phone Manager Desktop Clients • 250 Phone Manager Mobile Clients (up to 25 softphone calls in progress) • 250 Concurrent Call Recordings	• CPU: 2 x Intel quad core Xeon @ 3.1 GHz • RAM: 16GB • HDD: 100GB + 1GB for each million call records • HDD: 1TB for each 175,000 hours of call audio data (Only applies when using MiVoice Office Call Recorder) • SQL Server: Full • NIC: 1Gb

⚠ If a Teamed NIC is present on the server do NOT use this for licensing, Licenses the software against a physical NIC's MAC address only.

Software Requirements

The following software is required to be installed:

- Microsoft .NET Framework 3.5 SP1
- Microsoft .NET Framework 4.5.2
- Windows PowerShell 1.0

> The Mitel Communication Service can not be installed on a Domain controller or Small Business Server

Virtualization Environments

Mitel Communication Service is supported in a virtual environment. The supported environments are listed in the table below.

Environment	Supported?
VMWare vSphere ESXi v5.1, v5.5, v6.0	✓
Hyper-V 2008 R2, 2012 R2, 2016	✓

Co-Hosting with Xarios Call Recorder

If the MCS is being installed on the same server as a Xarios Call Recorder, it is advisable to change the following settings so that there are no clashes between the products:

Website Port

By default, both products will host their websites on port 80. To access the products individually, one of the websites must be reconfigured within IIS to use a different port. The website can then be accessed by appending the port to the URL:

http://[server_name]:81

> Be aware that the port will be reset to 80 after by any upgrade applied to the system.

Database Backup & Log Archive Directories

By default, both Xarios Call Recorder and MCS use the same folders for database backups and log archives. Both of these locations need to be changed otherwise files will be overwritten.

PBX Supported Versions

The following Mitel MiVoice Office 250 versions are currently supported:

- Call Processing Version 6.1.x
- Call Processing Version 6.2.x

The following Multi-Node configuration is supported:

- Multiple MiVoice Office 250 nodes via the use of a Mitel CT Gateway.
- Individual connections to multiple Mitel MiVoice Offices are not supported.
- Unique numbering plan across all nodes is required (this includes Trunk devices).

The following pre-requisites must be met on the telephone system:

- System OAI Call Control & 3rd Party Event enabled
- IP Based OAI Connection

The following requirements must be met if using desktop or mobile Phone Manager Softphones:

- Cat F licenses are required for each connected softphone device.

The following requirements must be met if using the MCS Record-A-Call feature:

- SIP Voicemail licenses are required on the MiVO 250 to match the number of concurrent calls to be recorded (Maximum of 8).

> ⚠ Only one SIP voicemail can be configured by default on the telephone system. If you are using NuPoint Messaging then the MCS will not be able to be added as a SIP Voicemail.

> If using Phone Manager Mobile Softphone then the relevant SIP extensions need to be configured to use G.711

> 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.

Installing the Communication Service

There is a single installation package that contains all components of the Communication Service.

> ⚠ Do not install the Communication Service from a network share. Copy it to a local drive first to ensure any prerequisites are installed correctly by the operating system.

> ⚠ If installing MCS on Windows 7 or 8 then .NET 3.5 must be installed prior to installing MCS. If not, the Pre-Requisites installation will failed stating it has been 'interrupted'.

> If a previous version of Communication Service is already installed the new version can be installed over the top.

To install the Communication Service:

1. Run the setup file and follow the on screen instructions (As part of the install additional Microsoft elements maybe installed. See software requirements for a detailed list).

   > If the setup prompts to restart during the process then allow the restart and re-run the installation afterwards.

2. The first prompt will ask you to select the language preference. Select the country where the server is to be located from the drop down menu and press '*OK*'.
3. If Microsoft SQL Server 2014 is not already installed, the setup will prompt to install. Follow the on screen instructions.

   > At this point please be patient, the installation of SQL Server can take over 30 minutes to complete.

4. Once the SQL installation has completed the installation of the Communication Service will automatically start.
5. Accept the License Agreement and complete the User & Organization section.
6. On the '*Setup Type'* screen select '*Complete'* and press '*Next'* to continue installation.

   > You may be presented with a confirmation form to indicate other applications need to be closed

before the setup can continue.

To configure Communication Service once the installer has finished two things will happen:

1. A web page will be displayed to guide you through the initial configuration process.
2. The Watchdog service will start automatically and will begin upgrading the database structure.

Before the initial configuration process can be started the Watchdog must have finished the database update process. Please wait for this to be completed.

The default login details for the Communication Service are: engineer / Teleph0ny!

If a site is being upgraded from a previous release of MCS, it will continue to use SQL Server 2008 R2. There is no requirement to upgrade the version of SQL beyond 2008.

Initial Configuration

The first time the MCS website is accessed it will guide the user through the Installation Wizard. The wizard covers the following configuration options:

- Licensing
- User Creation
- PBX Configuration
- Dial Plans
- Call Recording (If licensed)
- Email

All of these configuration options can be changed at any point after the wizard has been completed, but we always recommend using the wizard for initial setup.

Licensing

Mitel Communication Service needs to be licensed before it can be configured and be made operational.

To license a Mitel Communication Service you will need :

- Site ID and Serial number, this will be provided on the license certificate for the software when purchased.
- Reseller ID

The reseller ID is only requested when the license being installed is a stock license. It is requested so that the license is correctly registered to a reseller account on the Mitel Communication Service portal.

The reseller ID is the same as a reseller's Mitel SAP number. If you do not know your reseller ID, please contact Mitel or visit www.mitelcommunicationservice.com for more information.

Online Activation

If the server MCS is installed on has an internet connection then the software will attempt to activate the license automatically. On the licensing screen you will be prompted for the following:

- Site ID & Serial Number
- Site name
- MAC Address

The license will be linked to the MAC address of the server which you select. If the software has been installed in a VMWare or Hyper-V environment, make sure the MAC address is static.

> If the server that MCS is being installed on is using a proxy then the link to the license server might be blocked.
> The license server is accessed by MCS using HTTPS on port 443

Offline Activation

If the server the software is installed on does not have an internet connection then an offline activation will be required. This involves entering the same information required by the online activation but instead of the information being passed automatically to the license server it is saved in a license request file. This file then needs uploading to the Mitel Communication Service license portal (www.mitelcommunicationservice.com). The file can be transferred to another server or PC that does have internet access. Once the license request file has been processed on the portal a license activation file will be provided. This license activation file needs to be loaded into the MCS website to complete activation.

Offline Activation Through Wizard

1. Select the 'Activate offline (no internet connection)' option at the top of the wizard's license page
2. Select the license type as required
3. Enter the required information in the displayed fields
4. Following 'Step 1' by clicking the link to download the license request file. Save the file and make a note of the file name and location
5. Copy the file to a computer with an internet connection and browse to http://mitelcommunicationservice.com/activate and upload the license request file.
6. Save the license activation file returned and copy it back to the server running MCS
7. Follow 'Step 3' and upload the license activation file to complete the activation of MCS

Offline Activation Through License Page

1. On the Server License page press the 'Activate' button
2. Select the license type as required
3. Enter the required information in the displayed fields
4. Click the 'Download file for offline activation' on the bottom right activation form. Save the file and make a note of the file name and location
5. Copy the file to a computer with an internet connection and browse to http://mitelcommunicationservice.com/activate and upload the license request file.
6. Save the license activation file returned and copy it back to the server running MCS
7. On the Server License page press the 'Process files' button and browse to the activation file to complete the activation of MCS

> ⚠ If a Teamed NIC is present on the server do NOT use this for licensing, License the software against a physical
> NIC's MAC address only.

Phone System Configuration

To operate the MCS you must have a System OAI connection to the phone system. To aid in configuring this connection the wizard will broadcast and will try and find any phone systems or CT Gateways on the local network segment. This will appear in a box on the right hand side of the screen. If the broadcast finds a single system or a CT Gateway it will pre populate the connection details on the left hand side.

Once the correct PBX configuration details have been entered, press the *Next* button to test the connection. If the connection is successful the wizard will download the device configuration from the MiVoice Office 250.

For more information on the Phone System settings, please reference the Phone Systems section.

Dial Plans

The dial plans control how Phone Manager clients will initiate external calls on the MiVoice Office 250. The wizard should pre-configure the *Country* selection and the *Outside line* so only the following fields should need to be edited:

- DID Prefix to Add
- Local area codes
- Local override codes

For more information on the dial plan settings, please reference the Dial Plan section.

User Creation

Users are an integral part of the operation of the MCS. They are used for:

- Authenticating Phone Manager clients
- Giving engineers and supervisors access to the MCS website to make configuration changes
- Tracking calls made on the PBX for historical logging purposes

To ensure the system is as easy as possible to use and maintain the correct method for creating users needs to be selected.

For more information please reference the Users section.

Email

Emailing is used when creating manual user accounts, inviting Mobile Client Users and when using the alarm notification features.

For more information please reference the Email section.

Once you have completed the wizard the Mitel Communication Service should be operational.

Network Configuration

The MCS requires a 100Mb/1Gb LAN connection that has access to the telephone system. Phone Manager clients will also need access to the MCS over the network. If the server is installed into a Microsoft Active Directory environment then it should be added to the domain, ideally before the MCS software is configured.

> ⚠ Custom Active Directory Group Policies can adversely affect the system and they should be tested before going live.

To enable users to easily access the server with the website role a valid DNS entry should be created that can then be used when browsing to the server, for example http://communicationserver.

The table below details a list of firewall ports that may need to be opened. Which ports will depend on the features and system configuration.

Application	Name	Direction	Port
Licensing	HTTPS/SSL	Outbound (service.xarios.com)	TCP 443
Website access	HTTP	Inbound	TCP 80
Secure website access	HTTPS/SSL	Inbound	TCP 443
SQL Server	SQL Server	Inbound/Outbound	TCP 1433
Communication Gateway	Integration Services	Inbound	TCP 8188
Communication Service	Phone Manager Desktop Clients	Inbound	TCP 8187 & TCP 8186
Communication Service	Phone Manager Desktop Clients - CTI	Inbound	TCP 2001
Communication Service	Server Connections	Inbound/Outbound	TCP 8189
Communication Service	Broadcast location service	Inbound	UDP 8184
Communication Service	Phone Manager Mobile	Inbound	TCP 8185
Communication Service	Phone Manager Mobile Audio	Inbound	TCP 8190
Communication Service (SIP Proxy)	Phone Manager Mobile SIP Audio	Inbound/Outbound	UDP 20000-20500
Communication Service	Google Push Notification Service	Inbound	TCP 5228, 5229, 5230
Communication Service	MiVoice Office 250 OAI	Outbound	TCP 4000
Communication Service	MiVoice Office 250 SIP (RAC Call Recording & Phone Manager Mobile Softphones)	Inbound/Outbound	UDP 5060
Communication Service	MiVoice Office 250 Audio (RAC Call Recording)	Inbound/Outbound	UDP 12000-12100
Communication Service	MiVoice Office Call Recorder Live Streaming	Inbound	TCP 8201

During the installation rules will be added to the in-built Windows Firewall for ports used by the MCS services. When using the Record-A-Call or SIP/RTP recording, the IP address of the PBX (Base server, PEC & PS1) may need to be added to the firewall allowed list to allow traffic into the MCS.

Anti-Virus Recommendations

Anti-virus software can be installed onto the servers, but the following exclusions must be configured:

- Exclude the server logs
  - %ProgramData%\Mitel\Communication Service\logs
  - File extensions to exclude: *.log
- Microsoft IIS 7.0 Server
  - Web Server log files should be excluded from scanning. By default, IIS logs are saved in C:\inetpub\logs
- Disable real time / on demand scanning
- Microsoft SQL Server 2008 R2
  - %ProgramFiles%\Microsoft SQL Server\MSSQL\Data
  - File extensions to exclude: *.mdf,*.ldf, *.ndf, *.bak, *.tm
- %ProgramFiles%\Microsoft SQL Server\<instance name>\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL10_50.<Instance Name>\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL10_50.<Instance Name>\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL10_50.<Instance Name>\OLAP\Bin\MSMDSrv.exe

For servers with the call recording role:

- Disable real time / on demand scanning
- Exclude the recording paths (default path shown)
  - C:\Recordings (or D:\Recordings if there is a 'd' drive)
  - Local <Archive Location>

If a support issue is raised then the removal of the anti virus may be required to aid in any diagnostics.

3 Client Installation

System Requirements

To be able to install and run Phone Manager the client computer needs to meet the following **minimum** requirements. If installing into a multi user environment where multiple instances of the client will be running, for example Microsoft Terminal Service, Citrix etc. then see the Multi User Computer Requirements section.

> The Call Recorder Client is embedded within the Phone Manager installation. It has the same requirements as Phone Manager.

Operating Systems

- Windows 7 Pro/Enterprise/Ultimate 32-bit/64-bit
- Windows 8.1 Pro 32-bit/64-bit
- Windows 10 Pro/Enterprise 32-bit/64-bit
- Windows 2008 SP2 Standard/Enterprise/Datacenter 32-bit/64-bit
- Windows 2008 R2 Standard/Enterprise/Datacenter 32-bit/64-bit
- Windows 2012 Standard/Datacenter 64-bit
- Windows 2012 R2 Standard/Datacenter 64-bit

> The Windows 2008 or Windows 2008 R2 Server Core installation options are not supported.
>
> The Windows 2012 Foundation and Essential versions are not supported.

Hardware Requirements

Processor	Intel Core 2 Duo 1.8GHz or faster processor (or equivalent)
Memory	Minimum: 1GB RAM Recommended: 2GB RAM or more When Phone Manager is running it will use a minimum of 70MB of RAM per client. (Terminal environments) - this can be significantly more depending on configuration and number of devices and/or users on the system.
Network	IPv4, 100Mb / 1Gb LAN
Hard Disk	Minimum: 20GB free space
Video	Minimum: DirectX v9 compatibly graphics cards with 120MB RAM Recommended:DirectX v9 compatibly graphics cards with 1024MB RAM

Software Requirements

The following software is required to be installed.

- Microsoft .NET Framework 4.5
- Windows Installer 4.5

Multi Users & Virtual Desktop System Requirements

Phone Manager can be run in multi user and virtual desktop environments such as Microsoft Terminal/Remote Desktop Services, Citrix XenApp or VMWare Virtual Desktop Infrastructure (VDI) with the following limitations:

- The 1st Party TAPI drivers is not supported
- Phone Manager Softphone is not supported

When deploying in these environments, the amount of memory, CPU usage and Video resource that Phone Manager will use needs to be determined. As the resources required are dependent on configuration and the number of devices and Users in the system, you must exercise your own due diligence in reviewing, planning, implementing and testing a customer configuration.

There are options available on the Advanced tab in the Client Profiles section that can reduce the performance requirements for Phone Manager.

The Phone Manager installation is available in two versions, 32 bit and 64 bit. Ensure you use the correct version for the operating system you are running.

> ⚠ Do not install Phone Manager from a network share. Copy it to a local drive first to ensure any prerequisites are installed correctly by the operating system.

> ⚠ The installation package may request a restart of the computer depending on the packages that need to be installed.

> If a previous version of Phone Manager is already installed the new version can be installed over the top.

1. Run the correct client setup file for the PC and follow the on screen instructions (As part of the installation additional Microsoft elements maybe installed. See software requirements for a detailed list).

   > If the setup prompts to restart during the process then allow the restart and re-run the installation afterwards.

2. Accept the License Agreement, Softphone Agreement and complete the User & Organization section.
3. On the '*Setup Type'* screen make a selection between '*Typical*, *Complete* or *Custom'* and press '*Next'* to continue installation.
   - Typical - Installs most common Phone Manager components, excludes TAPI driver and Headset integration support
   - Complete - Installs all Phone Manager features
   - Custom - Allows the installer to choose which features to install
4. Select the client location options based on whether the PC will be moving around (laptop) and whether the current location is local to the office or remote.
5. If required enter the connection details for the Communication Service and local extension number If the Communication Service is on the same LAN segment this can be left blank, Phone Manager will send a broadcast to attempt to it.

The installation should now complete, all the user has left to do is enter their login credentials to connect.

Call Recorder Client

The Call Recorder Client is contained within the Phone Manager Desktop installation. If the *Typical* setup type is used the Call Recorder Client is NOT installed. The *Complete* or *Custom* setup type must be used to install the Call Recorder Client.

Unattended installations of just the Call Recorder Client are possible, please see the Unattended Installations section for more information.

There are various techniques to enable rapid deployment of Phone Manager or deployment on a large scale:

- Active Directory Group Policy
- Login Script

The choice of deployment method will depend on the customer's infrastructure and experience. Whichever method is chosen the customer will need to use the setup / msi command-line arguments to perform a silent installation and pass the necessary configuration information for a unattended installation.

The Phone Manager installations are MSI based installations that are embedded inside an executable that will ensure

the prerequisites are installed correctly.

Active Directory Group Policy

To roll out Phone Manager using group policy the MSI must first be extracted from the setup executable. To do this the following command-line arguments need to be passed to the executable:

setup_phonemanager_exex64_vX.X.XXXX.X.exe /a /s /v"/qn TARGETDIR=\"C:\Temp\""

The TARGETDIR can be replaced with any location, this will be where the MSI file is extracted to. The executable name in the example above needs to be replaced with the executable version being used.

The extracted MSI is called setup.msi. This process will have to be repeated for both 32bit and 64bit versions if required. Take care to use a different TARGETDIR for the 32bit and 64 bit versions as they will both generate an MSI with the same name, i.e. setup.msi.

When installing using the MSI package, ensure that .NET 3.5 SP1 & .NET 4.0 Extended is installed.

When installing using the MSI package, headset packages for Jabra and Plantronics need to be installed separately

Command-Line Arguments

The following command-line arguments can be passed to the executable or MSI to customize the installation.

Silent Installation

Used to ensure the end-user does not see any part of the installation while it is in progress.

/S /v/qn

Server Location

Used to specify the location of the Communication Service during the installation. This can be the IP address or hostname.

/VXDISCOVERYSERVER=

If no location is passed, Phone Manager will broadcast to find the server on start-up.

Extension Mapping Type

The options detailed in the table below are used to specify one of the three extension mapping types:

Parameter	Description	Usage
dynamicwithendpoint	Use the extension assigned to the computer, each different user that sits at the computer uses the same extension. If no extension is supplied using a '/VXENDPOINT' parameter, then an extension for the computer is prompted for and saved the first time Phone Manager is run.	User of Agent Hot Desking or general ACD users that move between phones.
static	Use the extension assigned to the User on the Communication Service. If no extension has been assigned to a user centrally then they will be prompted and have one assigned the first time they log in.	Users of native Hot Desking or people that sit at the same desk every day.
dynamic	Prompts the user for an extension each time Phone	Users of Terminal Services or

	Manager starts up.	thin clients where there is no correlation between the Phone Manager UI and the extension.

/VXENDPOINTMAP=dynamicwithendpoint

or

/VXENDPOINTMAP=static

or

/VXENDPOINTMAP=dynamic

Extension Number

Used to define the extension number for the computer during installation.

/VXENDPOINT=XXXX

Features

The options detailed in the table below are used to control the various features that can be installed. By default if no features are passed to the installation the features in **bold** will be installed.

Feature Name	Description
Client	Core Phone Manager Software.
Outlook	Phone Manager Outlook plug in Software.
Shortcut_Startup	Shortcut for Phone Manager in the start up folder.
Shortcut_Desktop	Shortcut for Phone Manager on the desktop.
TAPIx64	Phone Manager TAPI driver for 64bit systems.
TAPI	Phone Manager TAPI driver for 32bit systems.
URLProtocolsx64	Sets Phone Manager as the target for “tel://, dial://, callto://, sip://, dialfrompm://” URI’s in the Client PC Registry. When set, any telephone number (formatted with one of the supported URI’s) in a web page will use Phone Manager to dial the number when clicked.
URLProtocols	Sets Phone Manager as the target for “tel://, dial://, callto://, sip://, dialfrompm://” URI’s in the Client PC Registry. When set, any telephone number (formatted with one of the supported URI’s) in a web page will use Phone Manager to dial the number when clicked.
Plantronics	Support for manufacturer specific headsets.
CallRecorderClient	Installs the Call Recorder Client to control muting of recordings

To Add:

/VADDLOCAL=*featurename*

Removing Features:

Features cannot be individually removed once installed. To remove features the entire application must be uninstalled.

> ⚠ All feature names are case sensitive

> On initial install the *Client* feature must always be installed

> If no feature parameter is passed all features are installed except TAPI and headset support

Command-Line Examples: Executable

Silent Installation

Setup.exe /S /v/qn

Silent Installation with TAPI and Jabra Headset on 64bit

Setup.exe /S /v/qn /VADDLOCAL=TAPIx64, JABRA

Silent Installation with Server Location

Setup.exe /S /v/qn /VXDISCOVERYSERVER=192.168.100.2

Silent Installation with Server Location and Extension Mapping

Setup.exe /S /v/qn /VXENDPOINTMAP=static /VXDISCOVERYSERVER=102.168.100.2

4 Engineering Guidelines

The following section provides engineering guides on various aspects of the solution:

- Phone Manager Softphone (Desktop & Mobile)
- Remote Connections (VPN, MBG, Firewall)
- Backup & Restore Procedures
- Using a Certificate Authority Certificate

4.1 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 = Yes (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 Authorization 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.

> ⚠ Authorization 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:

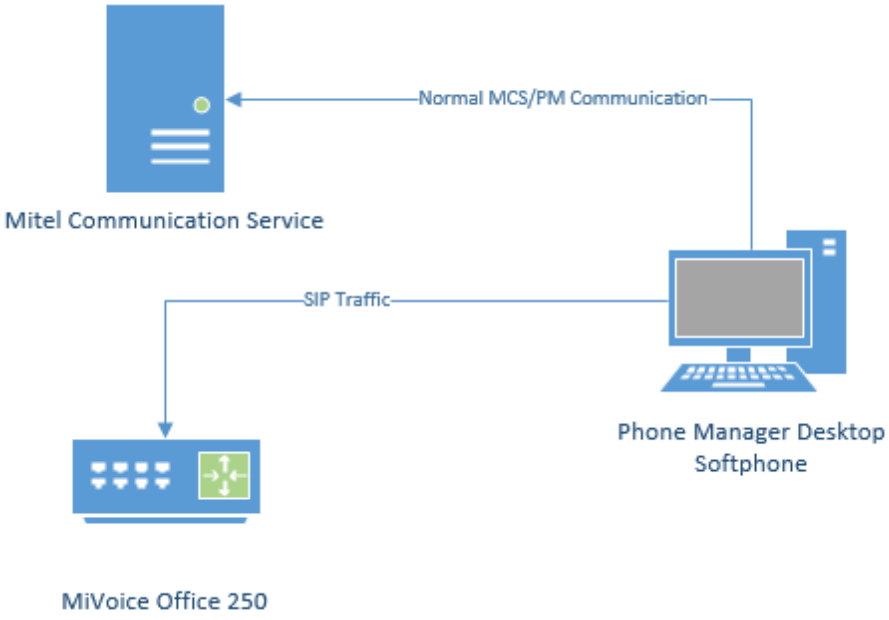
- On the MCS website, browse to "Configuration -> Site Settings -> Phone Systems -> <*PBX NAME*>"
- Locate the Nodes section at the bottom of the screen
- Edit each node and put in the Local & Remote IP address and port numbers for SIP (For remote, the IP address / Port will be those of the Router or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

MCS now knows the authorization 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:

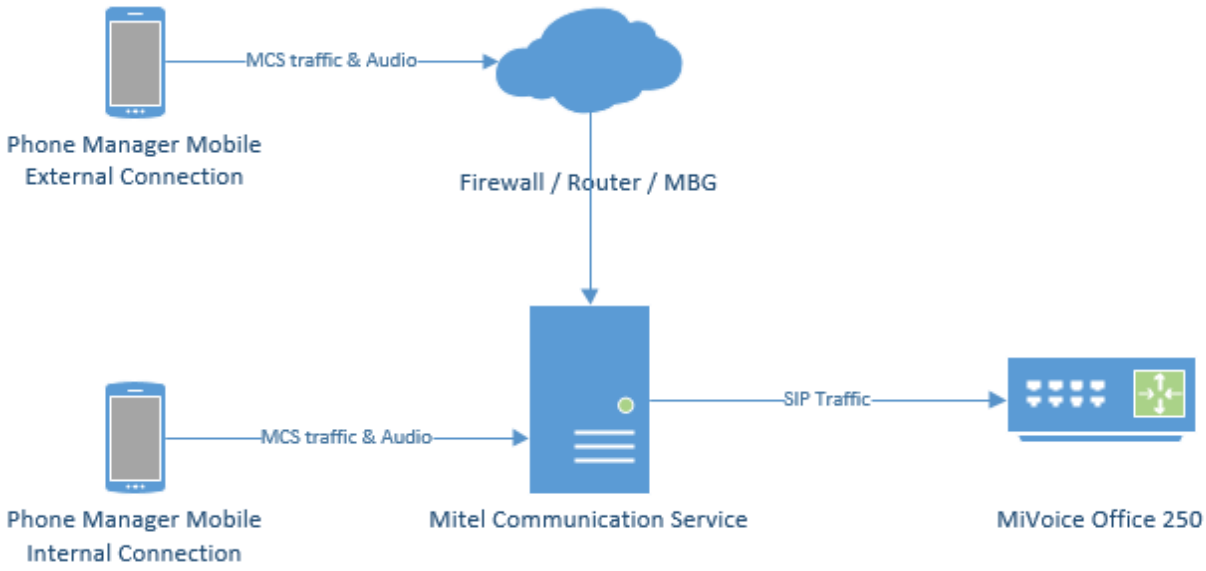
- Connecting Phone Manager Desktop using a MiVoice Border Gateway
- Connecting Phone Manager using a Router

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.

4.2 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.

4.2.1 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

4.2.2 MiVoice Border Gateway

When a Mitel Border Gateway is being used on the telephone system for remote connections there are certain configurations that must be made in order to allow Phone Manager Desktop, Phone Manager Mobile and Phone Manager Softphone connections to pass through it.

For information on the programming required, review the following sections:

- Mitel Border Gateway with Phone Manager Desktop
- Mitel Border Gateway with Phone Manager Mobile

4.2.2.1 MiVoice Border Gateway with Phone Manager Desktop

Phone Manager Desktop can be used remotely, connecting back to the Mitel Communication Service through a MiVoice Border Gateway (MBG).

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

Port	Target	Direction	Description
TCP 8187 & 8186	MCS Server	Outbound	Used to communicate to the MCS server to provide configuration, user data, chat etc.
TCP 8188	MCS Server	Outbound	Integration Services, only required if client access to the server-side API is required
TCP 2001	MCS Server	Outbound	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.

MiVoice Border Gateway Configuration

Complete the following configuration on the MBG:

- On the MBG Security -> Port Forwarding page create the following port forwarding rules 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	8187	172.19.22.49	8187	Yes	Remove
TCP	8186	172.19.22.49	8186	Yes	Remove
TCP	8188	172.19.22.49	8188	Yes	Remove
TCP	2001	172.19.22.49	2001	Yes	Remove

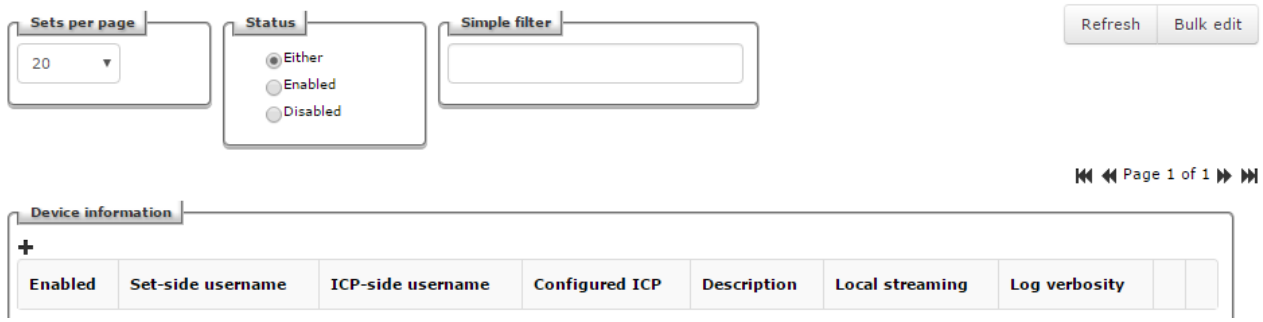
⚠ Do not Port Forward port 5060, use the SIP configuration outlined below

If using a Softphone then configure the SIP device:

- In the MiVoice Border Gateway -> Service Configuration -> SIP Devices add the required SIP device by pressing the + button below the Device Information label and configured the following settings (in this example the extension number is 1880 and password that has been configured against the device on the telephone system is m1t3l!, replace these values accordingly):
  1. Enable = True
  2. Set-Side username = In-bound authentication username (1880)
  3. ICP-Side username = In-bound authentication username (1880)
  4. Configured ICP = PBX the SIP extension is configured on
  5. Set-Side Password = In-bound authentication password (*Mitel*Server1!*)
  6. Confirm Set-Side Password = In-bound authentication password (*Mitel*Server1!*)
  7. ICP-Side Password = In-bound authentication password (*Mitel*Server1!*)

8. Confirm ICP-Side Password = In-bound authentication password (*Mitel*Server1!*)

> This will require a Teleworker license on the MBG



> For more information on configuring Remote Softphone connections, see here.

Phone Manager Desktop Configuration

To connect a the Phone Manager Desktop remotely, open the Settings page configure the following settings:

- General
    1. Default Location = Remote Connection

- Remote Connection
    1. Host Address = External IP Address of the MBG
    2. Override login details = true
    3. Username = MCS Username
    4. Password = MCS Password
    5. Extension details = User Preferred Method

MiVoice Office 250 Configuration

For Phone Manager Softphones connecting through an MBG, the following setting needs enabling against the SIP Peer on the telephone system:

- Use Registered Username
- NAT Address Type = Native

With both MBG, phone system and Phone Manager configuration complete the application should be able to connect remotely.

4.3 Upgrades, Backups, Restoring & Rollback Procedures

The MCS system has various persistent data stores which should be backed up on a regular basis to minimize the risk of data loss through hardware or software failure.

The following sections outline the places where MCS stores data and the processes that should be followed to:

- Create regular backups of the system.
- Perform pre-upgrade backups.
- Restore to the current or an alternate server using a backup.

The procedures outlined here cover all the data required for the Mitel Communication Service, MiContact Center Office Campaign Manager and MiVoice Office Call Reporter.

For systems using the MiVoice Office Call Recorder features of the solution, only the data associated with calls is backed up using these procedures. Call Archiving must also be implemented to ensure all call recording audio is backed up.

MCS Data Storage Locations

The following elements of the solution need to be backed up, ideally to location which is on different hardware to that which is running the MCS software:

- SQL Databases -> Used to store configuration and Call/Chat history.
- Registry configuration -> Used to store watchdog and database connection settings.
- User files -> User profile images etc.

SQL Databases

The MCS solution uses multiple databases to store configuration, call and chat data. The following table describes each of the databases used by the solution and what is contained within it:

Database	Description
CallRecorder	The working database for the MCS solution. Used to store configuration information (User, PBX), chat history and the call data for the current day.
CallRecorderArchive_1	The first archive DB used by the system, stores historical audit and call data.
CallRecorderArchive_N	Additional archive database where is N is a numeric value which increases over time. New archive databases are created if the time or record limit is reached of the current archive database. For more information please refer to the Database Maintenance section.
CampaignManager	The working database for the MiContact Center Office Campaign Manager solution. Used to store configuration information (schedules, imports, exports etc.), campaign data and the call/user data for the current day.
CampaignManager_Archive	Used to store historical call and user data.

All of these databases are automatically backed up on a nightly basis to the following location; *C:\DBBackups.*

For further resilience it is advised to keep a copy of these backups on hardware different to that which the MCS is running on.

For more information on Database Backups, please refer to the Database Maintenance section.

Registry

The MCS stores a subset of configuration information in the registry. This information includes:

- Server ID -> The unique ID given to the server if part of an MCS network (*For future use*).
- Roles -> Configuration of which roles the server is implementing.
- Watchdog -> Default configuration for the watchdog.

It is wise to back up the following registry location (including sub keys) after the initial MCS installation:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mitel\CommunicationService\Roles]

User Files

MCS stores some data outside the database so as not negatively impact database performance. Currently this is limited to the profile images users upload from Phone Manager Desktop and Phone Manager Mobile clients.

To retain profile images when restoring an MCS solution, ensure the following folder is backed up:

C:\ProgramData\Mitel\Mitel Communication Service\Net Store\ProfileImages

4.3.1 Restore & Rollback Procedures

In some circumstances it may be necessary to restore an MCS installation from backups. Reasons for this include:

- The database has become corrupt
- The hardware MCS is installed has failed
- An upgrade has failed because the system does not have the correct licensing

> ⚠ All of the tasks outlined below require a knowledge of how to use SQL Management Studio. If you are not confident in using this application then please contact Mitel support for guidance.

> To perform any of the database operations outlined here you will need permissions to access the SQL databases. Ensure you connect to the MCS SQL instance using the same user account from which the MCS was first installed.

Restoring MCS Databases

Before restoring the MCS's SQL databases, ensure that all MCS services are stopped. When stopping the MCS services, stop the watchdog service first before stopping any other service. For more information on the services used by MCS, please refer to the 'About Communication Service' section.

Once all the services have been stopped then the database restoring can be started. Using SQL Management Studio, connect to the MCS's SQL instance (usually '127.0.0.1\MCS').

One at a time, click on each for the databases in the SQL instance, right-click and select 'Tasks -> Restore -> Database'.

1. On the form that loads, select the 'Device' radio option and browse to the backup file for this database.
2. Browse to the 'Files' section of the form and double check the database to be overwritten with the backup is the correct one
3. When it has been confirmed that the correct database will be overwritten, browse to the 'options' section for the form and check the box 'Overwrite the existing database (WITH REPLACE)'.
4. Press 'Ok' at the bottom of the screen to start the restore process.
5. Repeat this step for each of the databases in the solution.

> The backups taken by the MCS server are zipped. They will need to be unzipped prior to restoring.

> ⚠ Restoring databases incorrectly can result in data loss. Restoring an SQL database should only be done when backups of all data is in place to restore from. If in doubt, please contact Mitel support for guidance..

> ⚠ Restoring a backup database will result in any new data that have been stored since the backup was taken being lost.

Restoring To A Different Server (if the original server is still accessible)

If the MCS solution needs to be restored to server other than the one it was originally installed then follow these steps:

> ⚠ The next steps involve detaching each of the databases from the original SQL server instance and re-attaching them to the SQL server instance on the new MCS. This can be done using the 'SQL Management Studio' application.

On the existing MCS Server

- On the existing server, make note of the Site ID and Serial number of the software. This can be found on the Server License section of the MCS website.
- Deregister the software, refer to the Server License section for more information

- Make a copy of the contents of the 'C:\ProgramData\Mitel\Mitel Communication Service\Net Store' folder from the old server.

On the new MCS Server

- Install and register MCS on the new hardware (or virtual environment).
- Stop all MCS services on the new server.
- Copy the SQL backups from the old server to the new server
- Follow the restore process above to restore all databases
- Copy the contents of the 'C:\ProgramData\Mitel\Mitel Communication Service\Net Store' from the old server to the new.
- Restart the MCS Watchdog service.

At this point the MCS should be back up and operational as it was on the old hardware.

Restoring To A Different Server (if the original server has failed)

If the server running MCS has failed, follow these stops to re-install the MCS on new hardware:

- Locate the original certificate used to install the MCS (the Site ID / Serial number will be needed)
- Contact Mitel support and explain what has happened. Request that the license be reset so that it can be reused on another server.
- Install the MCS on the new hardware and use the original certificate information to license it

At this point, the MCS should be installed and licensed. If there are backups of the original MCS then the normal restore procedure can be followed from this point. If there are no backups available then the MCS must be reconfigured as a new installation.

Rolling Back An Upgrade

If an upgrade MCS server is not working has required then the software can be rolled back to a previous version (this process assumes that all necessary backups were taken before upgrading). Follow these steps:

- Uninstall the MCS software from the server.
- Re-install the version of MCS software you wish to rollback to.
- Stop all MCS services (stop the watchdog first otherwise it will restart other services).
- Follow the database restore process outline above.
- Start the MCS Watchdog service.

At this point the MCS should be returned to the state it was in before the upgrade.

⚠ When rolling back the software, any data stored since the upgrade will be lost. This includes call recordings.

⚠ Rolling back the software without restoring the database can cause the system to be unstable. This can be because there are new database elements that the rollback version of software does not know about.

4.3.2 Upgrading

The following section outlines the steps that should be taken to successfully upgrade MCS to a later version.

1. Apply license upgrades and Make a note of license details
2. Perform Database Maintenance (including backups)
3. Run the upgrade installation

Applying License Updates

If the version number of MCS is being upgraded then it is important to apply licenses updates before the software is upgraded. This ensures that the license is available and that SWAS is correctly in place before doing any work and will minimize the risk of having to perform a rollback.

A version number upgrade applies to major and minor version of software but not revisions. For example:

4.2 to 4.3 or 4.3 to 5.0 would constitute as a version upgrade.

4.3.1 to 4.3.2 would not constitute as a version upgrade and no license update would be required.

Once any license update has been applied, make a note of the Site ID and Serial number of the solution and the current version that is running. The Site ID and Serial Number can be found on the Server License section of the website. The Site ID and Serial number would be required to re-license the solution if any problems occur with the upgrade. The version number that is running can be found by hovering the mouse of the Mitel icon in the top left hand corner of the MCS website.

Database Maintenance & Backup

Before performing any sort of upgrade it is important that full backups of the solution are taken so that the software can be rolled back to a previous version or restored to another server if required.

Before performing a backup, it is good practice to perform an 'Archive Now' under the Database Maintenance section. This will make sure all call data has been moved to the archive databases.

Once this has been completed, the Backup process can be followed.

Running the Upgrade

When upgrading MCS, it is important to note that the installer will stop all services and all functions of the solution will stop working.

Installation notes:

- There is no need to uninstall a previous version of MCS first, the installation can be run over the top.
- When running the installation, right click on the file and select 'Run as administrator'
- When running the installation, ensure the file is run from the local server and not from a network share.

When running the installation, following the instructions on screen. Once the installation has finished the Watchdog service will automatically be started. The watchdog service will then update the database schema for the solution, this can take some time to complete depending on the size of the MCS databases.

Once the database update process has been completed then the watchdog will restart all the appropriate MCS services and the solution should be operational again.

If for any reason the upgrade fails then the Rollback process can be followed to return the system to it's previous state.

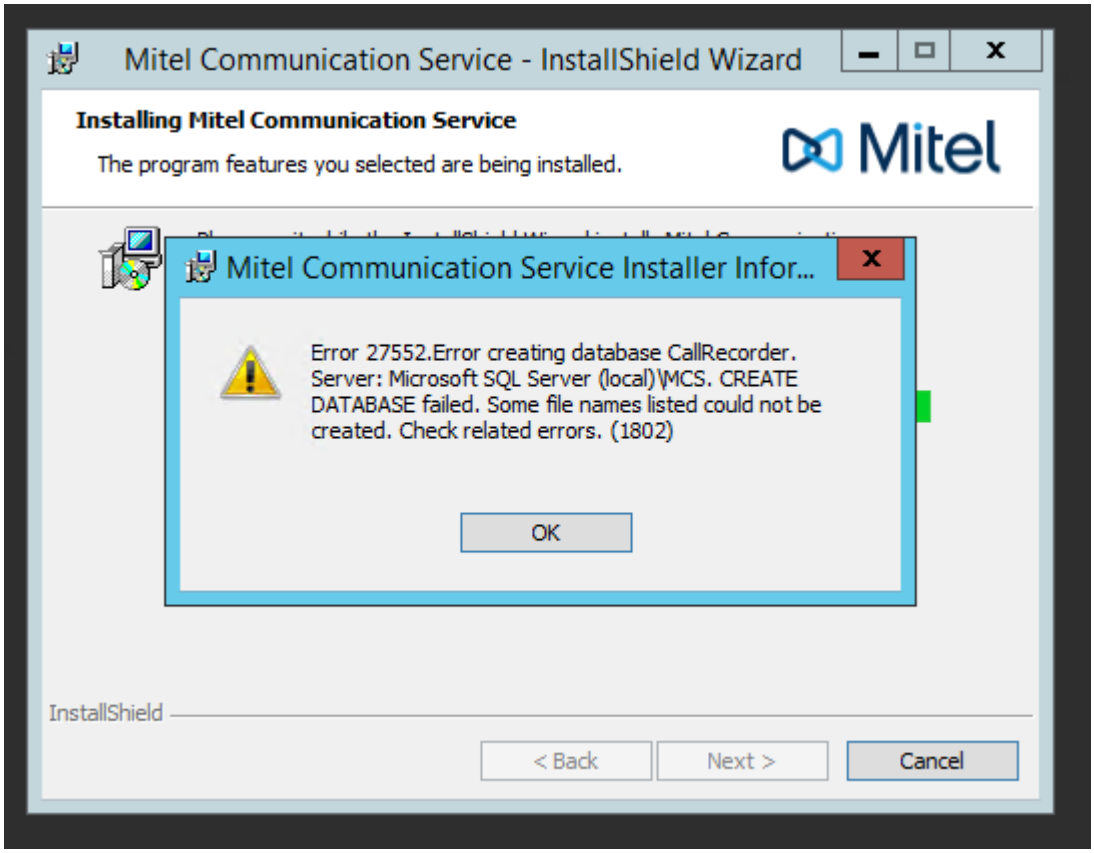
> ⚠ The system will go offline during the upgrade process, no data or call audio will be recorded during this time. It is advised that this process is completed outside of normal operating hours for the system.

Detached Databases

If for some reason the SQL Instance has been removed and re-installed by the MCS setup process then a situation can occur where the setup cannot complete because it cannot create the required databases due to the fact that they already exist on the hard drive.

This occurs because the database was automatically detached when the SQL instance was uninstalled.

The following 'Error 27552' will be seen:



If this occurs then there are two options available to continue installation:

Reattach Database Files

This method will keep any existing data from a previous MCS installation. Exit the installation and start the 'SQL Management Studio' application. Connect to the SQL instance '127.0.0.1\MCS' using windows authentication.

Right client on the 'Databases' menu item and select 'Attach' from the menu. On form that loads, press the 'Add' button and add all CallRecorder & CampaignManager .mdf files found in the following location:

C:\Program Files\Microsoft SQL Server\MSSQL12.MCS\MSSQL\DATA

Re-run the installation process, the install should now be able to see the existing databases and will be able to complete.

> If there is a permission issue when attempting to re-attach databases, ensure you are logged into the

server with the same windows credentials the software was installed with.

Move/Delete Existing Database Files

This method will allow the installation to create new databases when next run. Browse to the location below and move all CallRecorder/CampaignManager .mdf & .idf files to another location. It is recommended the files are moved and not deleted to reduce the risk of data loss.

C:\Program Files\Microsoft SQL Server\MSSQL12.MCS\MSSQL\DATA

Re-run the installation process.

5 Index

mitel.com