Mitel Communication Service Technical Manual

MAY 2018

DOCUMENT RELEASE 5.1

TECHNICAL MANUAL

Table of Contents

NOTICE

MiVoice Office Application Suite
Release 5.1 - May, 2018

1 What's New

Version 5.1

This version of MiVoice Office Application Suite sees the introduction of 'Real-Time Reporting' services, Mitel 6900 Handset support, Call Routing, Calling Party Number Substitution and other updates to existing features.

> If upgrading to 5.1 SP1, Phone Manager Desktop client software must also be upgraded if using the Call Recording Pause/Resume integration.

Automated Softphone/6900 Credential Updates

To simplify the deployment of 6900 phones and Phone Manager softphones, MiVoice Office Application Suite can now query SIP phone credentials from the telephone system* to simplify deployment.

* Requires 6.3 SP1 & CTGW 5.0.64

Link to the Softphone/6900 configuration section

Automated Teleworker Provisioning on MiVoice Border Gateway

To simplify the deployment of 6900 phones and Phone Manager softphones as teleworker phones, MCS has been updated to use the MBG provisioning API.

Link to the Teleworker API configuration section

MiVoice Office Real-Time Wallboard & Dashboard

View real-time call, DND* and ACD* statistics through the MiVoice Office Application Suite website. Users have access to single statistic and ticker tape tiles in addition to media streaming.

** Licence permitting*

Link to the Real-Time Reporting section

MiVoice Office Call Reporter Enhancements

Historical reporting has been updated to include DND* and ACD* based columns/reports. Keep track of when agents login/out and see how much time they spend wrap-up or do-not-disturb.

** Licence permitting*

Link to the Call Reporter section

MiVoice Office Call Recorder Enhancements

Remote MiNET IP extensions connecting through a MiVoice Border Gateway can now be recorded as long as there is no more than one extension behind each remote IP Address.

Link to the Call Recorder section

Mitel 6900 Handset Support

MiVoice Office Application Suite now supports the Mitel 6900 series of SIP handsets in conjunction with the MiVoice Office 250. MiVoice Office Application Suite acts as a configuration server to provide the handsets with firmware, keymaps and configuration. The 6900 handsets are new premium handsets with colour screens.

Link to the Mitel 6900 Handset section

Calling Party Number Substitution

This new feature provides a dynamic way of changing the calling party number presented based on the number being dialled. This feature works in conjunction with calls made through Phone Manager Desktop and

Phone Manager Outbound.

Link to the Calling Party Number Substitution section

Call Routing

This new feature provides dynamic call routing based on a database lookup, or fixed routing of calls queuing at hunt groups.

Link to the Call Routing section

Phone Manager Desktop Updates

Phone Manager Desktop now includes support Group Chat, DSS/BLF & Park Toolbar Buttons.

For more information on Phone Manager Desktop enhancements, please refer to the Phone Manager User Guide.

Campaign Manager Renamed to Phone Manager Outbound

Campaign Manager, the outbound progressive dialling solution for the MiVoice Office 250 has now been renamed to Phone Manager Outbound.

Licensing Updates

The following new licenses have been created to support the new features available in MiVoice Office Application Suite 5.1:

- DND Reporting -> System-wide licence
- ACD Reporting -> Per agent licence
- Call Router -> System-wide licence
- Calling Party Number Substitution -> System-wide licence
- Mitel 6900 Handset Standard -> Included with Phone Manager Outlook
- Mitel 6900 handset Enhanced -> Included with Phone Manager Professional & Team Leader
- External Data Sources -> System-wide license
- Real-Time Wallboard -> Per user license
- Real-Time Dashboard -> Per user license

User Connections Screen

The connected clients screen has been renamed 'User Connections' and has been updated to provide information on all user based connections, including Real-Time Wallboard/Dashboard Users and Mobile users. In addition, a new 'Connected Devices' screen provides information on licence usage of the new Mitel Handsets and ACD reporting licenses.

Refer to the User Connections or the Connected Devices section for more information.

Version 5.0

This version of MCS sees the introduction of MiVoice Office Call Reporter & MiVoice Office Call Recorder to the solution as well as some enhancements to Phone Manager Desktop & Mobile Clients..

MiVoice Office Call Reporter

Provides historical call reporting and scheduling for all internal and external calls on the system. Each user given permission can access reporting through the MCS website and run default reports or customise their own. Reports and filters can be shared between users and then scheduled to be emailed. Reporting and Scheduling are licensed features.

Link to the Call Reporting section

MiVoice Office Call Recorder

Provides the ability to record all or a subset of calls on the telephone system using a Record-A-Call or RTP/SIP based port mirroring. All calls that are recorded are stored centrally on the server and can be played back by users through the website or through Phone Manager Desktop.

Link to the Call Recording section

Phone Manager Updates

Phone Manager Desktop now includes support for initiating conferences from the Call Banner in addition to toolbar button improvements and access for users to easily Push/Pull calls using the HandOff feature of the telephone system, all form the Call Banner.

A new configuration option has been added to each user which allows the caller ID for any call they are on to be hidden from other users' Phone Manager displays. Please review the Users section for more information.

For more information on Phone Manager Desktop enhancements, please refer to the Phone Manager User Guide.

Licensing Updates

The system now supports voucher based licenses which means a known Site ID is no longer required when ordering license updates, simply apply a purchased voucher to any MCS 5.0 or higher system. In addition, a new concept of trial licenses has been introduced to allow customers to try features of the product before they buy. Software assurance and support (SWAS) contract for the software are now visible on the license pages of the website to keep users informed of the system's support status.

With this release of software, node based licensing has changed and additional licenses have been added for the new reporting and recording features. Please review the License Overview section for more information.

Refer to the Voucher License section and Trial License section for more information.

SQL Server and Operating System Support

On new installations SQL Server 2014 is now being installed (upgraded sites will continue to run on SQL 2008 R2). In addition, support for Windows Server 2016 has now been add including Hyper-V support on the platform.

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

Refer to the Requirements section for more information.

Connected Clients Screen

A new screen has been introduced to the Phone Manager Desktop section which provides details on all connected clients (Phone Manager, API and Call Recorder Clients). Information on the version of software the client us running is provided along with IP address and user details.

Refer to the Connected Clients section for more information.

Version 4.3

This version of MCS sees the introduction of Mitel Phone Manager Mobile along with a number of improvements to existing features of the solution.

Phone Manager Mobile

Phone Manager Mobile for iOS and Android provides access to Phone Manager features on the go. Features include access to Contacts, Global Directories, Chat with other Phone Manager users and receive Voicemail, Missed Call and Call Routing alerts. Phone Manager Mobile also has a Softphone capability.

Link to Phone Manager Mobile section

Presence Profiles

Presence Profiles are a new way of controlling DEE, Forwarding, DND and UCD status all from a single profile change. Presence Profiles are a requirement for using the new Phone Manager Mobile application and are enabled by default for users on new installations.

Link to Presence Profiles section

User Profile Updates

To improve the user's Phone Manager experience the MCS now downloads all Dynamic Extension Express devices a user has assigned.

Link to User Profiles section

Version 4.2

This version of MCS sees the introduction of MiContact Centre Campaign Manager along with a number of improvements to existing features of the solution.

Campaign Manager

Campaign Manager is a progressive dialling solution designed specifically for the MiVoice Office 250. Using the Mitel Phone Manager Professional or Team Leader client as a front end, Campaign Manager automates the process of making calls from a user's Mitel extension and provides centralised management and statistics for supervisors.

Link to MiContact Center Campaign Manager section

Telephone Profiles

The ability to add/edit/delete the telephone formats used by the Phone Manager plugins has been added to provide flexibility to customise the searches for screen popping and/or call history entries based on a customer's requirements.

Link to Telephone Profiles section

User Profile Updates

To improve the user's Phone Manager experience the MCS now offers the ability to store Hot Desk PIN and Voicemail PIN numbers against a user's profile.

Link to User Profiles section

Common SMTP Configurations

To help with the setup of email support, configurations for common SMTP servers have been documented.

Link to Gmail SMTP example section

Link to Office365 SMTP example section

1.1 Known Issues

DPAR/ID	Description	Notes/Work around
MN00537903	Unable to change the order of columns once added when creating a call banner.	To work around this issue, simply remove the column(s) and re-add in the order you would like.
MN00584795	Crackling noise on SIP Softphone when using G.711 A-law	To work around this issue, change Phone Manager Softphone SIP Extensions to use Mu-law.
MN00661458	4-5 Second delay when transferring calls with Phone Manager Softphones	This has been reported on some sites using A-Law. When experienced, change to use Mu-Law.
MN00663798	Recordings merged when routing external calls directly to a Phone List or using the 'Multiple' ring-in type	Routing calls to phone lists or using the ring-in type of 'Multiple' are not supported in conjunction with MiVoice Office Call Recorder in this release, either direct from a trunk group or through a call routing table. This affects both IP/SIP Extension and Record-A-Call methods. To work around this issue, a UCD hunt group should be used instead.

If upgrading to 5.1 SP1, Phone Manager Desktop client software must also be upgraded if using the Call Recording Pause/Resume integration.

2 Introduction

About this Document

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

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 Mitel Communication Service

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 dialler features through MiVoice Office Phone Manager Outbound
- Provides call logging and reporting features through MiVoice Office Call Reporter
- Provides call recording features through MiVoice Office Call Recorder
- Provides real-time call, DND & ACD statistics through MiVoice Office Real-Time Wallboard/Dashboard
- Acts as a configuration server for Mitel 6900 series handsets
- 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 Phone Manager Outbound
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.
14. MCS Realtime
    - Processes all call/DND/ACD in real-time to provide information to Wallboards & Dashboards
15. MCS Handset
    - Interacts with Mitel 6900 Series handsets, handling firmware, BLF updates, keymap and configuration profile updates and images.

> 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

2.1 Requirements

Overview

The system requires specific information and requirements to be met for any installation. Read each of the sections and ensure that the information requested is available prior to an installation.

1. System Requirements
2. PBX Supported Versions
3. Browser Requirements
4. Real-Time Client Requirements
5. Desktop Client Requirements
6. Network Configuration
7. Anti-Virus Recommendations
8. Email Details
9. Users & Business Units
10. Telephone Number Prefixes
11. PBX Integration
12. Backups

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) • 50 Mitel 6900 SIP Handsets • 8 Concurrent Call Recordings • 2 Concurrent Real-Time Wallboards/Dashboard	• CPU: 1 x Intel Core i3 dual core @ 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) • 100 Mitel 6900 SIP Handsets • 60 Concurrent Call Recordings • 5 Concurrent Real-Time Wallboards/Dashboard	• CPU: 1 x Intel Xeon quad core @ 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) • 500 Mitel 6900 SIP Handsets • 250 Concurrent Call Recordings • 10 Concurrent Real-Time Wallboards/Dashboard	• CPU: 2 x Intel Xeon quad core @ 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, License 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
- Call Processing Version 6.3.x

If Mitel 6900 Handsets are being supported, the Call Processing Version must be 6.3 SP1 (6.3.7.58) or higher.

The following Multi-Node configuration is supported:

- Multiple MiVoice Office 250 nodes via the use of a Mitel CT Gateway(Version 5.0.64 or higher is required).
- 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 Mitel 6900 Series Handsets:

- Cat F licenses are required for each connected 6900 handset.

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).

> MCS will not connect to CT Gateway Versions below 5.0.64. If it detects the version is lower than this it will fail to start.

> MCS does not support ACD member hunt groups, only ACD Agent hunt groups.

> 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 G711

> 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.

Browser Requirements

The system is managed and accessed through a web browser. The following web browsers are currently supported.

Browser	Version	Plugins
Microsoft Internet Explorer*	11 (not in compatibility view)	Windows Media Player v10 for call recording playback
Mozilla Firefox	45	
Chrome	49	

> * Microsoft Internet Explorer can be used to access the website, however performance for the Real-time Dashboard can be slow. When using the Real-Time Dashboard, Chrome or Firefox browsers are recommended.

> If accessing the website from an iOS device using Safari, the normal redirect does not work. Instead, use the following URL: http://[ServerAddress]/Login.aspx

Real-Time Wallboard/Dashboard Requirements

To be able to access the Real-Time Wallboard/Dashboard client device needs to meet the following **minimum** requirements. Please refer to the Browser Requirements section for further information.

PC Hardware Requirements

Processor	Intel Atom x5-Z8330 or better
Memory	Minimum: 2GB RAM Recommended: 4GB RAM or more
Network	IPv4, 100Mb / 1Gb LAN
Hard Disk	Minimum: 32GB free space
Video	Minimum: DirectX v9 compatibly graphics cards with 120MB RAM Recommended:DirectX v9 compatibly graphics cards with 1024MB RAM

Tablet/Mobile Hardware Requirements

Tablet	iPad 5 or higher
Mobiles	iPhone 5s or higher

Phone Manager / Call Recorder Client 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 R2 Standard/Enterprise/Datacenter 32-bit/64-bit
- Windows 2012 R2 Standard/Datacenter 64-bit
- Windows 2016 Standard/Datacenter 64-bit

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

Hardware Requirements

Processor	Intel Core 2 Duo 1.8GHz or faster processor (or equivalent)
	Minimum: 1GB RAM

Memory	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 4.5.2

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.

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
Website access	HTTP	Inbound	TCP 80
	HTTPS/SSL	Inbound	TCP 443
Licensing	HTTPS/SSL	Outbound (service.xarios.com)	TCP 443
SQL Server	SQL Server	Inbound/Outbound	TCP 1433
Phone Manager Desktop	CTI Link	Inbound	TCP 2001
	Client Sessions	Inbound	TCP 8187 & TCP 8186
	Client Personal Wallboard Sessions	Inbound	TCP 8204
	Broadcast location service	Inbound	UDP 8184
	SIP Audio	Inbound/Outbound PM Desktop to MCS	UDP 20000-20500
Communication Gateway	Integration Services	Inbound	TCP 8188
Communication Service	Server Connections	Inbound/Outbound	TCP 8189 TCP 8183
Phone Manager Mobile	Client Sessions	Inbound	TCP 8185
	Audio	Inbound	TCP 8190
	SIP Audio	Inbound/Outbound PBX to MCS	UDP 20000-20500
	Google Push Notification Service	Inbound	TCP 5228, 5229, 5230
	SIP Proxy	Inbound/Outbound	TCP 8196
	Server Connections	Inbound/Outbound	TCP 8190

CTI Link	MiVoice Office 250 OAI	Outbound	TCP 4000
MiVoice Office Call Recorder	MiVoice Office 250 SIP (RAC Call Recording & Phone Manager Mobile Softphones)	Inbound/Outbound	UDP 5060
	MiVoice Office 250 Audio (RAC Call Recording)	Inbound/Outbound	UDP 12000-12100
	Live Streaming	Inbound	TCP 8201
	Server Connections	Inbound	TCP 8197
Handset Service	Server Connections & 6900 Handset Requests	Inbound	HTTPS 8202 HTTP 8203
	6900 Handset Requests	Inbound	TFTP 69
MiVoice Office Real-Time Wallboard/Dashboard	Server Connections	Inbound/Outbound	TCP 8191
	Data Link from client browser	Inbound	TCP 8200

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\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\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
- Microsoft SQL Server 2014
    - %ProgramFiles%\Microsoft SQL Server\MSSQL12.MCS\MSSQL\Data (File extensions to exclude: *.mdf,*.ldf, *.ndf, *.bak, *.tm)
    - %ProgramFiles%\Microsoft SQL Server\MSSQL12.MCS\MSSQL\Binn\SQLServr.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.

Email Details

The system uses email as a key alert, notification and messaging system and needs to be configured correctly. There are five main areas where email is used:

1. Internal Monitoring: There is an internal monitoring system that can report any potential problems or issues when they occur and the system can also send out emails to alert the administrator about these problems.
2. New account details, password reminders for users.
3. Phone Manager Mobile user invitations.
4. For sending reports out from the scheduler
5. For emailing call recordings

> Configuring email is a mandatory requirement and without this the system will not generate alerts until this is made available.

See the Email & SMTP section for details.

Users & Business Units

The system uses the concept of Users to control security and access to the system and to assign a Phone Manager license class in the user's profile.

Each user can have multiple agent IDs and/or extensions associated to it. When a call is handled by this agent/extension the "User" is tagged against this call.

Users can either be created manually, via Active Directory or automatically whenever a new agent ID/extension is created on the PBX. User creation choice needs to be determined before installation to ensure that all calls are tagged correctly.

See the Users and Business Units section for details.

Telephone Number Prefixes

When a call is logged the outside number (caller ID or dialled number) and the inbound direct dial number will be logged against the call. The numbers that are logged may not contain all the digits expected or show extra digits that are not required.

- For outbound calls the dialled number may contain LCR (least cost routing) or Automatic Route Selection (ARS) digits if this is used by the customer
- For outbound calls the number may not have the local area code dialled if this was not dialled when the call was made
- For inbound calls the direct dial number may only contain the last 4 or 6 digits depending on how many digits that the line provider sends

See the Dial Plan section for more details.

PBX Integration

The solution integrates with the MiVoice Office 250 PBX system either directly or through a CT Gateway. The solution monitors devices through the System OAI Protocol and logs all call information as well as acting as a proxy for any Phone Manager clients.

See the Phone Systems section for details.

Backups

The system stores all of the information relating to the calls and the configuration of the system in a Microsoft SQL Server database installed on the server with the Database role. The system will back up the database every night to a user defined location. This needs to be set to a location that is NOT on the server itself.

If the database fails or becomes corrupted and this backup is available then the database can be easily restored. If the database backup is not available then the call information may be permanently lost.

See the Database Maintenance section for details.

If using the call recording features of the solution then recorded calls need archiving separately from the database. Please refer to the Call Archiving section for more information.

2.2 Installation

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 fail 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.

2.3 After Installation

After the setup has been run the Watchdog service will start then upgrade the database to the current version and start the relevant services automatically. This may take a few minutes to complete and once this has finished the configuration website is automatically loaded at http://serveripaddress_host.

In addition to the configuration settings accessible via the website user interface the software installs an administration application on the server called "MCS Admin Tool" with a desktop icon and when running, a system tray icon to indicate the running state of the server and to provide two configuration options:

1. Setting the Server ID (the default is 1 and will not need to be changed unless additional servers to share the load are installed)

2. Configuring which SQL server to use for the system. (the default is to use the SQL database installed with the server locally but if required this can be changed to an external SQL database)

If required a manual database update can be performed by following the steps below:

1. Once you have a connection to the desktop on the server run the *MCS Admin Tool*. If this is not shown then this can be opened via either the *MCS Admin Tool* shortcut on the desktop or from the Start Menu (*Programs -> Mitel -> Communication Service -> MCS Admin Tool*). Using the mouse and hovering over the system tray icon will display the status of the system. On a new installation there may be a red exclamation icon in the bottom right hand corner to indicate that the system is not running and that a database update is required.
2. To open the configuration tool the icon can be double clicked on or right clicked and the Settings menu selected. The main configuration tool will be displayed and if the tool detects that the Communication Service database either does not exist (i.e. for new installs) or an earlier version (if been upgraded) then it will prompt you to upgrade.
3. Click on Ok to continue and then use the Update button on the Database tab.
4. If this is an upgrade then ensure database backups have been performed and then click on Ok. This may take a few minutes (or if there are high volumes of historical calls then it could take several hours) and the database will then be upgraded to the current version.
5. When complete a confirmation message will be displayed.
6. If the upgrade fails check the error logs for details, the default location is here: %PROGRAMDATA%\Mitel\Mitel Communication Service\Logs\Admin\logs.
7. The configuration tool tray icon will then display the message below and the WCF Service will need to be started before any further configuration can be performed.
8. To start the WCF service from the start menu, select *Run* (or press the Windows key + R) and enter *services.msc.*
9. This will open the Microsoft Services snap tool. Find the service named *Mitel MCS Watchdog Service* and then select *Start* from the menu toolbar.
10. Once this service has been started the rest of the configuration can be done from the website. The website can be accessed using the default details of:
    http://<serveripaddress_host> (U: engineer, P: Teleph0ny!)

2.4 Administration Overview

The main administration section for the Mitel Communication Service is accessed through a website.

Browser Requirements

The system is managed and accessed through a web browser. The following web browsers are currently supported.

Browser	Version	Plugins
Microsoft Internet Explorer*	11 (not in compatibility view)	Windows Media Player v10 for call recording playback
Mozilla Firefox	45	
Chrome	49	

* Microsoft Internet Explorer can be used to access the website, however performance for the Real-time Dashboard can be slow. When using the Real-Time Dashboard, Chrome or Firefox browsers are recommended.

If accessing the website from an iOS device using Safari, the normal redirect does not work. Instead, use the following URL: http://[ServerAddress]/Login.aspx

License Agreement

When a user first logs in they will be prompted to accept the license agreement before continuing. This has to be done by each user that logs in.

If the *Accept* and *Decline* buttons are not displayed then scroll down to the bottom of the license agreement.

Navigation

To navigate around the website there is a menu bar that is displayed at the top of the page which gives access to all the features as shown.

Depending on the users access rights some of the menu options may not be visible.

If you hover over the Mitel logo it will give you the version number of the product

2.5 User Management and Security

Access to the website is controlled through user accounts configured on the system. In order to access any of the features on the website you need to be logged in with a valid user account.

> User accounts are an MCS concept that can be stand alone or linked to a Domain account. For more information please refer to the Users section.

The system is pre-configured with two default user accounts for engineer access and supervisor access. The engineer account has full access to the website to configure the system and create users. This restriction cannot be changed. The supervisor account has limited rights but is able to perform basic management functions. The default credentials with the username and passwords are shown below.

Username	Password
Engineer	Teleph0ny!
Supervisor	M1t3l!Superv!sor

Logging on

To logon to the website browse to the *Website address* of the Communication Service. The logon screen will then be displayed as shown in the image below. Enter your username and password in the relevant boxes and click on *Logon*.

> When your user account is linked to a Domain account, Windows Integrated Logon can be used for the MCS website. Refer to the website configuration for further information.

Forgotten Password

If a user has forgotten their password they can click on the *Forgotten Password* link in the top right hand corner of the logon page. They are then able to enter their username or email address and the password will be emailed to the address configured under their account.

My Settings

Each user that is logged in has access to change some of their details, including name, password email address, and language options. This is accessed from the *My Settings* menu as shown. Once any changes have been made click on *Save* to save the changes, this will also prompt to enter your password as an additional security check. If you need to remove any changes that you have made click on the *Reset* button.

2.6 Initial Configuration

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 Serial number as the license type
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 Site ID as the license type
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:

- DDI 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.

2.7 Best Security Practice

The overall security of the Mitel Communication Service deployment relies on the many installation factors, primarily the security in place on the host operating system and network infrastructure.

The following sections outline recommendations for improving security of Mitel Communication Service installations.

> Securing the installation and ensuring only relevant users have access to the system is the responsibility of the installer of the system.

Secure User Access

It is essential to secure access to both the host operating system and the MiVoice Office Application website to ensure that only users that should be accessing the system, can access the system. In addition, any user accounts created on the system should use the 'principle of least privilege', using the Roles & Profiles provided to limit user access to only the features they require.

The system also has a number of 'Built-In' user accounts which provide a pre-determined level of access. These include:

- engineer
- supervisor

The default passwords of these accounts should be changed after installation to restrict access to the system.

For more information on managing user accounts, please refer to the Users & Business Units section.

HTTPS Website Access

The MiVoice Office Application Suite Website provides users with access to the configuration settings for the system as well as being the front end to the following features:

- Call Reporting
- Call Recording
- Real-Time Wallboard/Dashboard

By default, access to this website is through HTTP on port 80. To improve security for users logging into the system, HTTPS should be enabled on the website and HTTP access should be disabled.

To enable HTTPS, a certificate must be uploaded to server and the IIS server (local web server) configuration must be updated. For information on how to do this, please refer to the Enabling HTTPS section.

> If the MiVoice Office Application Suite website is to be made available to users outside the Local Area Network (LAN) through port forwarding, ensure that HTTPS is enabled and restrict access to specific external IP addresses to increase security.

Secure Host Operating System

It is important that the operating system hosting the MiVoice Office Application Suite has security policies in place to minimize the risk of any unauthorised access to data and/or features. The following security steps should be taken on ALL host operating systems as a bare minimum:

- Implement an Anti-Virus Solution - Information on anti-virus exceptions can be found in the Anti-Virus Requirements section.
- Implement a Firewall - Information on the network ports used by the solution can be found in the Network Requirements section.

- Install OS Security Updates - Either automatically or manually, all OS security updates should be installed on a regular basis.
- Disable Weak Ciphers & Protocols - Disable older TLS ciphers and other less secure protocols.

Following the steps above will make the system more secure and will reduce the risk of unauthorised access.

Disabling Weak Ciphers & Protocols

Access to weaker ciphers/protocols needs to be done in the operating system registry in most instances. Information on how to do this can be found in the following Microsoft articles:

- https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc
- https://support.microsoft.com/en-gb/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in

Alternatively, the following free tool can be used - https://www.nartac.com/Products/IISCrypto

- Install ISSCrypto Tool
- Apply PCI 3.1 template
- Remove TLS 1.1 & Triple DES Cipher

> ⚠ This is not an exhaustive list and should be taken as a bare minimum of security precautions that should be applied to the host operating system.

Email Configuration

If using the email based features of the solution (alerts, alarms, schedules etc) it is advisable to configure the SMTP connection to the server to use both authentication and SSL/TLS.

Audit Personal Data

To comply with local data protection laws (such as GDPR), it is important to understand what personal data is being stored within the solution and what it is being used for. There are several areas where personal data could be stored within the MiVoice Office Application Suite system:

- Contact Directory - Custom data fields can be inputted along with telephone numbers and other contact information
- Call Recordings - Personal data could be discussed on calls and stored in call recordings. Calls can also be tagged with custom data and notes
- Call Reporting - Telephone numbers can contact/speed dial names are stored within the call history system
- Phone Manager Outbound - Campaign data can contain personal information if imported in addition to the contact information

In all cases where customer's or employee's personal data is stored in the system, the following guidelines should be followed:

- The location and type of data stored should be documented
- Permission should be obtained from the person whose data it is
- Access to the data should be restricted to users who require it to perform the specific function the data is stored for

For more information on GDPR, where data is stored within MiVoice Office Application Suite, please refer to the GDPR section. For information relating to Mitel Phone Manager Outbound, please refer to the Phone Manager Outbound Technical Manual.

Software Patch Management Policy

It is necessary for the administrator to ensure that the MiVoice Office Application Suite is always updated and equipped with all critical patches to guarantee the highest level of security. Mitel has developed best practices for the management and installation of security patches released by the operating system vendors aiming to guarantee the highest level of security and the correct functioning of the system.

Mitel Product Security Policy

As part of Mitel's ongoing commitment to customers and product excellence, Mitel maintains a dedicated product security incident response program to handle the discovery of potential vulnerabilities and security flaws in products. Mitel's product security policy is published at www.mitel.com/mitel-product-security-policy.

Mitel Security Advisories

Public notices regarding moderate and high-risk product security vulnerabilities are published at www.mitel.com/security-advisories.

3 Real-Time Reporting

Real-Time Reporting provides users with real-time visibility of calls and status of various different aspects of the telephone system.

This system provides two levels of real-time access for users:

- Wallboard, a single real-time view restricted to single statistic tiles, media tiles and a ticker.
- Dashboard, a supervisor real-time UI with access to multiple views and additional tile support.

Users can be assigned permission to access either the Wallboard or the Dashboard. This is done using a Security Profile.

For information on how to use the Real-Time Wallboard, please refer to the Quick Start Guide.

The following sections provide a breakdown of all aspects of Real-Time Reporting use:

- Tiles
- Statistics
- Tile Alarms
- Real-Time Filtering
- Full Screen Views
- Global Variables

3.1 Real-Time Wallboard Quick Reference Guide

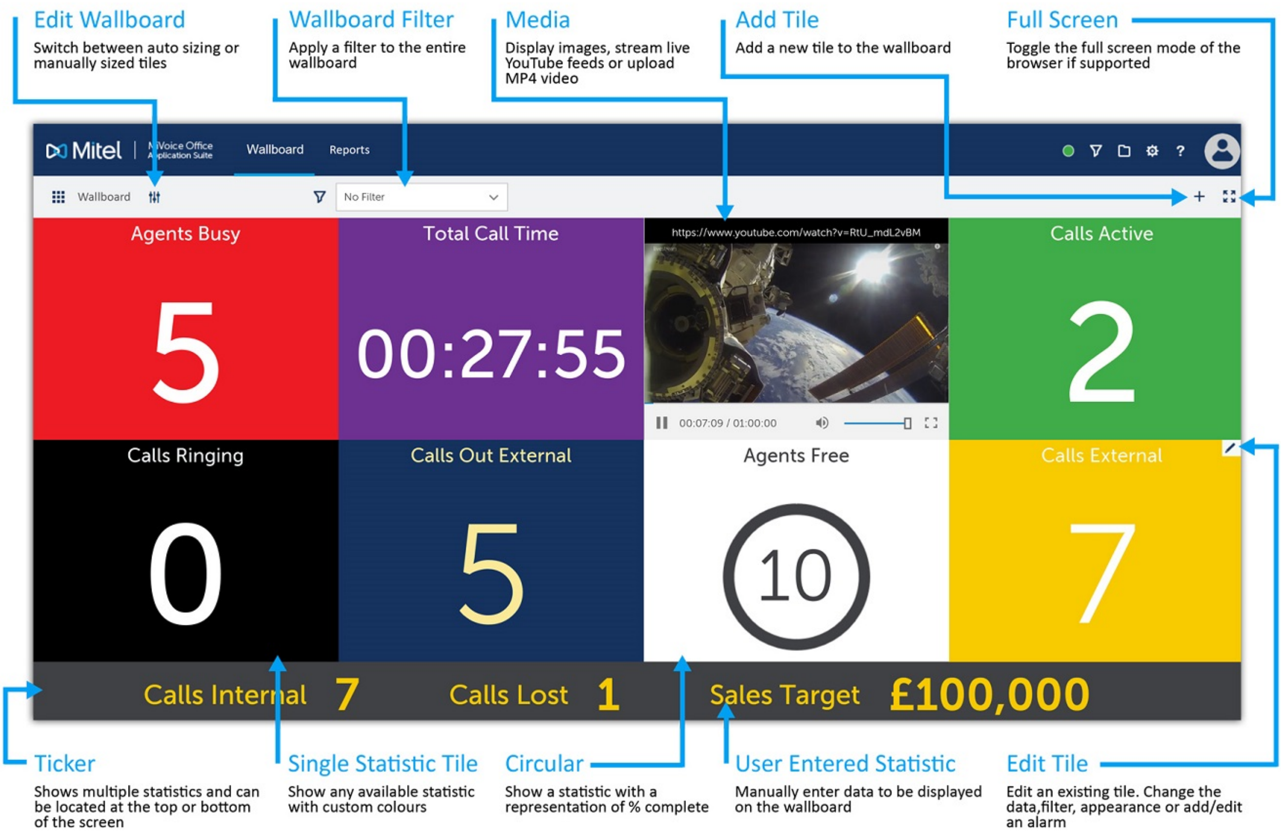
The following guide is designed to provide an introduction to the core features of the Real-Time Wallboard.

Wallboard UI

The webpage provides real-time visibility of calls, do-not-disturb status* and agent status* on the telephone system. By default, a standard view containing some commonly used statistics are added on first logon to the wallboard. This view can then be customized with a variety of tiles which can be filtered as required. The wallboard provides the following types:

- Single Statistic
- Multi-Statistic 'Cycling'
- Media (Video/Images)
- Ticker

** Agent & DND visibility require additional licensing.*



Single & Circular Statistic Tiles

Choose a single statistic from the call, DND & agent field options. The foreground & background colours of the tiles will be selected randomly by the wallboard (dependant on the default option chosen) but can be changed as required. Optionally, the appearance of a single statistic tile can be changed to show a circular gauge displaying the % of a target value.

Cycling Multi-Statistic Tiles

These tiles display similar information as single statistics tiles but can cycle through multiple statistics. Each statistic added can have a different appearance to help distinguish between them.

Media Tiles

These tiles can display images, live streaming video from live feeds or display an uploaded video file on a loop. Audio from videos can be turned on or off.

Ticker

The ticker can be used to show up to 20 different statistics that loop round the screen. As with the multi-statistic tiles, each statistic added to the ticker can be given a different appearance to help distinguish between them.

> Only one ticker can be added to a Real-Time Wallboard view. It can either be located at the top or bottom of the view and has various options for size and speed.

Full Screen

The full screen mode can be toggled* using the icon provided. When enabled, the browser frame/toolbar and the website title bar are removed so that the the wallboard fills as much of the screen as possible.

** Full Screen mode is not supported in all browsers*

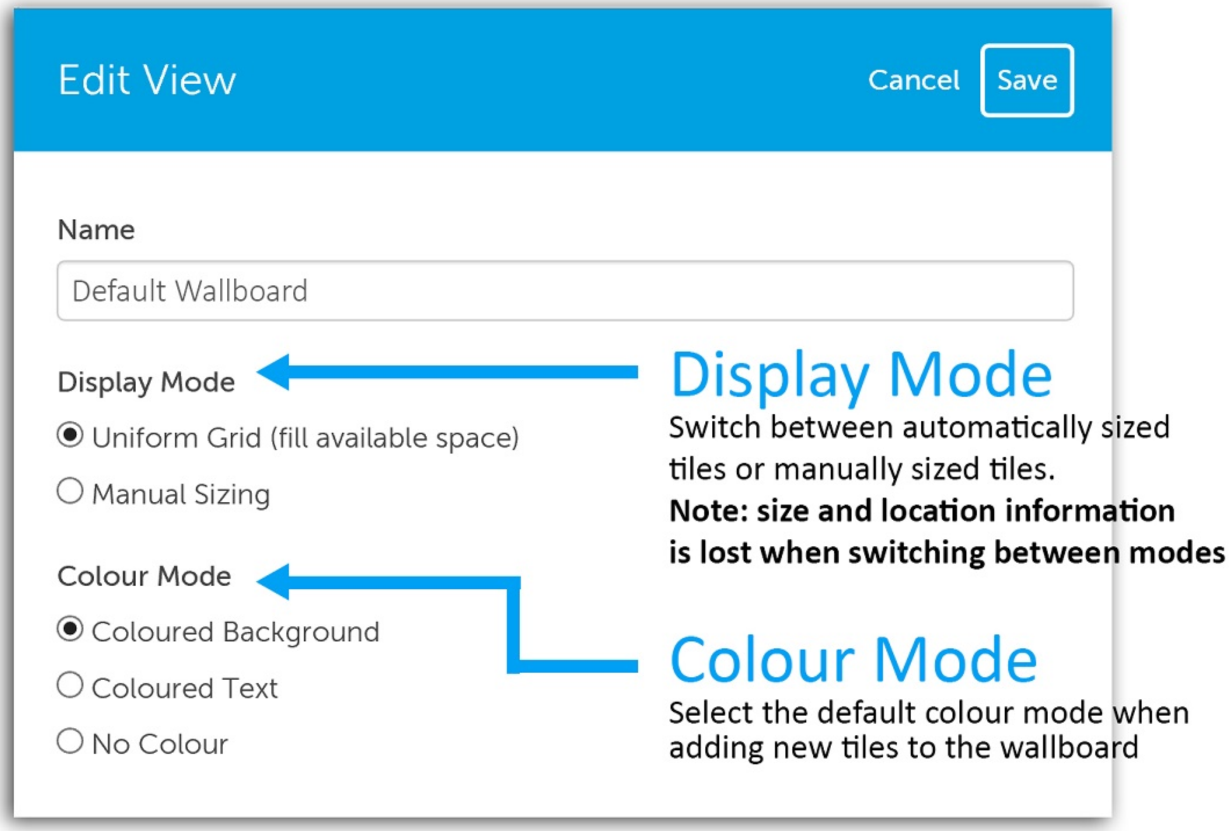
Manual/External Statistics

If required, manually added data (Global Variables) or data from external databases can be displayed on any of the tiles. This is useful for displaying general information to users such as sales targets, promotions, support information etc.

> Global Variables are edited in the configuration section ( ) of the website. This will only be available with the correct permissions.

> There is an additional licence for enabling external data sources.

The wallboard view has two settings which can be changed by pressing the edit icon ( ) in the top-left of the Wallboard.



Display Mode

The display mode can be set to either 'Uniform Grid' (default) or 'Manual Sizing'. When uniform grid is enabled, the tiles on the wallboard will automatically resize as tiles are added or removed, simplifying the setup of the wallboard. When manual sizing is enabled, each tile must be individually located and sized. The benefit of manual sizing is that tiles can be different sizes if required.

> Switching between display modes will cause the tile location and sizing to be lost.

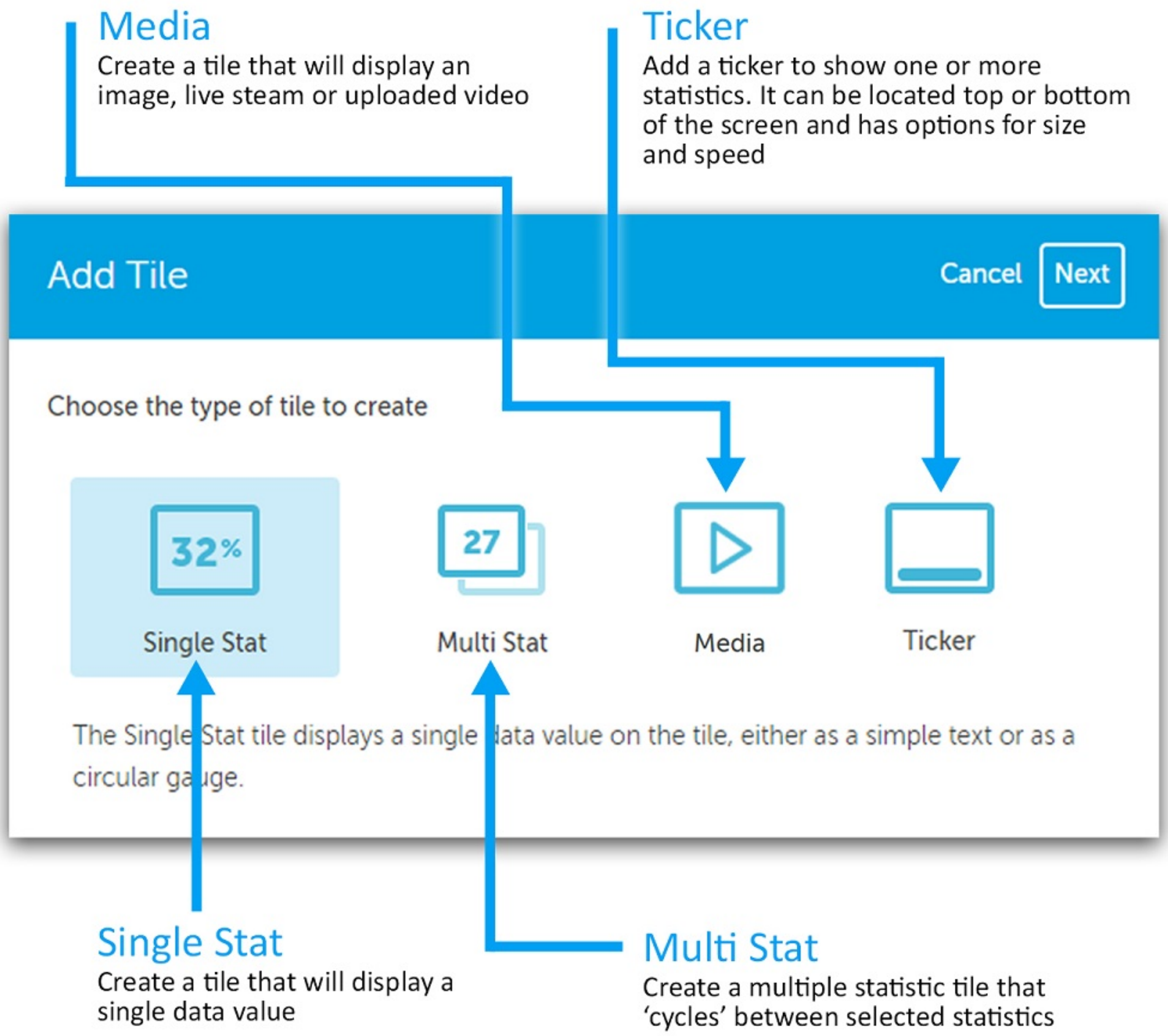
Colour Mode

The colour mode can be set to either 'Coloured Background' (default), 'Coloured Text' or 'No Colour' (black and white). When coloured background is selected, each new tile added will be given a randomly selected background colour with white text (recommended for viewing from a distance). When coloured text is selected, each new tile added is given a randomly selected foreground colour with a white background (recommended for viewing close up). When 'No Colour' is selected, each new tile added is given a white background with black text.

> The colour mode only affects new tiles that are added to the view. Existing tiles' backgound/foreground colour must be changed manually.

Edit Mode

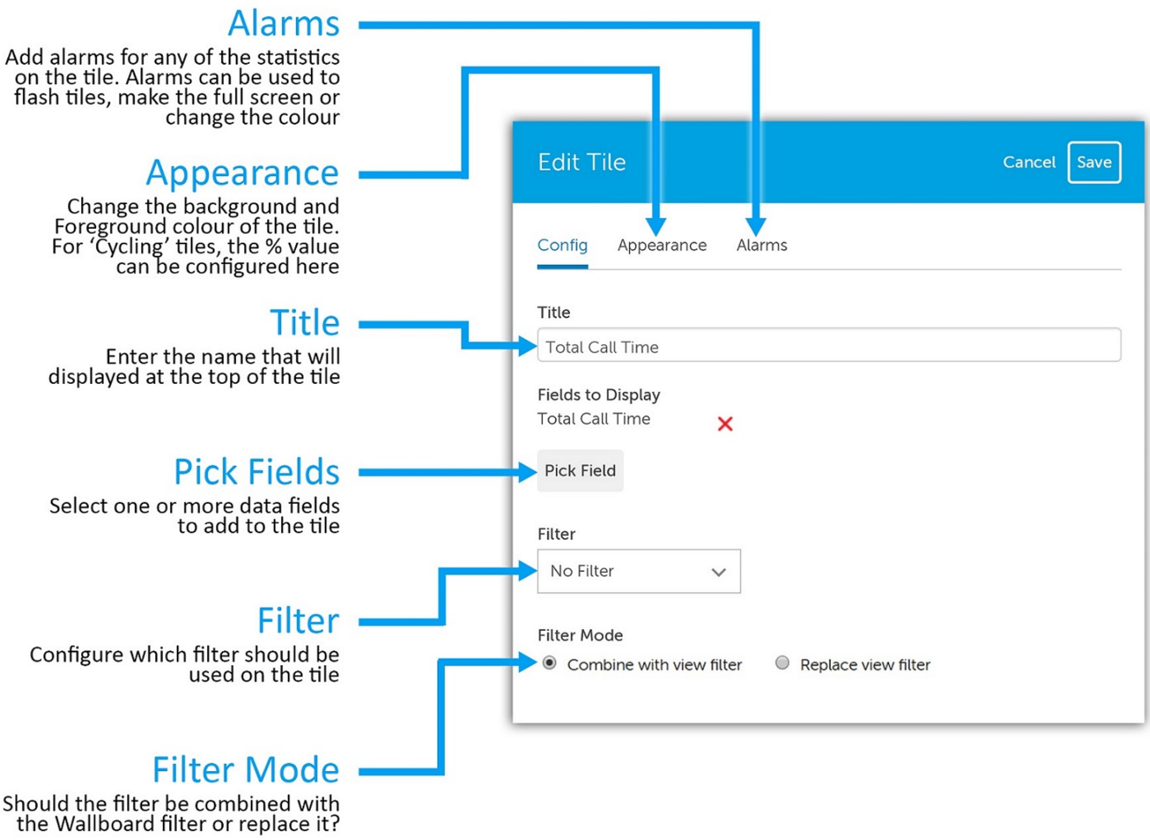
To add new tiles or move/resize existing tiles, edit mode must be enabled. Press the edit () icon on the top right-hand side of the view to enter edit mode. Once enabled the plus (+) icon can be used to add new tiles to the view. When pressed, the 'Add Tile' form is displayed, providing a choice between the different types of tiles available. Additionally, while in edit mode any existing tiles can be moved or resized (when using manual display mode). Press the tick (✓) icon to exit edit mode.



Once the tile type has been selected, press the 'Next' button to view the tile properties form.

> Only one ticker is allowed per Wallboard. If there is already a ticker added, the ticker tile will not appear when adding new tiles.

Each tile has a set of properties so that it can be customised. The properties available will differ depending on the type of tile being edited/added. The image below shows the property form based on a single statistic tile.



Title & Fields

The title will be displayed at the top of the tile. By default, this will be set to the name of the data field selected, but can be changed. To add fields to a tile, press the 'Pick Field' button and then select the required field from the context menu. To aid selection, the fields have be grouped together into categories.

> For more information on the fields available and how they are calculated, please refer to the help file.

Filter & Filter Mode

The data on each tile can be filtered if required. By default no filter is applied. The filter mode is used to select whether the overall Wallboard view filter is applied or not. When set to 'Combined with view filter' (default), any filter set on the Wallboard view will be combined with any filter set on the tile. If set to 'Replace view filter' any filter set on the Wallboard view will be ignored.

> To ensure a tile never has a filter set, leave the filter set to 'No Filter' and select 'Replace view filter' as the filter mode.

Appearance

The appearance section provides access to change the foreground/background colour of the tile and also any other display options (such as 'Circular Gauge').

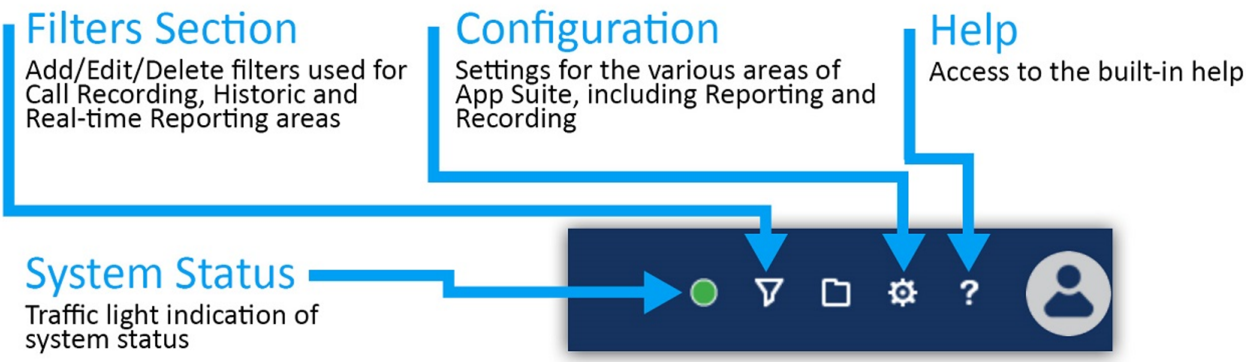
Alarms

Each tile can have one or more alarms configured. Alarms can be used to bring attention to tiles when thresholds are reached or breached. Alarms can be set to do the following:

- Flash the tile
- Make the tile full screen (double-click the tile to revert it back)
- Override the foreground/background colour
- Play a sound file

Overriding a tile's foreground and/or background colour is very useful for creating traffic light style tiles. For example, thresholds can be set to change a tiles colour from green to amber to red based on the data field's value. This can be used to help bring attention to specific performance targets.

The title bar provides access to areas of the App Suite. The image below outlines each of the navigation icons:

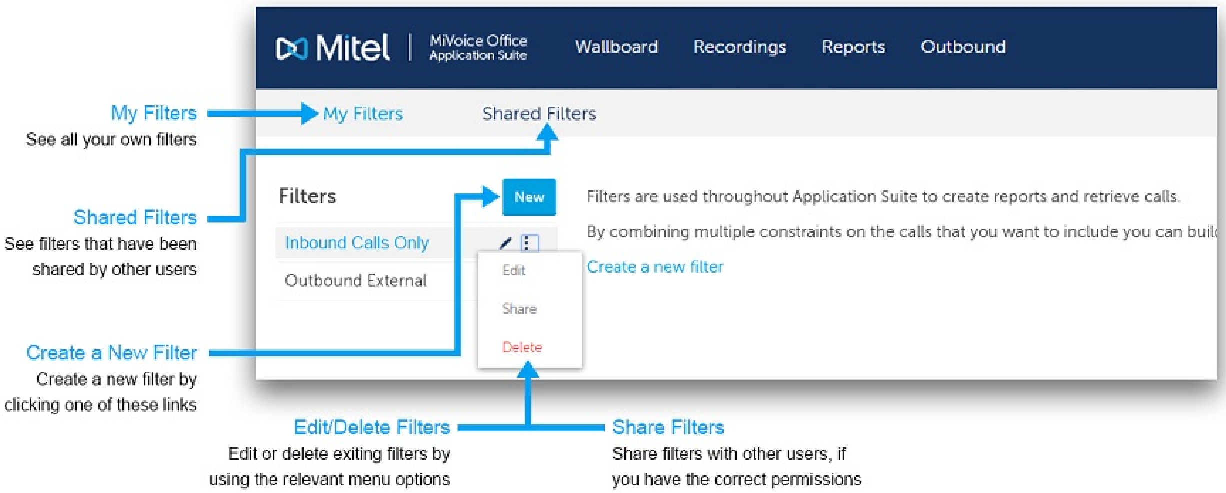


The configuration section and system status will only be visible with the correct permissions.

Filters

The 'Filters' section of the website is used to manage all the saved filters on the system. Filters can be used with reports or recordings.

Each user has their own 'My Filters' section that provides a list of all filters they have created.

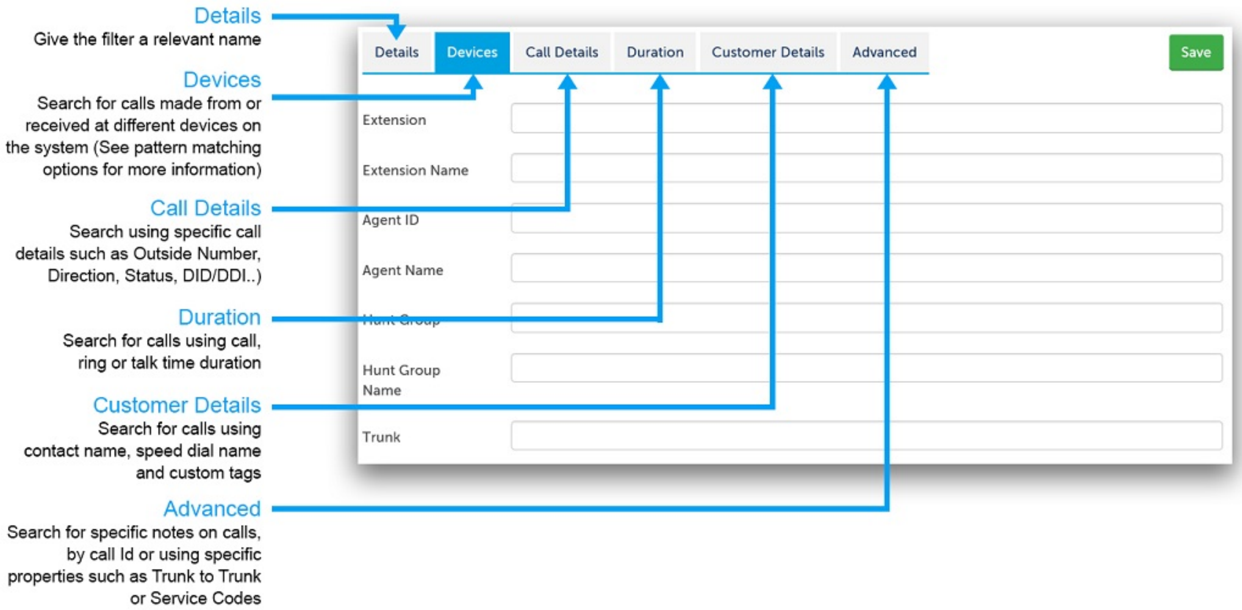


Shared Filters (Permission dependant)

Filters can be shared between users to avoid duplicating work and to allow administrative staff to set up filters that can be used by everyone.

Adding / Editing Filters

Each filter provides the ability to search on one or more details about a call. The details are grouped into tabs. The tabs are displayed with descriptions in the image below:



The use of special characters within the text boxes for a Filter enables the use of complex filter strings.

All Fields

The following characters are supported:

Special Characters	Description
Exclamation mark (!)	Not equal to
Percent (%)	Fuzzy matching (equivalent to a SQL LIKE %)
Underscore (_)	Fuzzy matching of a single character
Comma (,)	Can be used to search for multiple values at the same time

Device Fields

In addition to the special characters above, the following characters are supported when searching using a device based field (Extension, Agent, Trunk, Hunt Group):

Special Characters	Description
Plus sign (+)	Greater than or equal (e.g. 1000+ for extensions greater than or equal to 1000)
Hyphen (-)	Delimits a range of values to match (e.g. 1000-2000 for all extensions between 1000 and 2000 inclusive) or less than or equal to (e.g. -1000 for extensions less than or equal to 1000)

The example below shows what would be matched when entering combining multiple special characters using a comma:

- 1000-1005,!1003,1040,18%5,2000+

Matching endpoints: 1000, 1001, 1002, 1004, 1005, 1040, any that start with 18 and end with a 5, any with a value greater or equal to 2000.

> Device numbers are stored as text so when using greater than or less than, it is compared on an alphabetic level not a numeric level

3.2 Real-Time Dashboard Quick Reference Guide

The following guide is designed to provide an introduction to the core features of the Real-Time Dashboard.

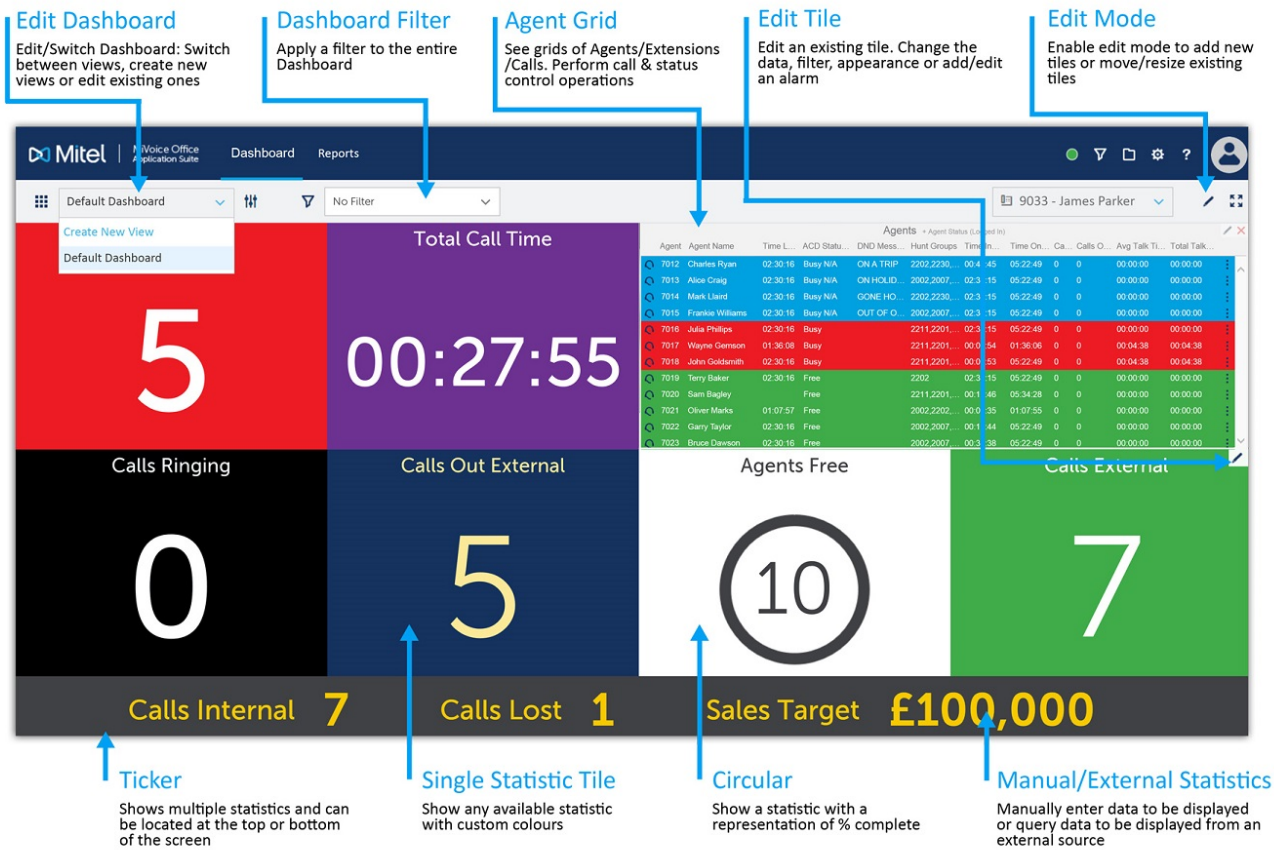
Dashboard UI

The webpage provides real-time visibility of calls, do-not-disturb status* and agent status* on the telephone system. By default, a standard view containing some commonly used statistics are added on first logon to the dashboard. This view can then be customized with a variety of tiles which can be filtered as required. The dashboard provides the following types:

- Single Statistic
- Multi-Statistic
- Media (Video/Images)
- Ticker
- Grid (Agent, Call, Extension & Trunk)

** Agent & DND visibility require additional licensing.*

A Dashboard can have multiple views configured by the user, they can then switch between the views via the dropdown box.



Single & Circular Statistic Tiles

Choose a single statistic from the call, DND & agent field options. The foreground & background colours of the tiles will be selected randomly by the wallboard (dependant on the default option chosen) but can be changed as required. Optionally, the appearance of a single statistic tile can be changed to show a circular gauge displaying the % of a target value.

Multi-Statistic Tiles

These tiles display similar information as single statistics tiles but can display multiple statistics at once, or cycle through multiple statistics. Each statistic added can have a different appearance to help distinguish between them.

Media Tiles

These tiles can display images, live streaming video from live feeds or display an uploaded video file on a loop. Audio from videos can be turned on or off.

Ticker

The ticker can be used to show up to 20 different statistics that loop round the screen. As with the multi-statistic tiles, each statistic added to the ticker can be given a different appearance to help distinguish between them.

> Only one ticker can be added to a Real-Time Dashboard view. It can either be located at the top or bottom of the view and has various options for size and speed.

Grid

Grid tiles provide real-time information about specific devices/calls rather than system wide. Grids are provided for agents, calls, extensions & trunks. In addition to summarised and current status information, grids provide third party control over other calls/device. Change an agent's ACD or DND status or move/steal telephone calls. To access the call/status control menu, left-click on the status icon at the far left of a row or the more icon (⋮) at the far right.

Full Screen

The full screen mode can be toggled* using the icon provided. When enabled, the browser frame/toolbar and the website title bar are removed so that the the dashboard fills as much of the screen as possible.

** Full Screen mode is not supported in all browsers*

Manual/External Statistics

If required, manually added data (Global Variables) or data from external databases can be displayed on any of the tiles. This is useful for displaying general information to users such as sales targets, promotions, support information etc.

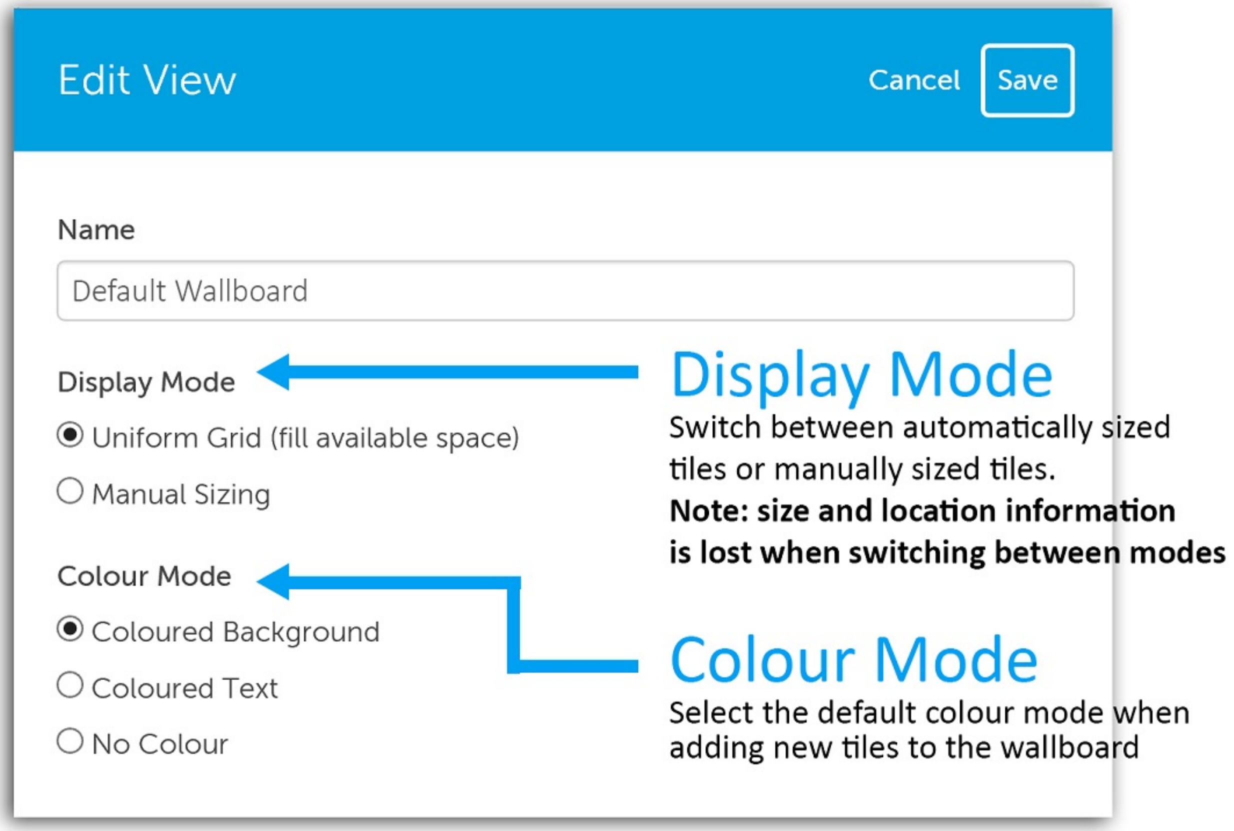
> Global Variables are edited in the configuration section ( ) of the website. This will only be available with the correct permissions.

> There is an additional licence for enabling external data sources.

The following guide is designed to provide an introduction to the core features of the Real-Time Dashboard.

View Settings

The dashboard provides real-time visibility of calls, extensions* and agents* on the telephone system. Each user can customise multiple views with a variety of tiles which can be filtered as required.



Display Mode

The display mode can be set to either 'Uniform Grid' (default) or 'Manual Sizing'. When uniform grid is enabled, the tiles on the wallboard will automatically resize as tiles are added or removed, simplifying the setup of the wallboard. When manual sizing is enabled, each tile must be individually located and sized. The benefit of manual sizing is that tiles can be different sizes if required.

> Switching between display modes will cause the tile location and sizing to be lost.

Colour Mode

The colour mode can be set to either 'Coloured Background' (default), 'Coloured Text' or 'No Colour' (black and white). When coloured background is selected, each new tile added will be given a randomly selected background colour with white text (recommended for viewing from a distance). When coloured text is selected, each new tile added is given a randomly selected foreground colour with a white background (recommended for viewing close up). When 'No Colour' is selected, each new tile added is given a white background with black text.

> The colour mode only affects new tiles that are added to the view. Existing tiles' backgound/foreground colour must be changed manually.

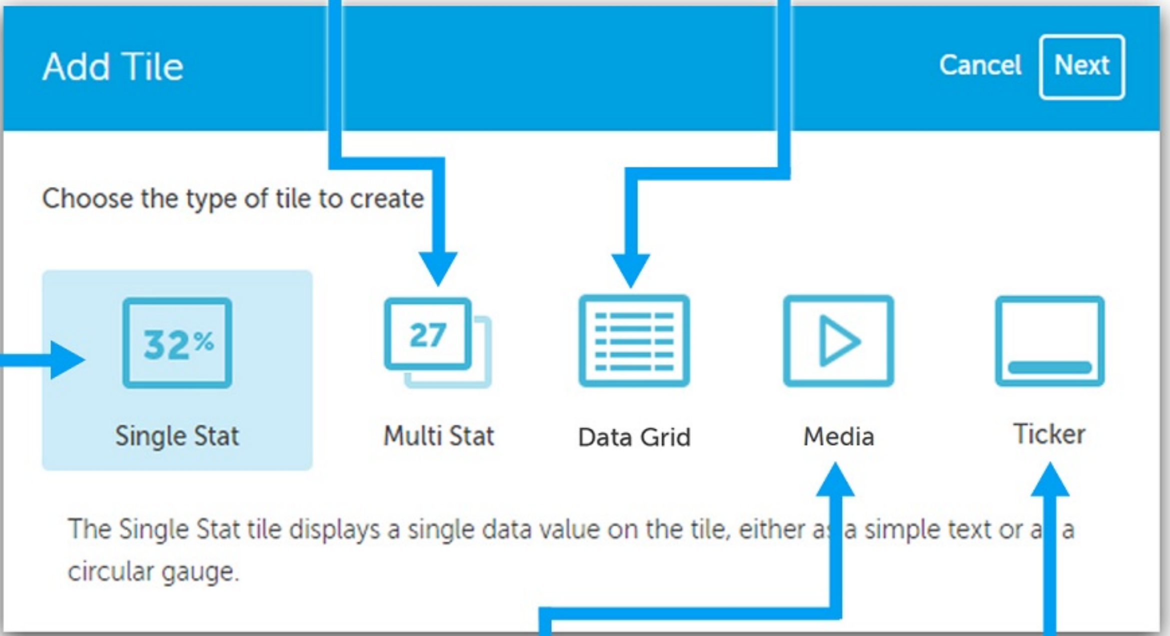
Edit Mode

To add new tiles or move/resize existing tiles, edit mode must be enabled. Press the edit ( ) icon on the top right-hand side of the view to enter edit mode. Once enabled the plus (+) icon can be used to add new tiles to the view. When pressed, the 'Add Tile' form is displayed, providing a choice between the different types of tiles available. Additionally, while in edit mode any existing tiles can be moved or resized (when using manual display mode). Press the tick ( ) icon to exit edit mode.

Single Stat
Create a tile that will display a single data value

Multi Stat
Create a multiple statistic tile that 'cycles' between selected statistics

Grid
View real-time data by Agent, Call, Extension or Trunk



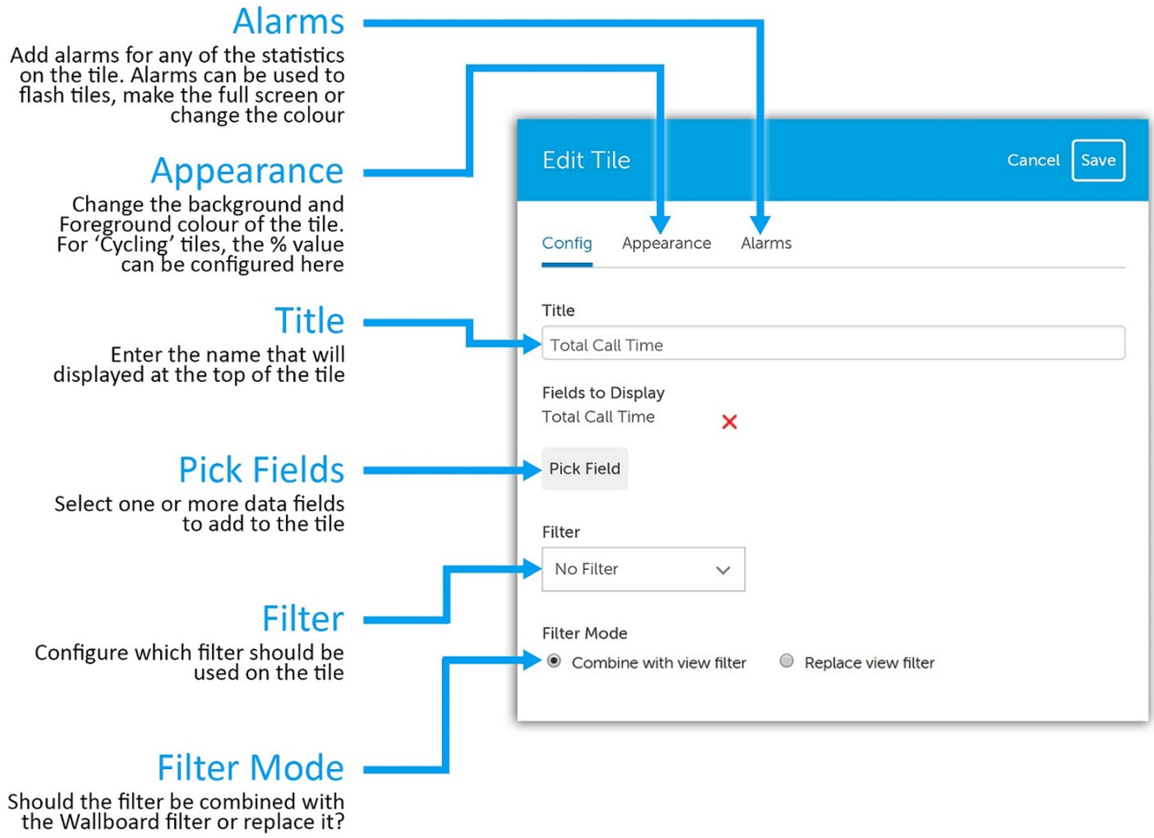
Media
Create a tile that will display an image, live steam or uploaded video

Ticker
Add a ticker to show one or more statistics. It can be located top or bottom of the screen and has options for size and speed

Once the tile type has been selected, press the 'Next' button to view the tile properties form.

> Only one ticker is allowed per Dashboard view. If there is already a ticker added, the ticker tile will not appear when adding new tiles.

Each tile has a set of properties so that it can be customised. The properties available will differ depending on the type of tile being edited/added. The image below shows the property form based on a single statistic tile.



Title & Fields

The title will be displayed at the top of the tile. By default, this will be set to the name of the data field selected, but can be changed. To add fields to a tile, press the 'Pick Field' button and then select the required field from the context menu. To aid selection, the fields have be grouped together into categories.

> For more information on the fields available and how they are calculated, please refer to the help file.

Filter & Filter Mode

The data on each tile can be filtered if required. By default no filter is applied. The filter mode is used to select whether the overall Wallboard view filter is applied or not. When set to 'Combined with view filter' (default), any filter set on the Wallboard view will be combined with any filter set on the tile. If set to 'Replace view filter' any filter set on the Wallboard view will be ignored.

> To ensure a tile never has a filter set, leave the filter set to 'No Filter' and select 'Replace view filter' as the filter mode.

Appearance

The appearance section provides access to change the foreground/background colour of the tile and also any other display options (such as 'Circular Gauge').

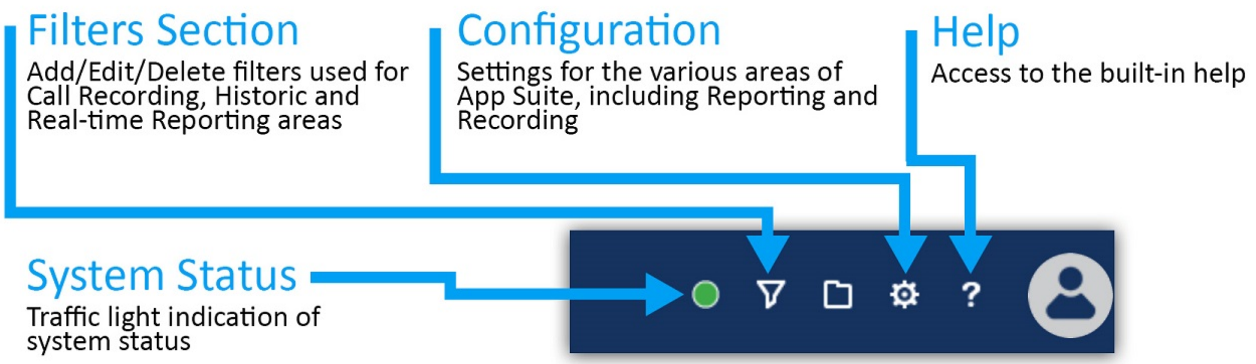
Alarms

Each tile can have one or more alarms configured. Alarms can be used to bring attention to tiles when thresholds are reached or breached. Alarms can be set to do the following:

- Flash the tile
- Make the tile full screen (double-click the tile to revert it back)
- Override the foreground/background colour
- Play a sound file

Overriding a tile's foreground and/or background colour is very useful for creating traffic light style tiles. For example, thresholds can be set to change a tiles colour from green to amber to red based on the data field's value. This can be used to help bring attention to specific performance targets.

The title bar provides access to areas of the App Suite. The image below outlines each of the navigation icons:

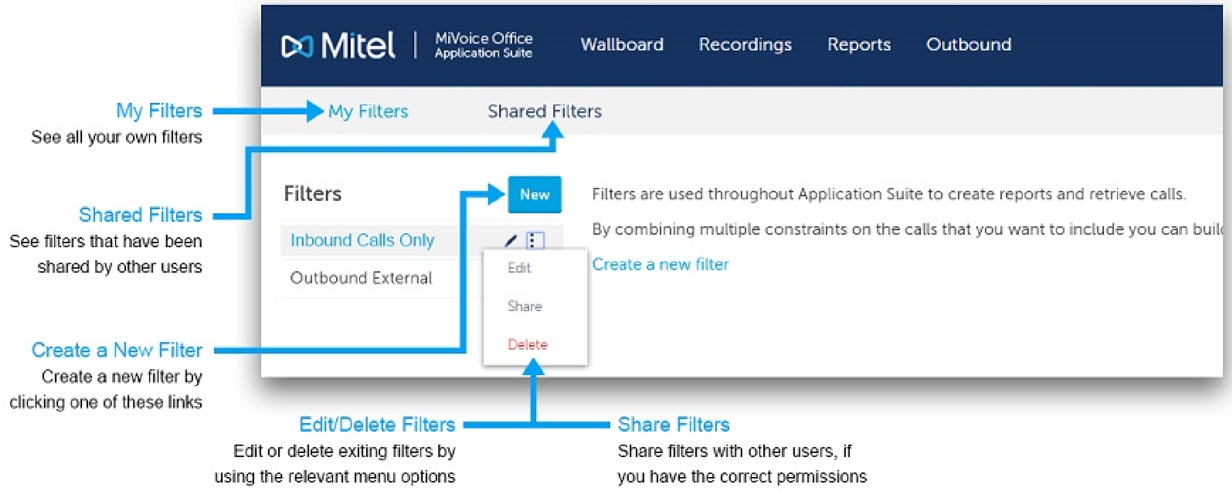


The configuration section and system status will only be visible with the correct permissions.

Filters

The 'Filters' section of the website is used to manage all the saved filters on the system. Filters can be used with reports or recordings.

Each user has their own 'My Filters' section that provides a list of all filters they have created.

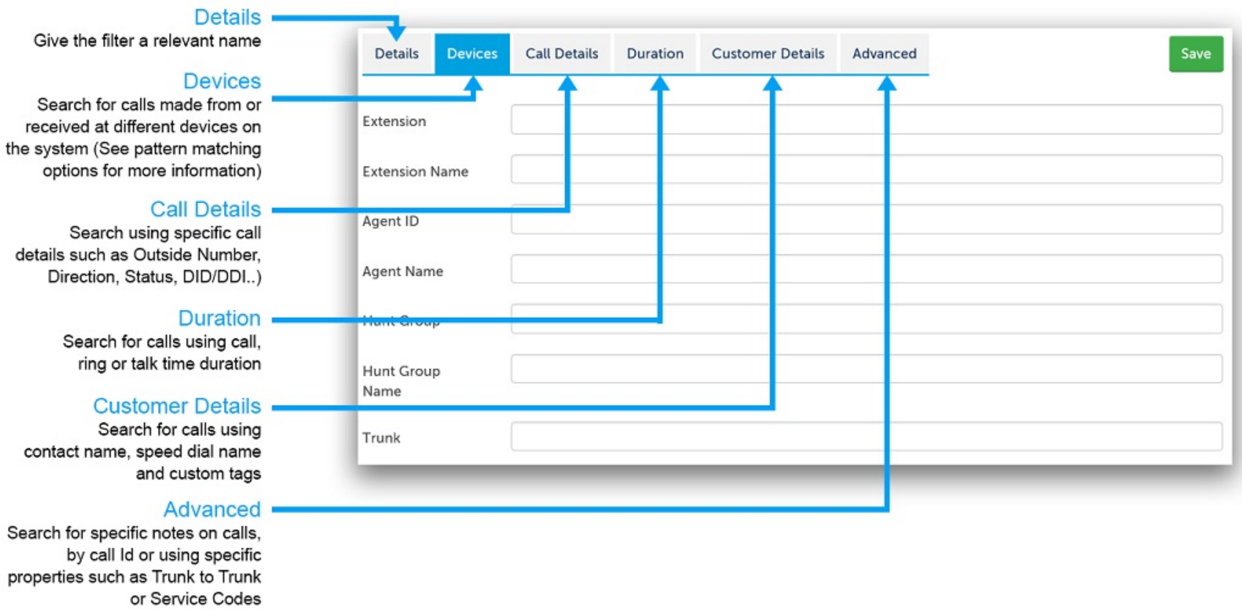


Shared Filters (Permission dependant)

Filters can be shared between users to avoid duplicating work and to allow administrative staff to set up filters that can be used by everyone.

Adding / Editing Filters

Each filter provides the ability to search on one or more details about a call. The details are grouped into tabs. The tabs are displayed with descriptions in the image below:



The use of special characters within the text boxes for a Filter enables the use of complex filter strings.

All Fields

The following characters are supported:

Special Characters	Description

Exclamation mark (!)	Not equal to
Percent (%)	Fuzzy matching (equivalent to a SQL LIKE %)
Underscore (_)	Fuzzy matching of a single character
Comma (,)	Can be used to search for multiple values at the same time

Device Fields

In addition to the special characters above, the following characters are supported when searching using a device based field (Extension, Agent, Trunk, Hunt Group):

Special Characters	Description
Plus sign (+)	Greater than or equal (e.g. 1000+ for extensions greater than or equal to 1000)
Hyphen (-)	Delimits a range of values to match (e.g. 1000-2000 for all extensions between 1000 and 2000 inclusive) or less than or equal to (e.g. -1000 for extensions less than or equal to 1000)

The example below shows what would be matched when entering combining multiple special characters using a comma:

- 1000-1005,!1003,1040,18%5,2000+

Matching endpoints: 1000, 1001, 1002, 1004, 1005, 1040, any that start with 18 and end with a 5, any with a value greater or equal to 2000.

> Device numbers are stored as text so when using greater than or less than, it is compared on an alphabetic level not a numeric level

3.3 Real-Time Wallboard

The Real-Time Wallboard is designed to provide real-time statistics on a screen that is visible from across a room if necessary.

Wallboard licenses are used on a per concurrent connection basis, each user that has a Wallboard view open within a browser will consume a Wallboard license.

> Opening multiple tabs with Wallboards on will use multiple licenses.

Each Wallboard has a single Real-Time View which can contain any of the following tile types:

- Single Statistic
- Cycling Multiple Statistic Tile
- Ticker (limited to one per view)
- Media

The following sections of the document provide more information on various aspects of the Real-Time Wallboard:

- Views
- Tile Types
- Appearance
- Filtering
- Alarms
- Full Screen

A user's access to the Real-Time Wallboard is controlled using the Security Profile that has been assigned to their user account.

3.4 Real-Time Dashboard

The Real-Time Dashboard is designed to provide real-time statistics to a supervisor/manager. It provides all the features of the Real-Time Wallboard but with the following additional features:

- Multiple Views, users are not restricted to a single view. Multiple views can be configured to show different aspects of the system. Users can then switch between views as required.
- Grid Tiles, the dashboard provides access to grid based tiles. These provide information on a device/call basis for more detailed real-time analysis
- Multiple Statistic Tiles, these provide improved support for displaying multiple statistics on a tile and include the Primary/Secondary and List based appearances.
- Call/Status Control, this provides the user with the ability to change another user's status or to move calls around the telephone system

Dashboard licenses are used on a per concurrent connection basis, each user that has a Dashboard view open within a browser will consume a Dashboard license.

> Opening multiple tabs with Dashboards on will use multiple licenses.

Each Dashboard provides access to configure multiple Real-Time Views which can contain any of the following tile types:

- Single Statistic
- Multiple Statistic Tile
- Ticker (limited to one per view)
- Media
- Grids

The following sections of the document provide more information on various aspects of the Real-Time Dashboard:

- Views
- Tile Types
- Appearance
- Filtering
- Alarms
- Full Screen
- Call Control

A user's access to the Real-Time Dashboard is controlled using the Security Profile that has been assigned to their user account.

3.5 Real-Time Views

A Real-Time View is a collection of real-time tiles. On the Wallboard, only a single view is visible. On the Dashboard, multiple views can be added by the user.

Each view has the following configuration options:

- Name, the user definable name for the view (this is not available on the Wallboard)
- Display Mode, switch between different tile layout modes
- Colour Mode, switch between different colour modes that applies when creating new tiles.

To access the configuration of a view, Press the edit button ( ) to the top left of the Wallboard/Dashboard.

Display Mode

The display mode controls how the tiles in the view are located and sized.

Uniform Grid

Default for Wallboards.

When set in this mode, each tile's size is automatically controlled by the view. As new tiles are added, the size of existing tiles is reduced so each tile has the same size and they all fit in the optimum way on the view.

The location of tiles can be changed by dragging and dropping tiles within the view.

Manual Sizing

Default for Dashboards.

When set in this mode, each tile's size is directly controlled by the user. This provides a more flexible view where tiles can be different sizes. This mode is ideal for when using the Media Tile and allows it to be large than the other tiles around it.

> When switching between modes, the order and size of tiles will be lost.

> Neither of the Display Mode options will affect a Ticker Tile. These will display at the top or bottom of the screen based on their own display mode setting.

Colour Mode

The colour mode controls how the background/foreground of tiles are automatically generated by the system when new tiles are added.

> Changing the colour mode has no effect on tiles that have already been added to the view.

Coloured Background

Default for Wallboards.

When this mode is selected, a random background colour will be selected for any new tiles added and the foreground (text) will be set to white.

Coloured Text

Default for Dashboards.

When this mode is selected, a random foreground (text) colour will be selected for any new tiles and the background will be set to white.

No Colour

When this mode is selected, all new tiles added will start with a white background and blank foreground (text).

> The colour mode only affects the initial colour of the tile and is designed to simplify initial view creation. The foreground and background colours can be changed as required by the user at any time.

3.6 Real Time Tiles

The following table shows the types of tile that are available, what sort of data they can display and which real-time license they are supported on.

Tile	Data	Wallboard	Dashboard
Single Statistic	• Aggregated (Totals/Averages/Percentages) • Minimum/Maximum Values • Global Variables • External Data	Yes	Yes
Multiple Statistic	• Aggregated (Totals/Averages/Percentages) • Minimum/Maximum Values • Global Variables • External Data	Cycling Statistic Tile Only (Limited to 2 Statistics)	Yes
Ticker	• Aggregated (Totals/Averages/Percentages) • Minimum/Maximum Values • Global Variables • External Data	Yes (Limited to 1)	Yes (Limited to 1 per View)
Media	• YouTube Live Streams • Uploaded MP4/M4V Video • Images	Yes	Yes
Grids	• Agent Grid* • Call Grid • Extension Grid • Trunk Grid	No	Yes

* Requires ACD Reporter licenses

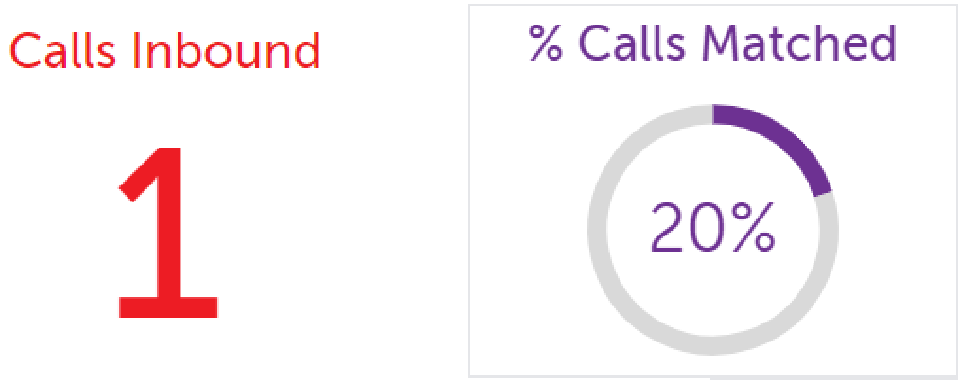
Single Statistic Tiles

One or more of these tiles can be added to a view. Each tile can show a single piece of information at a time and can have it's fore/background colour customized as required.

Single statistic tiles have two display modes:

- Text
- Circular Gauge

Example single statistic tiles:



Multiple Statistic Tiles

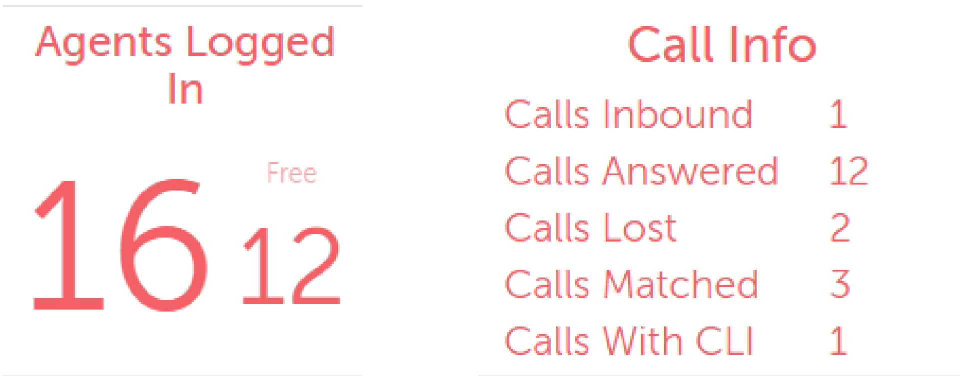
One or more of these tiles can be added to any real-time view (limited to cycling tiles only on a Wallboard view). The multiple statistic tile can be configured with up to 20 pieces of information. There are three display modes to choose from when creating a multiple statistic tile:

- Primary / Secondary, up to 2 pieces of information can be displayed using this mode.
- List, up to 20 pieces of information can be displayed on the tile with this mode.
- Cycle, the tile will cycle through up to 20 pieces of information in this mode. Only one statistic will be visible at a time.

Once the tile has been created, the display mode can be changed at anytime from the tile's appearance tab.

The foreground colour of each statistic added can be configured separately so they can be distinguished from each other.

Example multiple statistic tiles:



> On Real-Time Wallboards, Cycling tiles are limited to 2 statistics per tile.

Ticker

A single ticker tile can be added to a view. The ticker can have up to 20 pieces of information added to it. There are three appearance options associated with the ticker:

- Location, the ticker can be located at the top or bottom of the view
- Size, the ticker has three size modes: Small, Normal & Large

- Scroll Speed, the ticker has three speed modes: Slow, Normal & Fast

Each piece of information added to the tile will scroll along it in the order it was added. If there are a large amounts of data on the ticker it may not be possible to see all pieces of information at the same time.

Example ticket tile:

Agents Free **12** Calls Ringing **0** Calls Active **0** Call Rate **1** Calls Inbound **1** Calls Answered

Media

One or more media tiles can be added to a view. Each media tile can be configured to play one of the following:

- Local content, the tile will loop an MP4 video provided by the user
- YouTube Videos, the tile can display video and live streams from YouTube. Simply paste in the URL for the specific video/stream.
- Display an image file

If displaying video content, the media tile will start with the audio on. However, this can be changed by the user.

> ⚠ Depending on the media content being displayed, there may be specific license requirements either in the form of a 'TV License' and/or in the form of a license from the content provider. It is up to the customer to ensure they are licensed correctly to display any content they choose to add to the media tile.

Grids (Agent, Call, Extension & Trunk)

One or more grid tiles can be added to a view. Grid tiles can be used to show data by device or call rather than system wide.

Agent Grid

Displays all the ACD agents on a system with the background colour for each row indicating their ACD status. The agent grid can be filtered as per any other tile but also has the option for not displaying agents that are currently logged out.

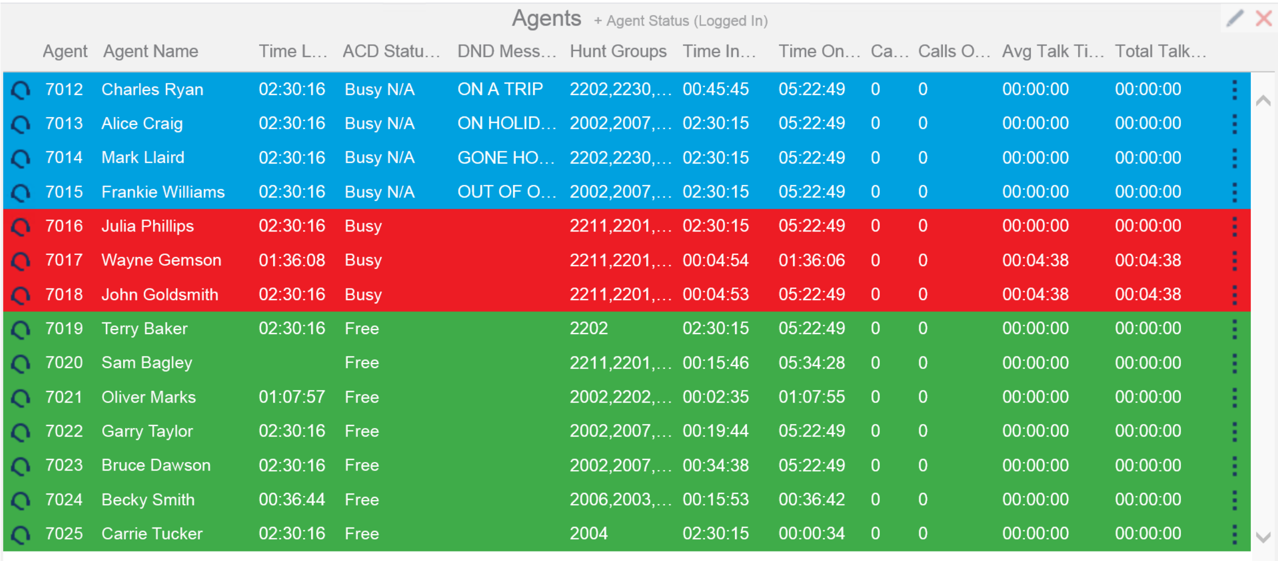
Background Colour	Status
White	Logged Out
Green	Free
Red	Busy (On a call)
Yellow	Wrap-Up
Blue	Do-Not-Disturb
Grey	Unlicensed

The table below shows the status icons that are shown on an Agent Grid.

Icon	Description
	Logged In
	Logged Out

	Call In Progress
	Busy N/A (Do-Not-Disturb)

The screen shot below shows an example Agent Grid.



Agents + Agent Status (Logged In)

Agent	Agent Name	Time L…	ACD Statu…	DND Mess…	Hunt Groups	Time In…	Time On…	Ca…	Calls O…	Avg Talk Ti…	Total Talk…
7012	Charles Ryan	02:30:16	Busy N/A	ON A TRIP	2202,2230,…	00:45:45	05:22:49	0	0	00:00:00	00:00:00
7013	Alice Craig	02:30:16	Busy N/A	ON HOLID…	2002,2007,…	02:30:15	05:22:49	0	0	00:00:00	00:00:00
7014	Mark Llaird	02:30:16	Busy N/A	GONE HO…	2202,2230,…	02:30:15	05:22:49	0	0	00:00:00	00:00:00
7015	Frankie Williams	02:30:16	Busy N/A	OUT OF O…	2002,2007,…	02:30:15	05:22:49	0	0	00:00:00	00:00:00
7016	Julia Phillips	02:30:16	Busy		2211,2201,…	02:30:15	05:22:49	0	0	00:00:00	00:00:00
7017	Wayne Gemson	01:36:08	Busy		2211,2201,…	00:04:54	01:36:06	0	0	00:04:38	00:04:38
7018	John Goldsmith	02:30:16	Busy		2211,2201,…	00:04:53	05:22:49	0	0	00:04:38	00:04:38
7019	Terry Baker	02:30:16	Free		2202	02:30:15	05:22:49	0	0	00:00:00	00:00:00
7020	Sam Bagley		Free		2211,2201,…	00:15:46	05:34:28	0	0	00:00:00	00:00:00
7021	Oliver Marks	01:07:57	Free		2002,2202,…	00:02:35	01:07:55	0	0	00:00:00	00:00:00
7022	Garry Taylor	02:30:16	Free		2002,2007,…	00:19:44	05:22:49	0	0	00:00:00	00:00:00
7023	Bruce Dawson	02:30:16	Free		2002,2007,…	00:34:38	05:22:49	0	0	00:00:00	00:00:00
7024	Becky Smith	00:36:44	Free		2006,2003,…	00:15:53	00:36:42	0	0	00:00:00	00:00:00
7025	Carrie Tucker	02:30:16	Free		2004	02:30:15	00:00:34	0	0	00:00:00	00:00:00

> To use an Agent Grid, ACD Reporting licenses are required in addition to the Real-Time Dashboard license. If any agent does not have a license, they will display with a grey background.

> MCS does not support ACD member hunt groups, only ACD agent groups.

Call Grid

Displays all active calls on the system (internal & external) with the background colour for each row indicating the calls status.

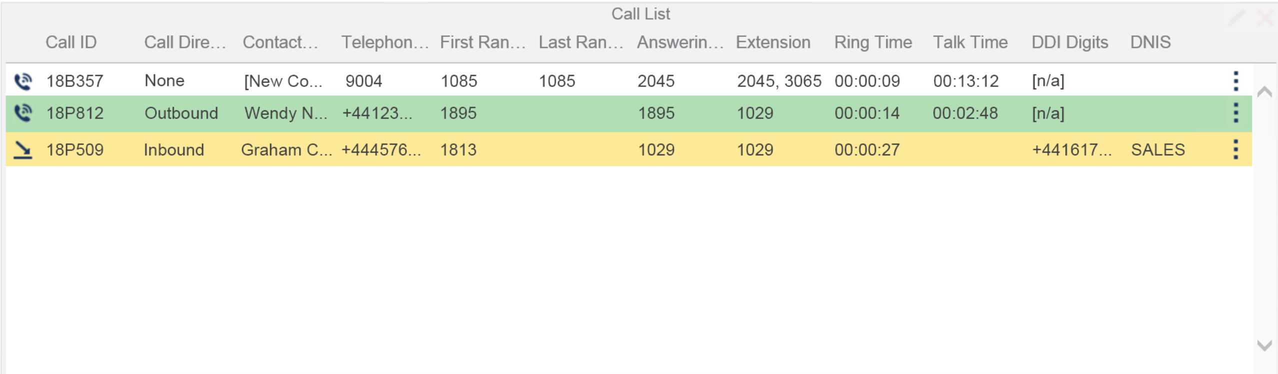
Background Colour	Status
White	Internal Call
Green	Outbound Call
Yellow	Inbound Call

The table below shows the status icons that will display on a Call Grid.

Icon	Description

	Call In Progress
	Call On Hold
	Call Ringing In
	Call Ringing Out

The screen shot below shows an example Call Grid with an inbound, outbound and an internal call.


Call List

Call ID	Call Dire…	Contact…	Telephon…	First Ran…	Last Ran…	Answerin…	Extension	Ring Time	Talk Time	DDI Digits	DNIS
18B357	None	[New Co...	9004	1085	1085	2045	2045, 3065	00:00:09	00:13:12	[n/a]	
18P812	Outbound	Wendy N...	+44123...	1895		1895	1029	00:00:14	00:02:48	[n/a]	
18P509	Inbound	Graham C...	+444576...	1813		1029	1029	00:00:27		+441617...	SALES

Extension Grid

Displays all the extensions configured on the system with the background colour of each row indicating the trunk/call status.

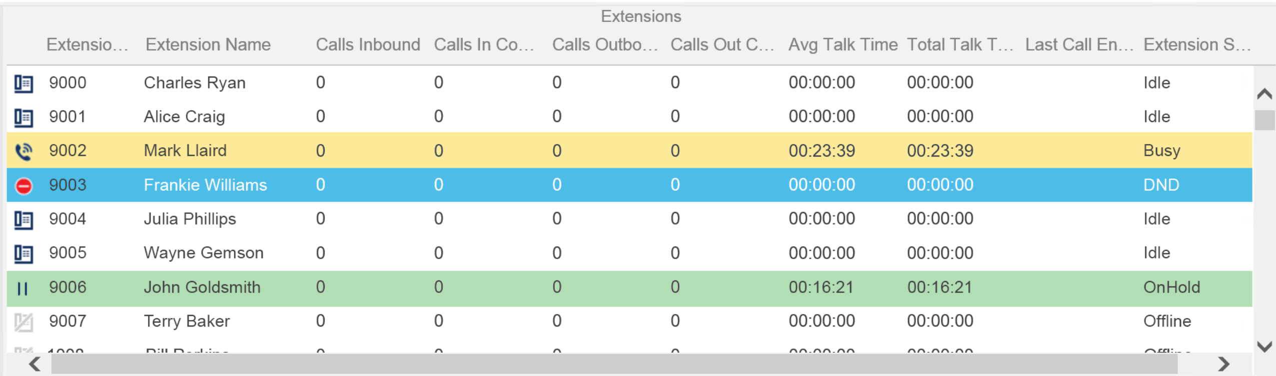
Background Colour	Status
White	Idle (No call)
Green	Outbound Call
Yellow	Inbound Call
Grey	Offline

The table below shows the status icons that can be displayed on an Extension Grid.

Icon	Description
	Extension Idle
	Extension Offline

	Call In Progress
	Call On Hold
	Call Ringing In
	Call Ringing Out
	Do-Not-Disturb

The screen shot below shows an example Extension Grid.



Extensions

Extensio…	Extension Name	Calls Inbound	Calls In Co…	Calls Outbo…	Calls Out C…	Avg Talk Time	Total Talk T…	Last Call En…	Extension S…
9000	Charles Ryan	0	0	0	0	00:00:00	00:00:00		Idle
9001	Alice Craig	0	0	0	0	00:00:00	00:00:00		Idle
9002	Mark Llaird	0	0	0	0	00:23:39	00:23:39		Busy
9003	Frankie Williams	0	0	0	0	00:00:00	00:00:00		DND
9004	Julia Phillips	0	0	0	0	00:00:00	00:00:00		Idle
9005	Wayne Gemson	0	0	0	0	00:00:00	00:00:00		Idle
9006	John Goldsmith	0	0	0	0	00:16:21	00:16:21		OnHold
9007	Terry Baker	0	0	0	0	00:00:00	00:00:00		Offline

Trunk Grid

Displays all trunks that are active on calls. The background colour indicates the direction of the call (Yellow -> Inbound, Green -> Outbound). The Icon to the left shows the status of the call.

Background Colour	Status
White	Internal Call
Green	Outbound Call
Yellow	Inbound Call

The table below shows the status icons that can be displayed on a Trunk Grid.

Icon	Description
	Call In Progress
	Call On Hold

	Call Ringing In
	Call Ringing Out

The screen shot below shows an example Trunk Grid.

Trunks											
Trunk	Call Dire…	Contact…	Telephon…	First Ran…	Last Ran…	Answerin…	Extension	Ring Time	Talk Time	DDI Digits	DNIS
94301	Inbound	[New Co…	+441618…	2522	1834	1032	1032	00:00:23	00:02:31	+441617…	MAIN
94302	Inbound	CHRIS R…	+447968…	1828	1828		1828	00:00:03		+441617…	CHRIS R…
94303	Inbound	James P...	+449876...	1872	2531	1046	1046	00:00:07	00:05:19	+441617...	SALES
94304	Inbound	Graham C...	+444576...	1813	1811	1029	1029	00:00:27	00:02:48	+441617...	SALES
94305	Inbound	Mark B...	+444123...	2501	1862		1042	00:00:19		+441617...	SUPPOR...
94309	Outbound	Grace H...	+441958...	1863			1863	00:00:22		[n/a]	
94309	Outbound	Mary M...	+445820...	1871			1871	00:00:20		[n/a]	
94310	Outbound	Phil C...	+449756...	1845			1845	00:00:31	00:11:15	[n/a]	
94311	Outbound	Garry M..	+449856...	1804			1804	00:00:12		[n/a]	
94312	Outbound	Chris Ra…	+447968…	1828			1828	00:00:05		[n/a]	

A maximum of 20 columns can be added to a real-time grid at a time.

3.7 Real-Time Tile Properties

Each tile has a set of properties that control various aspects of the tile's look and feel as well as the data displayed.

Title & Fields to Display

The title will be displayed at the top of a tile that is added to a view. The title of a tile will automatically be defaulted to the name of the first data field that is selected to be displayed on the tile.

Depending on the tile type, one or more data fields can be added to the tile for display. To add a field, press the 'Pick Field' button and select the field required from the context menu displayed.

The fields that are available will depend on the tile type. For more information on the fields available, please refer to the following sections:

- Statistics
- Global Variables

> The Media tile has different properties to other tile types. Please refer to the Tile Types section for more information.

On multiple statistic tiles, the name of the data field selected will be used to identify the statistic when it is displayed. This can be overridden if required. While the 'Edit Tile' window is open, click on any of the fields and text box will appear allowing the name to be overridden.

The order of fields added can also be changed by drag and drop.

Appearance

The appearance tab provides configuration of the background and foreground colours of the tile, as well as any Display Mode options that may be relevant to the specific tile being edited. On multiple statistic (list) tile, the colour of each of the fields that have been added can be changed.

Each tile also has properties for filtering and alarms. For more information, please refer to the Real-Time Filtering & Real-Time Alarms Sections.

3.8 Real-Time Filtering

By default, when tiles are added to a Real-Time View, they will show unfiltered data. This means that the data will include all relevant calls/extension etc.

Under normal circumstances, it is necessary to apply a filter to a tile so that the data displayed is meaningful.

Any of the following filters can be used to filter the data on a tile:

- Built-In filters
- User Filters
- Shared Filters

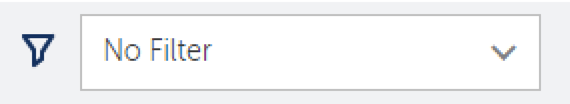
For more information on different filters and how they are managed, please refer to the Filters section.

There are two ways in which filters can be used on a Real-Time View:

- Tile filters, apply a filter directly to a tile
- View filters, apply a filter to all tiles within a view

Applying View Filters

At the top of the current Real-Time View, the filter dropdown will indicate if there is a filter currently assigned. In the image below, there is no filter assigned at view level:



To apply a filter to all the tiles within a view, select the required filter from the drop down.

To add a new filter or edit an existing one, press the filter icon ( ) on the title bar to access the filter configuration section.

Tile Filters

Each tile can control how filters are applied to the data it is showing. The filter options available on each tile are:

- Filter, select a filter to apply to this tile
- Filter Mode, choose how the filter is applied

Each tile can have a filter applied to directly to it. By default, a tile will have no filter applied.

The Filter Mode can then be used to control whether any filter applied to the tile is combined with or overrides any view based filter.

If 'Combine with view filter' is selected, the view and tile base filter are merged together and applied to the data on the tile.

If 'Replace view filter' is selected, the view filter is ignored and the tile's filter is applied. If the tile has no filter applied when this mode is selected, the view's filter is still ignored and the tile's data will not be filtered.

Filter Visibility

Depending on the Filter Mode selected on the tile, any filter applied to the tile will be displayed below the tile name.

If the filter is combined with the view's filter, it will be displayed with a (+) next to the filter name:

Calls Lost
+ Agent (1002)

If the filter is set to replace the view's filter, just the filter name will be displayed:

Calls Lost
Agent (1002)

3.9 Real-Time Alarms

Real-Time Alarms provide a way to bring attention to aspects of the telephone system that are running outside of acceptable parameters. Each tile on the system can have one or more real-time alarms configured.

To add an alarm, navigate to the 'Alarms' tab while editing a tile, then press the 'Add New Alarm' button. Once the alarm properties have been configured, remember to save the tile as well as the newly added alarm.

More than one alarm can be added to a tile to handle different scenarios.

> Real-Time Alarms are not available on Media tiles.

Triggers

The trigger defines when the alarm should be activated. The following comparisons can be used for trigger configuration:

- >
- <
- =
- Between (inclusive)

The alarm created will be active for as long as the statistic matches the trigger configured.

If the alarm is being created on a multiple statistic tile, the statistic the trigger will be calculated against must be selected.

Actions

For each real-time alarm created, one or more of the following actions can be configured.

Flash Tile

This action will cause the tile's foreground and background colours to swap back and forth, causing the tile to flash to get peoples attention. The tile will continue to flash while the conditions that caused the trigger remain.

Change Background Colour

This action will cause the background colour of the tile to change to the configured colour. The background will revert back to its normal colour when the trigger is no longer valid.

> This action type can be used to create a traffic light style tile, where the background colour can be changed from green to yellow to red based on changing statistic values.

Change Stat Colour

This action will cause the foreground colour of the tile to change to the configured colour. The foreground will revert back to its normal colour when the trigger is no longer valid.

Make the tile fill the screen

This action will cause the tile to display full screen on the view, in front of all other tiles. The tile will revert back to it's original size and location when the trigger is no longer valid or by double clicking on the tile.

Play a sound

This action will cause a sound/music file to be played out of the configured speakers of the computer. The 'Play Count' setting can be used to control how many times the file is played (*Default 1*).

Any sound/music files that have been added within the logged in user's Folders. The system will display any files ending with the .mp3 file extension.

For information on how to upload sound files, please refer to the Folders section.

3.10 Real-Time Full Screen

The wallboard is designed to be used on a wall mounted display screen, visible to multiple users at a time. To optimise this usage, a full screen toggle ( ) is provided which activates the browsers full screen mode This can be found in the top right of the View.

When full screen mode is enabled, the browser's application border along with the main title bar for the website should be hidden, allowing the view to grow to the size of the screen.

Opening the Wallboard Full Screen

In most circumstances where a wall mounted display is used, a dedicated PC will be installed to drive the screen and run the browser that the wallboard will be displayed in.

When this setup is used, the PC and wallboard need to handle reboots and come back to an operational state without any user intervention. For this to happen, the following needs to take place:

1. The PC needs to be configured to automatically logon after a reboot
2. A shortcut needs to be called on start-up that opens the browser at the appropriate page
3. The MiVoice Office Application Suite website needs to have 'Use Windows Authentication' enabled so it automatically logs the user in.

Auto PC Logon

> Configuring a PC to automatically logon can be a security risk. Before doing this, ensure the user account to be used as no access beyond that of the target computer.

To setup a computer to automatically logon, the following keys need to be added to the registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon

- AutoAdminLogon = 1
- DefaultDomainName = [Your domain name]
- DefaultUsername = [Wallboard username]
- DefaultPassword = [Wallboard user account password]

Once these keys have been created and their values populated, the PC should automatically logon each time it is rebooted.

Browser Shortcuts

When using Internet Explorer or Chrome, it is currently possible to load the browsers in 'Kiosk' mode. This will take the browser straight to the specified URL and will load it full screen. In addition, it will stop general interaction with the website.

To activate Kiosk mode, create a shortcut for the browser required:

Internet Explorer:

"C:\Program Files\Internet Explorer\iexplore.exe" -k http://[APP_SUITE_SVR]/Secure/Dashboard/Index

Chrome:

"C:\Users\[USERNAME]\AppData\Local\Google\Chrome\Application\chrome.exe" -Kiosk "http://[APP_SUITE_SVR]/Secure/Dashboard/Index" http://[APP_SUITE_SVR]/Secure/Dashboard/Index

> At the time of writing, there is no way to automate loading a URL in Full Screen mode in either Firefox or Edge.

Windows Authenticated Website Login

If MiVoice Office Application Suite has been installed on a Windows Domain, the website can be configured to automatically log users in with their windows credentials, saving them the effort of typing out their username and password each time.

This is extremely useful when setting up a Wallboard to automatically load when a PC starts up. To make use of this feature, ensure the steps below are followed:

- Enable 'Use Windows Authentication' in the Website settings (''\Servers\Website)
- Make sure the Windows Username parameter is set against any user wishing to use the feature.
- Configure the browser to recognise the MiVoice Office Application Suite URL as a Local Intranet site.

Once the steps above have been correctly followed, anytime a configured user browses to the MiVoice Office Application Suite website, they will automatically be logged on.

3.11 Real-Time Global Variables & External Data

In most implementations of the Real-Time Wallboard/Dashboard, there is a requirement to display information that comes from outside of the telephone system. This information could relate to other areas of the business which also need monitoring. Two methods are provided to display non-telephone system related information:

- Global Variables, manually updated data fields
- External Data, automatically updated data that is queried from an external data source

If global variables and/or external data fields have been configured on the system, they will appear on the context menu when adding a field to a tile. No formatting is applied to these fields, the data will appear on the tile in exactly the format it has been entered/queried.

Global variables and external data fields can be added to the following tile types: Single Statistic, Multiple Statistic & Ticker.

Global Variables

Global variables can be created, edited or deleted by any user that has the appropriate permission. For more information on managing global variables, please refer to the dedicated section within the Call Reporter configuration.

External Data Sources

External data sources can be created, edited or deleted by any user that has the appropriate permission. For more information on managing external data fields, please refer to the dedicated section within the Call Reporter configuration.

4 Recording

Overview

If the MCS is licensed for Call Recording the recordings section will be visible on the main toolbar. Selecting Recordings on the toolbar will open up the a window that allows users to find and playback recordings.

The left hand side has the filtering options that control what calls are displayed on the grid on the right. The calls can be filtered down by:

- Date Range - the date range option is shown above the grid and provides easy access to modifying the date range of the calls.
- Business Unit Filters - the business unit that the User who handled the call is assigned to.
- Filter Details - these are filters that have been created and saved by a User for common conditions.
- Additional Filters - these are ad hoc conditions that need to be added each time.

> If the MCS has Call Recording licenses but the Recordings section is not visible, the user logged into the website does not have permission to view recordings. To give a user permission, apply and Access Scope or Access filter to their role.

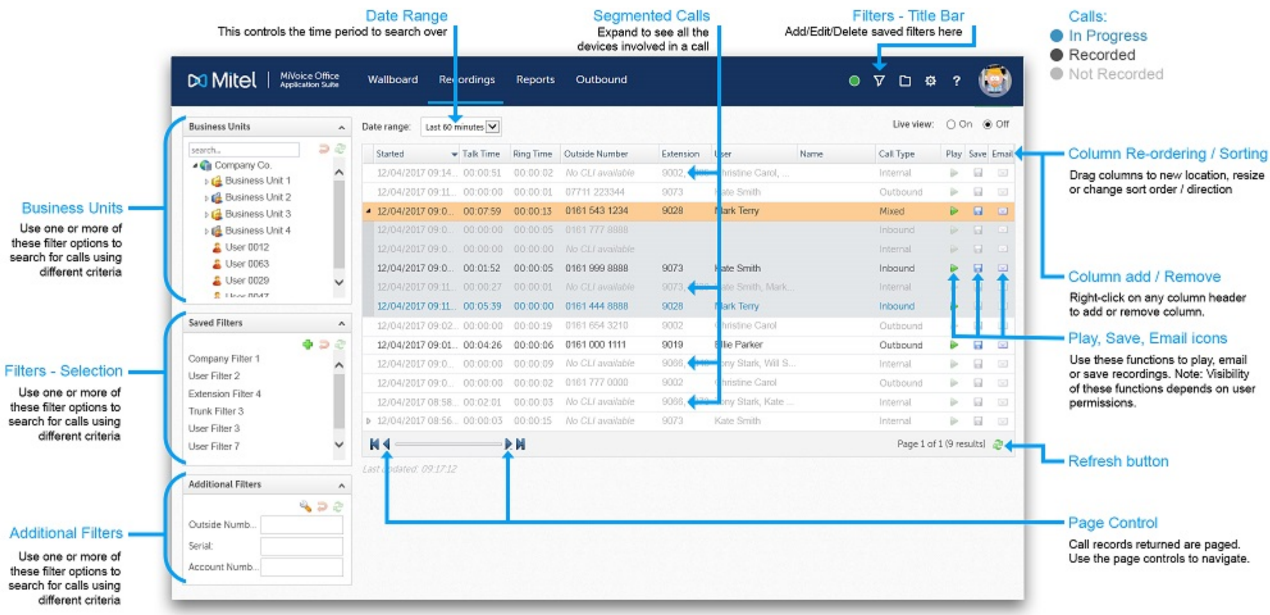
The right hand side shows the list of calls that match the filters that are currently selected, see the Recordings Grid section for more details.

4.1 Call Recorder Quick Reference Guide

The following guide is designed to provide an introduction to the call recording search and playback features of the MiVoice Office Application Suite.

Recordings

The recordings page provides access to search for recorded calls. The page is split into two sections; on the left side are search tools that can be used to search for specific calls or types of calls. On the right side is the recordings grid, this shows a list of all calls that match the current search criteria.



Segmented Calls

The system creates a new call segment each time a call rings or gets answered by a different device on the telephone system. To help locate calls, they are grouped together so that a call's route through the telephone system can easily be tracked. The image above shows a segmented call that has been expanded to display each call segment.

Call Status

The colour of the text in the recordings grid denotes its status. Blue text indicates that a call is currently in progress on the telephone system (with the correct permission, these can be listened to live). Grey text indicates that a call was not recorded. Black text indicates that a call was recorded and is now finished.

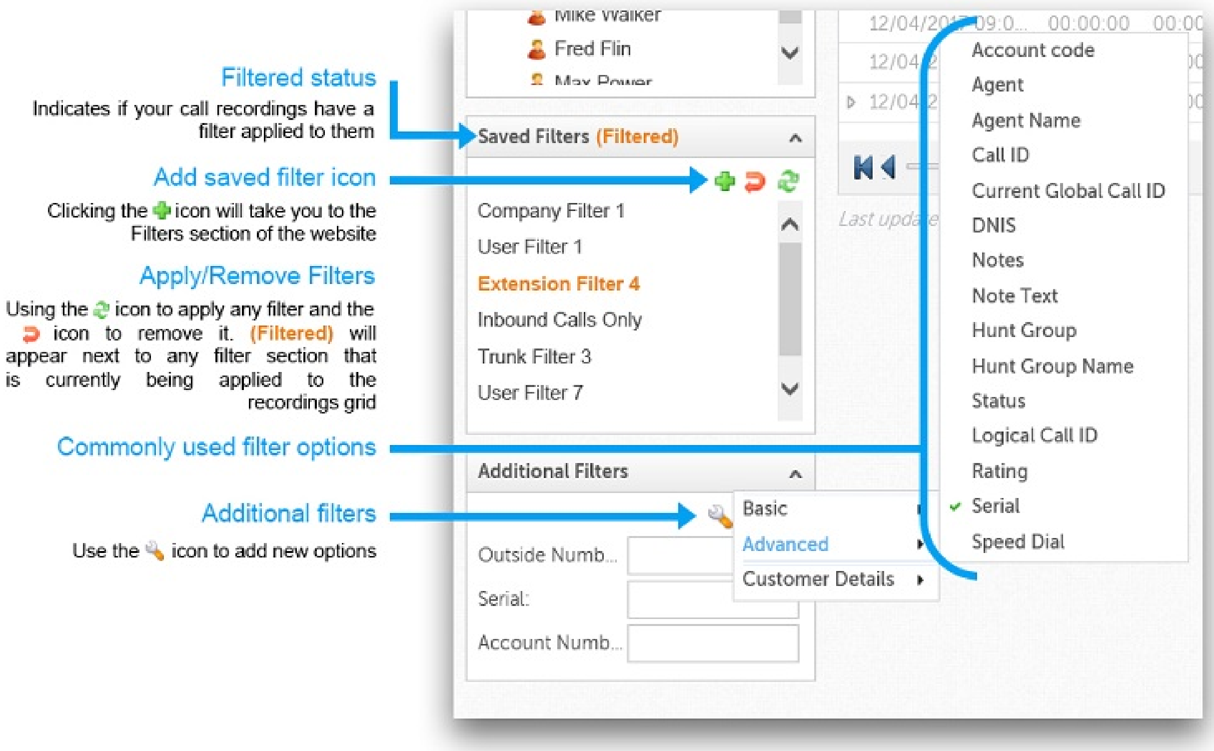
There are many reasons why a call may not have been recorded, hovering over the play icon with the mouse will display a tool-tip which will indicate why a call was not recorded.

Date Range

The date range is used to select the time period to search for calls to show in the recordings grid. A limited number of calls can be displayed in the call grid, if the date range to be searched is large, it is recommended that additional filters are also applied to reduce the number of calls returned by the search.

Searching for Calls

Using the search tools on the left side of the screen, it is quick and easy to find specific calls. The 'Business Unit' section can be used to search for calls for specific users or departments. The 'Saved Filters' section can be used to apply a filter that you or someone else has previously created. The 'Additional Filters' section can be used to create single use filters. One or more of these methods can be used to reduce the number of calls displayed in the recordings grid. Remember to use the refresh button to apply any new filters.



Business Units

This section shows the business units (departments/teams) and people within the organisation. Applying a filter for a specific business unit will filter the recordings grid to show only calls made by people that are a member of the unit. Alternatively, individual users can be selected. Select more than one user by holding down the Ctrl or Shift key and selecting the users required.

Saved Filters

Each user's personal filters and filters that have been shared by other users will be visible here. These can be applied to the recordings grid as required. To manage filters, navigate to the filters section (⊽) of the website using the main title bar.

Additional Filters

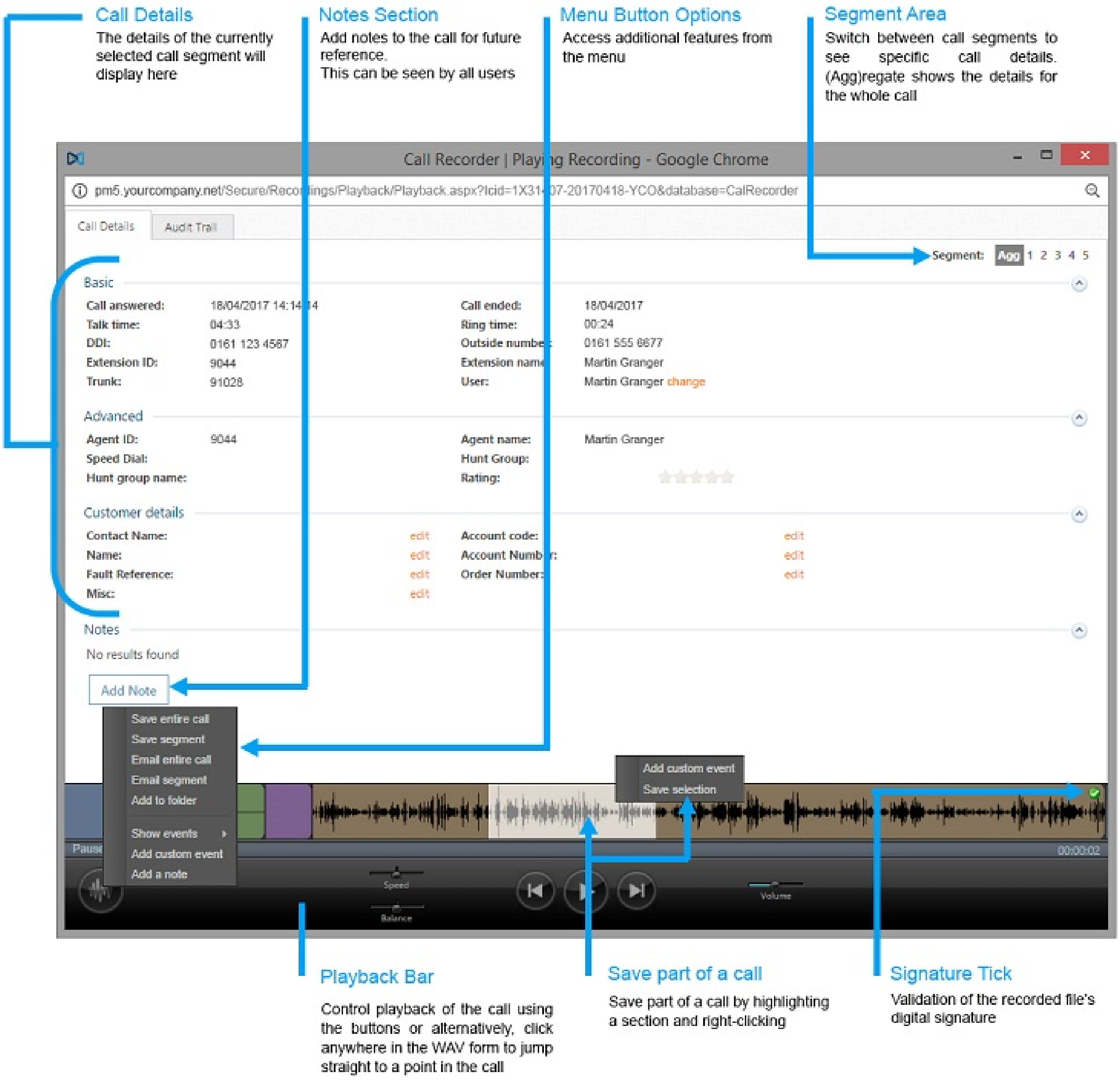
The most commonly used ad-hoc search criteria are displayed by default. Text can be entered into any of options displayed and applied to the recordings grid using the refresh button. Search options can be added or removed from this section using the spanner.

Security/Permissions

Access to recordings and recordings management (Playback, Save, Email) can be strictly controlled using security profiles. Depending on the profile assigned, not all calls may be displayed in the recordings grid. If you cannot find a specific call, please contact your system administrator to ensure you have the correct permissions.

Playback Window

The playback window will show whenever the play icon is selected in the recordings grid. The call details tab provides all the data the system has stored about the call. The segment selector in the top right of the page can be used to look at the details of individual segments. The (Agg)regate option shows the durations for all segments added together.



Call Navigation

Each segment of call is displayed along the bottom of the playback window in a different colour. Playback of calls can be controlled using the media control buttons or by simply clicking at different locations along the timeline. The black lines within the coloured segments is the 'Waveform' for the call. It indicates the existence of audio within the call. If a segment is displayed without any waveform at all, it has not been recorded.

Saving/Emailing Calls (Permission dependant)

Entire calls or segments of calls can be saved or emailed to internal or external parties. Clicking the button in the bottom-left of the playback window displays the email and save call options. Alternatively, a section of a call can be saved by highlighting and right-clicking. Selecting 'Save selection' from the menu will save only the section of the call that has been highlighted (See the image above).

Folders

Each user has their own folder structure that can be used to store important calls. Selecting the 'Add to folder' option from the bottom-left menu provides access to store the current recording for future reference. Folders can be accessed by clicking on the folder icon on the title bar.

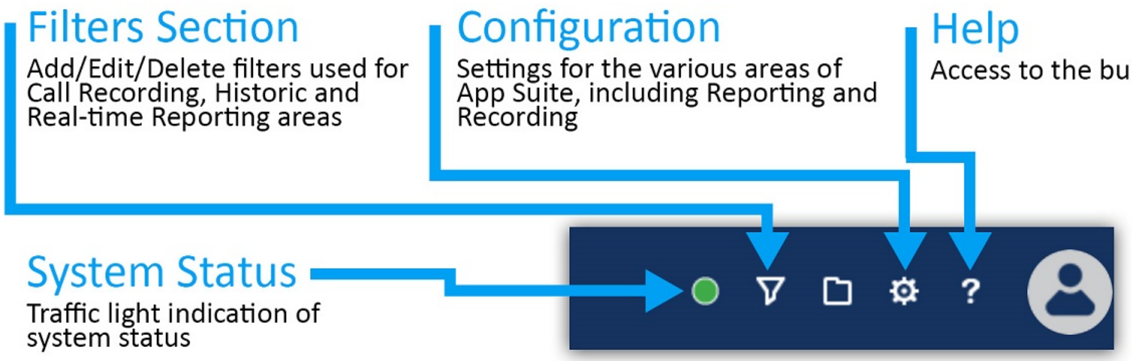
Events

The system stores events information about all calls on the system. Events stored include; hold/retrieve, pause/resume and account code entry. In addition, users can add their own custom events to mark specific time lines within a call which they can then refer to later. Events can be accessed through the bottom-left menu on the playback bar.

Audit Trail

The audit trail tab shows historical information about when calls are accessed and by whom. This includes when calls are played back via the user interface or when they are saved or emailed.

The title bar provides access to areas of the App Suite. The image below outlines each of the navigation icons:

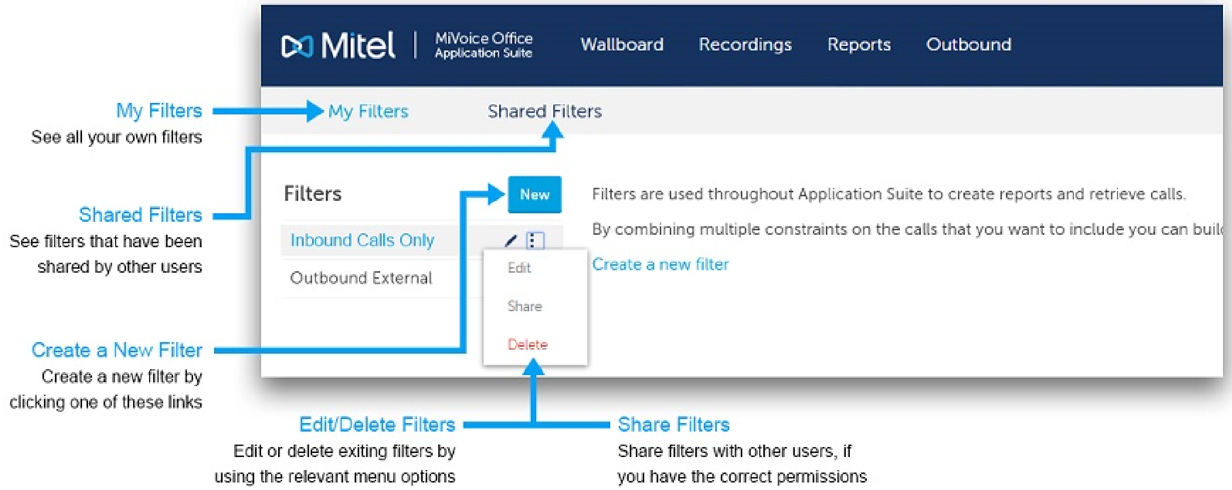


The configuration section and system status will only be visible with the correct permissions.

Filters

The 'Filters' section of the website is used to manage all the saved filters on the system. Filters can be used with reports or recordings.

Each user has their own 'My Filters' section that provides a list of all filters they have created.

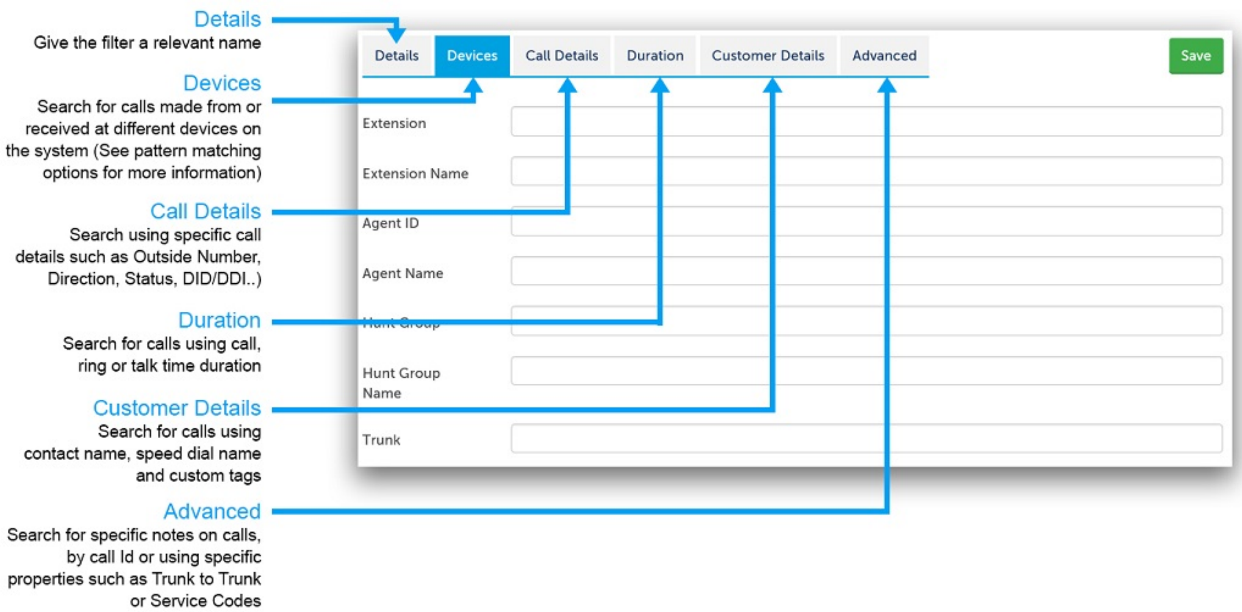


Shared Filters (Permission dependant)

Filters can be shared between users to avoid duplicating work and to allow administrative staff to set up filters that can be used by everyone.

Adding / Editing Filters

Each filter provides the ability to search on one or more details about a call. The details are grouped into tabs. The tabs are displayed with descriptions in the image below:



The use of special characters within the text boxes for a Filter enables the use of complex filter strings.

All Fields

The following characters are supported:

Special Characters	Description

Exclamation mark (!)	Not equal to
Percent (%)	Fuzzy matching (equivalent to a SQL LIKE %)
Underscore (_)	Fuzzy matching of a single character
Comma (,)	Can be used to search for multiple values at the same time

Device Fields

In addition to the special characters above, the following characters are supported when searching using a device based field (Extension, Agent, Trunk, Hunt Group):

Special Characters	Description
Plus sign (+)	Greater than or equal (e.g. 1000+ for extensions greater than or equal to 1000)
Hyphen (-)	Delimits a range of values to match (e.g. 1000-2000 for all extensions between 1000 and 2000 inclusive) or less than or equal to (e.g. -1000 for extensions less than or equal to 1000)

The example below shows what would be matched when entering combining multiple special characters using a comma:

- 1000-1005,!1003,1040,18%5,2000+

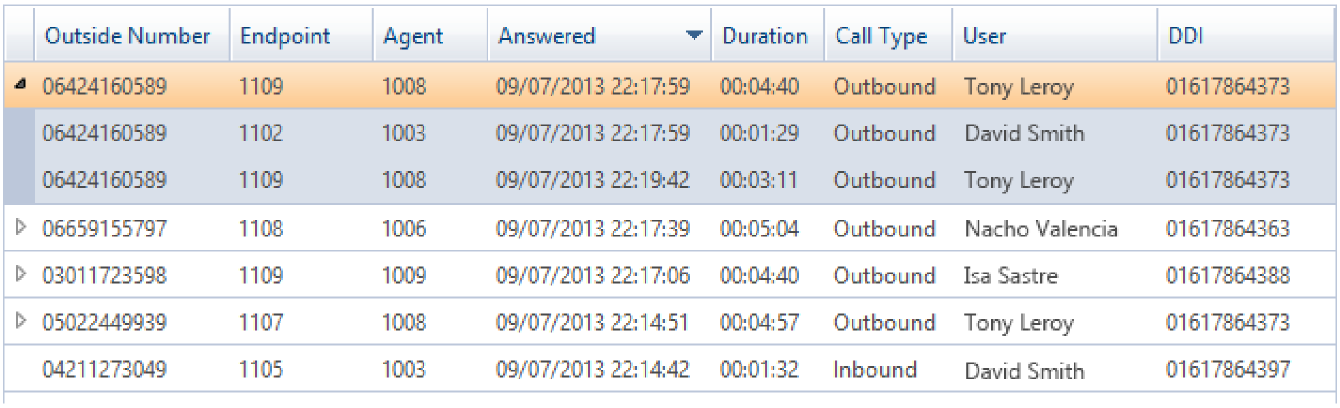
Matching endpoints: 1000, 1001, 1002, 1004, 1005, 1040, any that start with 18 and end with a 5, any with a value greater or equal to 2000.

> Device numbers are stored as text so when using greater than or less than, it is compared on an alphabetic level not a numeric level

4.2 Recordings Grid

Overview

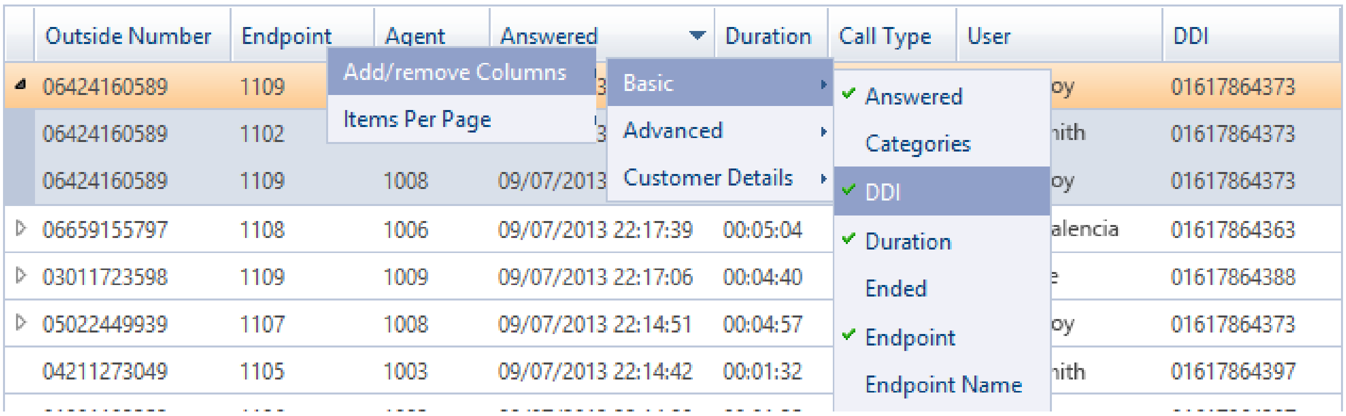
The recordings grid shows all the calls that match the current user's Date Range, Business Unit Filters, Filter Details, Additional Filters combined with the current user's Access Filters.



Outside Number	Endpoint	Agent	Answered	Duration	Call Type	User	DDI
06424160589	1109	1008	09/07/2013 22:17:59	00:04:40	Outbound	Tony Leroy	01617864373
06424160589	1102	1003	09/07/2013 22:17:59	00:01:29	Outbound	David Smith	01617864373
06424160589	1109	1008	09/07/2013 22:19:42	00:03:11	Outbound	Tony Leroy	01617864373
06659155797	1108	1006	09/07/2013 22:17:39	00:05:04	Outbound	Nacho Valencia	01617864363
03011723598	1109	1009	09/07/2013 22:17:06	00:04:40	Outbound	Isa Sastre	01617864388
05022449939	1107	1008	09/07/2013 22:14:51	00:04:57	Outbound	Tony Leroy	01617864373
04211273049	1105	1003	09/07/2013 22:14:42	00:01:32	Inbound	David Smith	01617864397

Each row on the grid shows either a single call or an aggregate call if a call has been segmented. See the Call Segmentation section for more details.

The columns displayed on the grid can be added or removed to show different information based upon Users preferences. To change the columns displayed right click on the grid and select *Add/Remove Columns* from the menu. If there is a ✔next to the column name, then it is already displayed.



The list of available columns is divided into *Basic, Advanced* and *Customer Details* options.

Basic Options

Field	Description
Answered	The date and time the call was answered.
Call Type	Internal or External.
Categories	The list of call categories that have been assigned.
DDI	The direct dial number.
Duration	The duration of the call.

Ended	The date and time the call ended.
Extension	The extension number.
Extension Name	The extension name.
Outside Number	The dialled number or caller id.
Ring Time	The amount of time the call was ringing.
Started	The date and time the call started
Talk Time	The amount of time the call was connected.
Trunk	The trunk number the call was on.
User	The user associated with the call

Advanced Options

Field	Description
Account Code	The telephone system account code.
Agent	The agent id.
Agent Name	The agent name.
Call ID	The PBX generated call ID.
DNIS	The DNIS value.
Global Call ID	The unique call id for this segment.
Hunt Group	The name of the hunt group.
Hunt Group Name	The hunt group number.
Logical Call ID	The unique call id for this entire call.
Notes	The number of notes attached to the recording.
Rating	The star rating for this record.
Scored	Shows if the record been scored.
Serial	The recording serial number.
Site	The site the record is associated with.
Speed Dial	The speed dial information associated against the outside number of this call.

Customer Options

Field	Description
Field 1	This is custom tag field 1.
Field 2	This is custom tag field 2.
Field 3	This is custom tag field 3.

Field 4	This is custom tag field 4.
Field 5	This is custom tag field 5.

Ordering Sorting

The ordering of the grid can be changed by clicking on any of the column headings, by default the results are order by *Answered* time in descending order, i.e. the most recent calls first. You can see how the grid is currently ordered by the arrow to the right of a column header.

Real-Time & Silent Monitoring

By default, the recordings grid shows calls that have completed and that have been recorded. If a user has permission, the grid can also show calls that are currently in progress. If they are being recorded by the system, then they can be silently monitored through the browser. To initiate a silent monitor, press the silent monitor icon which will be in the same location the play icon normally is in the recordings grid.

> This is different to silent monitoring on the PBX. No PBX configuration is required.

To configure the recordings grid to show calls in progress, refer to the website configuration section.

For information about giving users permission to silent monitor call, refer to the security profiles section.

Unrecorded Calls

By default, the recordings grid only shows calls that have been recorded. If a call was not recorded for any reason, then it will not display on the grid. Under the website configuration section the grid can be configured to show calls that were not recorded if required.

Some example reasons why a call was not recorded:

- It matched an exclusion list rule.
- It was made on an unrecorded device.
- There were no resources at the time (conference resources for Record-A-Call)

4.3 Business Unit Filters

Overview

Business Units are used throughout the system to automatically group calls together based upon the area of the business that they are applied to. A User is associated with a specific agent or range of endpoints and any calls involved on those devices are tagged against the User. The User is then assigned to a Business Unit and any calls for the User become part of the Business Unit.

See the Users and Business Units section for more details configuring Business Units.

The filter window shows all the Business Units that the current User has permissions to access. If they do not have permission to view a Business Unit then this and any child units will not be displayed.

See the Access Filters section for more details on configuring access permissions.

To filter the recording grid, select an individual User or Business Unit, multiple items can be selected by holding the Ctrl or Shift key and clicking on each item. When they are selected the item will turn orange. After all the required items have been selected, then click on the icon in the filter window. The recordings grid will then update to show any calls that meet this filter criteria. To clear the filter, click on the icon in the filter window.

> When a filter is applied, then word *filtered* will appear in orange at the top.

To help in finding specific Users the filter window provides a *search...* option at the top. Typing a name will then provide a list of any matches and then clicking on the User will select this within the window.

4.4 Date Range

Overview

The date range option is available for use on the recordings and reporting pages of the website. It is used to restrict the call data returned and based upon the Start Time of calls.

On the recordings page, the default date range will be automatically set to show calls that have started within the last 15 minutes.

On the reporting page, the default date range is set to Today.

The drop down provides options for:

- Today
- Yesterday
- This Week
- Last Week
- This Month
- Last Month
- Last 15 minutes
- Last 30 minutes
- Last 60 minutes
- Custom

When *Custom* is selected, the start and end date ranges can be entered into the fields shown. Once the dates have been entered then click on the *Apply* button to update the recordings grid or report.

> Example: If Last 30 minutes was selected at 13:42, the calls returned would be those started between 13:12 and 13:42.

> Selecting large date ranges can take a long time to return and can adversely effect server performance.

4.5 Additional Filters

Overview

When ad hoc searching is used to try and find a specific call the Additional Filters option can be used to do this. This enables specific meta data of the call to be used to filter the recording grid just by entering this into the appropriate field without having to create a Saved Filter.

The list of meta data fields that are shown can be changed by using the icon. For a complete list of the fields available see the Recordings Grid section.

To filter the recording grid enter a value into the appropriate field then click on the icon in the filter window. The recordings grid will then update to show any calls that meet the filtered criteria. To clear the filter click on the icon in the filter window.

4.6 Exporting Recordings

Overview

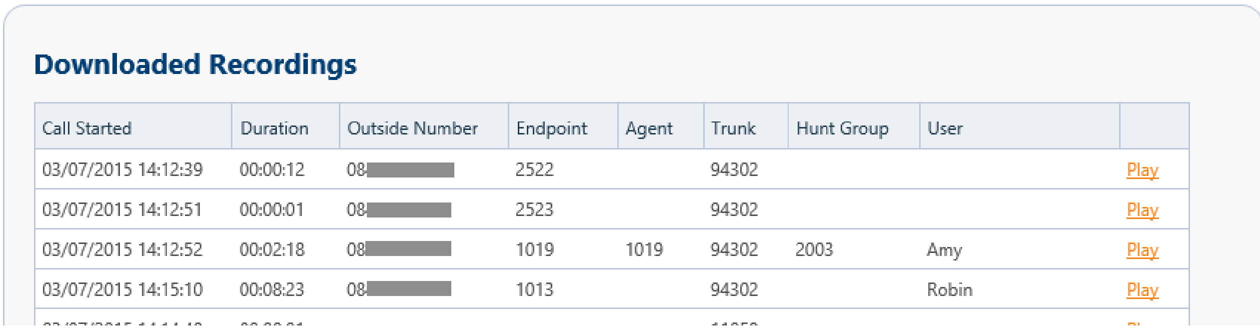
From the Recordings Grid calls can be exported and be either emailed out individually or when saved can be emailed in bulk. The user needs to have the *Email* or *Save* option enabled on their Security Profiles to perform these actions. When the recordings are exported any meta data that has been assigned to these calls is also provided.

Saving Recordings

To save a recording, from the Recordings Grid click on the icon next to the relevant recording. This will then download the relevant recording WAV files into a compressed ZIP file.

To bulk download a selection of recordings, from the Recordings Grid multi select a range of recordings using the Control and Shift keys. Then right click on the grid and select "Download selected". Alternatively, right click the "Download all" option to include all calls shown in the grid. A progress meter will be shown in the bottom right hand corner of the page whilst the download is being prepared and once complete will provide a "Download ready" link to save the compressed ZIP file with the recordings.

The ZIP file will contain all of the recording WAV files and a *Recordings.htm* index page that can be opened in a web browser to show the contents of the ZIP file. This will include a link to the WAV file with the following $$meta data$:



Downloaded Recordings

Call Started	Duration	Outside Number	Endpoint	Agent	Trunk	Hunt Group	User	
03/07/2015 14:12:39	00:00:12	08[redacted]	2522		94302			Play
03/07/2015 14:12:51	00:00:01	08[redacted]	2523		94302			Play
03/07/2015 14:12:52	00:02:18	08[redacted]	1019	1019	94302	2003	Amy	Play
03/07/2015 14:15:10	00:08:23	08[redacted]	1013		94302		Robin	Play

Email Recordings

To email a recording directly from the Recordings Grid click on the icon next to the relevant recording. This will open a new form where the *To:* address field and the *Subject:* and *Body* can be entered. Multiple email addresses can be entered by separating each one with a comma. Once these fields have been completed click on the *Send* button to send the email.

> The email server details configured in the Email & SMTP section are used when sending emails.

How the recording is sent out can be set to be one of three options:

- **Attachment**: The WAV files are sent out as an un encrypted attachment to the email. The attachment will be either a WAV file or in a compressed ZIP file if there are multiple WAV files.
- **Permanent link**: A direct playback link is sent that when clicked will download the file.
- **Single use link**: A direct playback link is sent that when clicked will download the file. This link can only be used once, if the link is used more than once then a message will be displayed informing the user this link has expired.

> Using the direct links to download the files requires that the **Website URL** configured in the Website section can be accessed by the user receiving the email.

The email body will contain the text that you entered in the send email form and also include the following $$meta data$$.

Call Answered	Duration	Outside Number
Extension	Hunt group	

5 Reporting

The reporting section of the MCS solution provides access to run and manage call and configuration based reports. For information on using the reporting features of the solution, please refer to the following sections:

- Report Templates
- Report Grouping
- Report Creation
- Running Reports
- Exporting Reports
- Shared Reports
- Report Scheduling

For information on licensing and permissions, please refer to the Reporting Overview section.

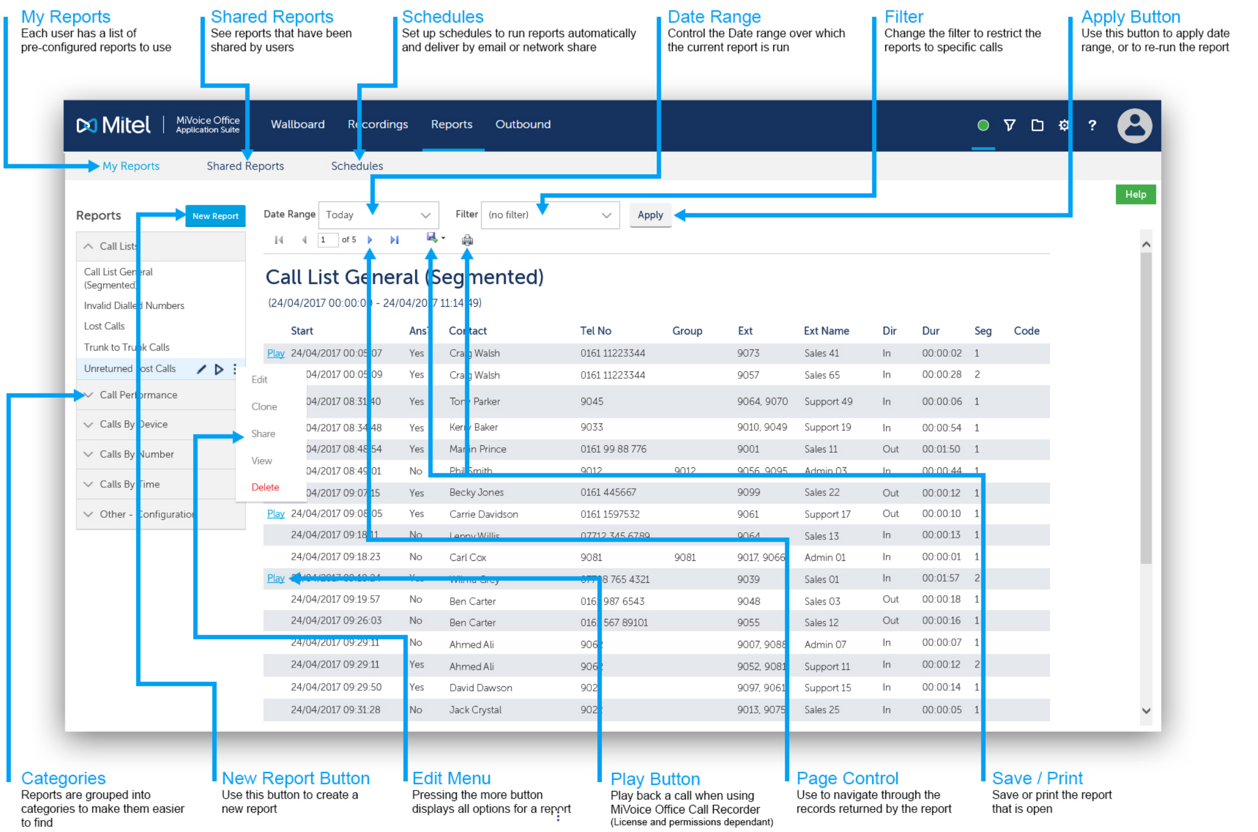
5.1 Call Reporter Quick Reference Guide

The following guide is designed to provide an introduction to the call reporting features of the MiVoice Office Application Suite solution.

Reports

The Reports page provides access to run reports on any internal or external calls. Depending on the license applied to the system, the following report types can be accessed:

- Call Lists
- Status Lists (DND & ACD)
- Grouped Reports (by Extension, User, Agent, Hunt Group, Trunk, DDI & Start Time)
- Configuration Lists (Extensions, Agents, Trunks & DDIs)



Any report or column that is not licensed for use will be indicated with a padlock symbol.

Running Reports

Each user has their own copy of the default reports to run. These can be modified, added to, or deleted without affecting other users on the system. The reports are grouped together in categories on the left side of the screen. To run a report, press the play icon to the right of the report in the list. The report will appear on the right side of the page using the default filter and date range that were saved against the report.

A report may be presented across multiple pages, when this happens the page navigation buttons can be used to move through the report. If the report is a grouped report, the last row will show the totals of each column where applicable. Reports can be saved in Excel, PDF or Word format or they can be printed directly from the page.

Segmented Reports

When a call is logged to the database, a new call segment is created each time the call rings or is answered by a different device on the telephone system. A single external call can have many call segments. It is important to understand this when looking at call reports and evaluating call totals. For example, if looking at a Segmented Call List, a call will appear multiple times, once for each destination it was delivered to.

For more information on call segmentation and how it applies to different Reports/Templates, please refer to the product help document.

Report Types (Lists / Grouped)

There are two different types of reports that can be run; lists or grouped reports. Lists can provide details of individual calls or call segments. Grouped reports provide aggregate columns that include totals, averages and minimum/maximum values. These reports provide a way of analysing call traffic and how quickly calls are being answered.

Date Range & Filtering

The date range and filter can be used to select which calls are included in the reports. Any changes to a filter or date range require the report to be re-run using the 'Apply' button. The system will cache reports that have be run before, if the report has not been edited and the date range/filter has not changed, a cached version of the report will be loaded to improve performance.

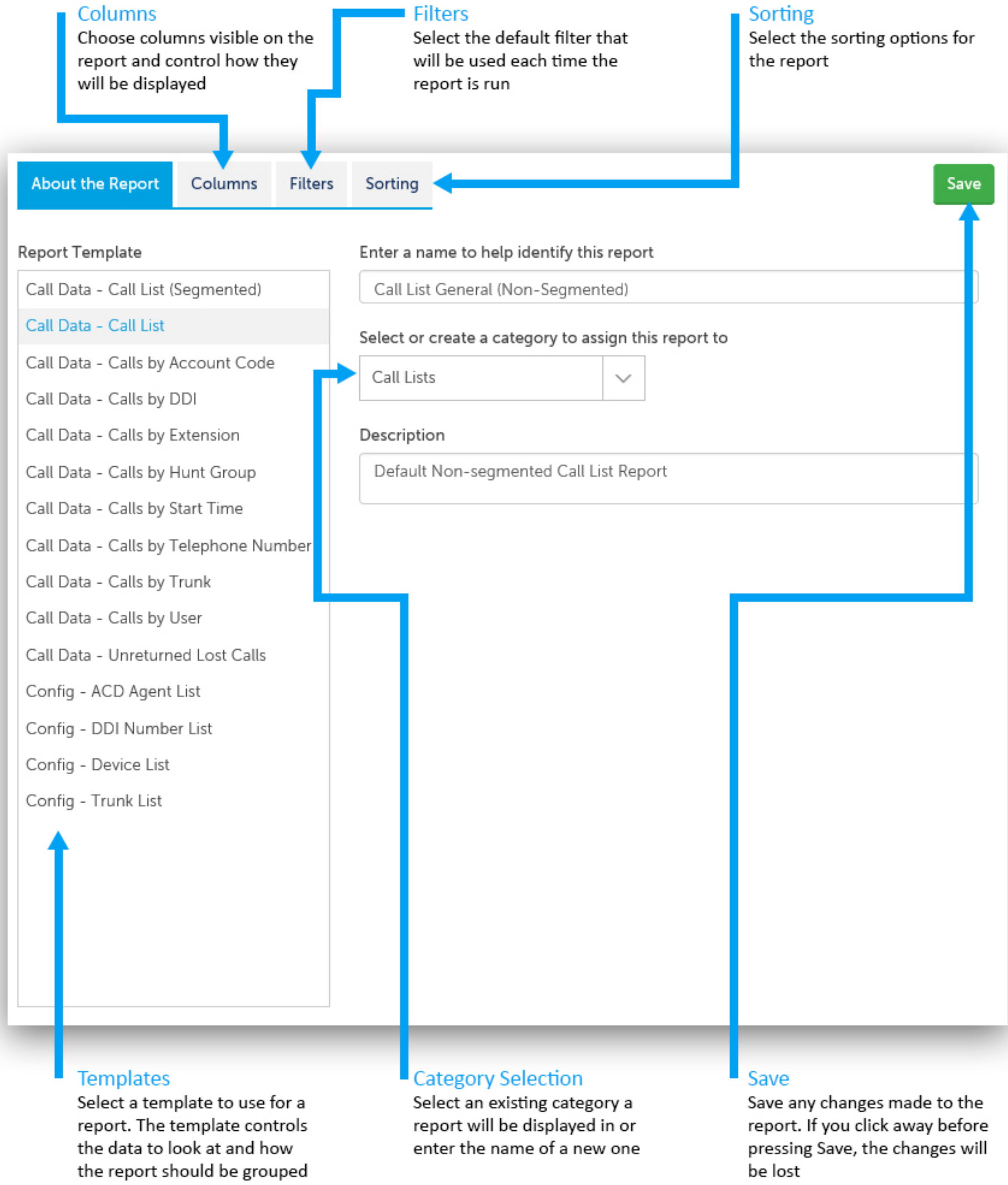
> The more data that is being included in the report, the longer the report will take to run and display on the right of the screen. It is beneficial to limit the data by using filters and date ranges so that it only includes the data required. A maximum of 5000 records will be displayed.

Shared Reports

Reports can be shared so that other users can see and modify them. When a report is shared, a shared copy of the report is created, leaving the original in the 'My Reports' section. Shared reports can be modified by any users with permission to access them.

> For a report to be used in a schedule, it must first be shared.

Every report in the 'My Reports' section is specific to the user logged in and can be added to, edited, or deleted as required without affecting other users. When editing a report, the form pictured below will be displayed.

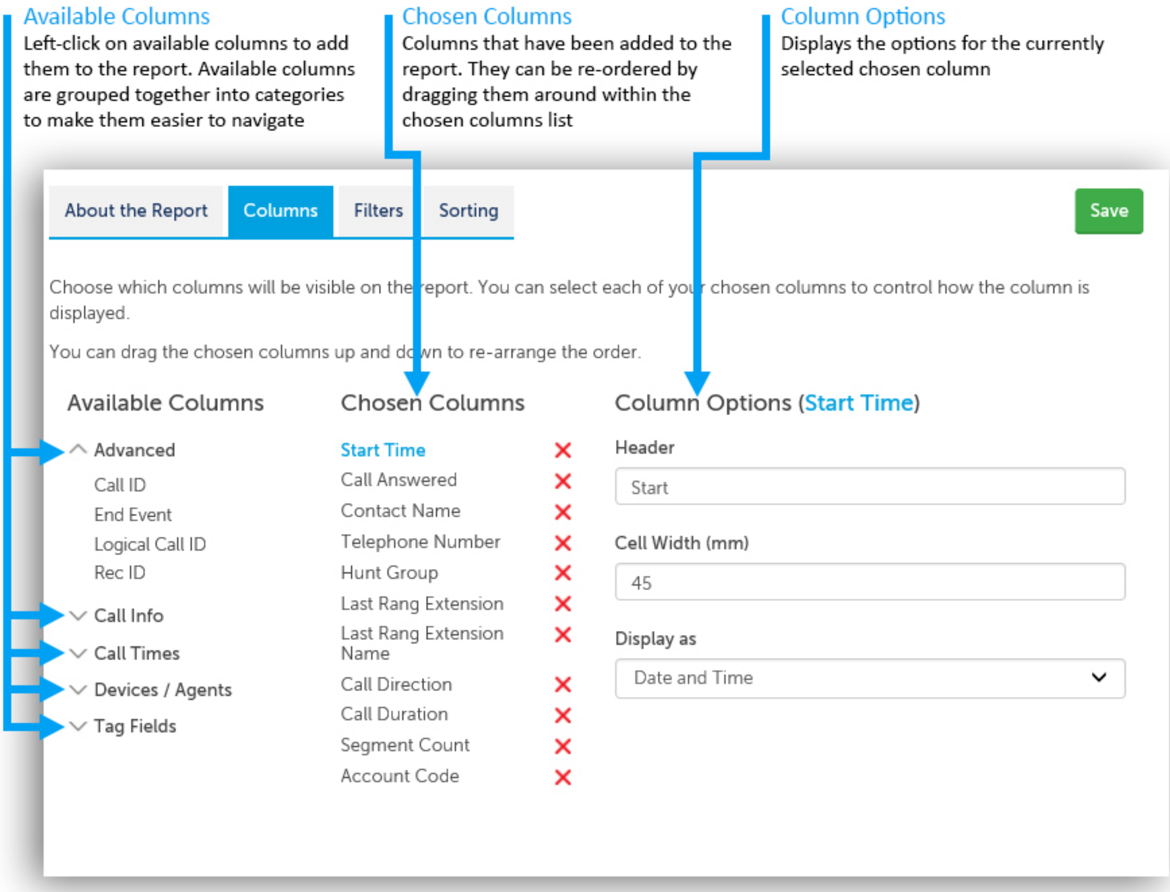


Report Templates

Each report is based on a report template. A report template defines what data is being reported on (call or configuration), how the data is to be grouped (By Extension, By Agent, Not Grouped etc..) and which columns are available to choose from. Changing the template of an existing report will change the available columns, this in turn will set the chosen columns back to default.

Report Categories

Reports are saved into different categories to make them easier to find in the user interface and to group together similar reports. The category a report is saved in can be selected from the list or a new category name can be entered.



Adding / Removing Columns

Each report comes with default columns added. A list of the available columns to add to the report appears on the left side of the 'Columns' tab, split up into categories to help locate the required column. To add a column to a report, left click on it. Chosen columns can be re-ordered by drag and drop or removed using the cross icon.

If the report is grouped, the column the report is grouped by will appear in blue. Grouped by columns cannot be removed from a report.

> Please refer to the product help file for detailed information of each column.

Column Options

The options available to configure will be different depending on the column type. The 'Header' is the name that will be displayed for this column in the report. These are defaulted to a shortened variant of the column name but can be overridden by the user (the column name appears as a tooltip if you hover over it in an open report).

Where applicable, the 'Display as' option controls the format of the data shown in the report.

> Changing the format of a grouped column can change the way the report is grouped. For example, if a report is grouped by 'Start Time' changing the format from 'Date and Time' to 'Time Only' will group multiple days calls into a single row based on time of day.

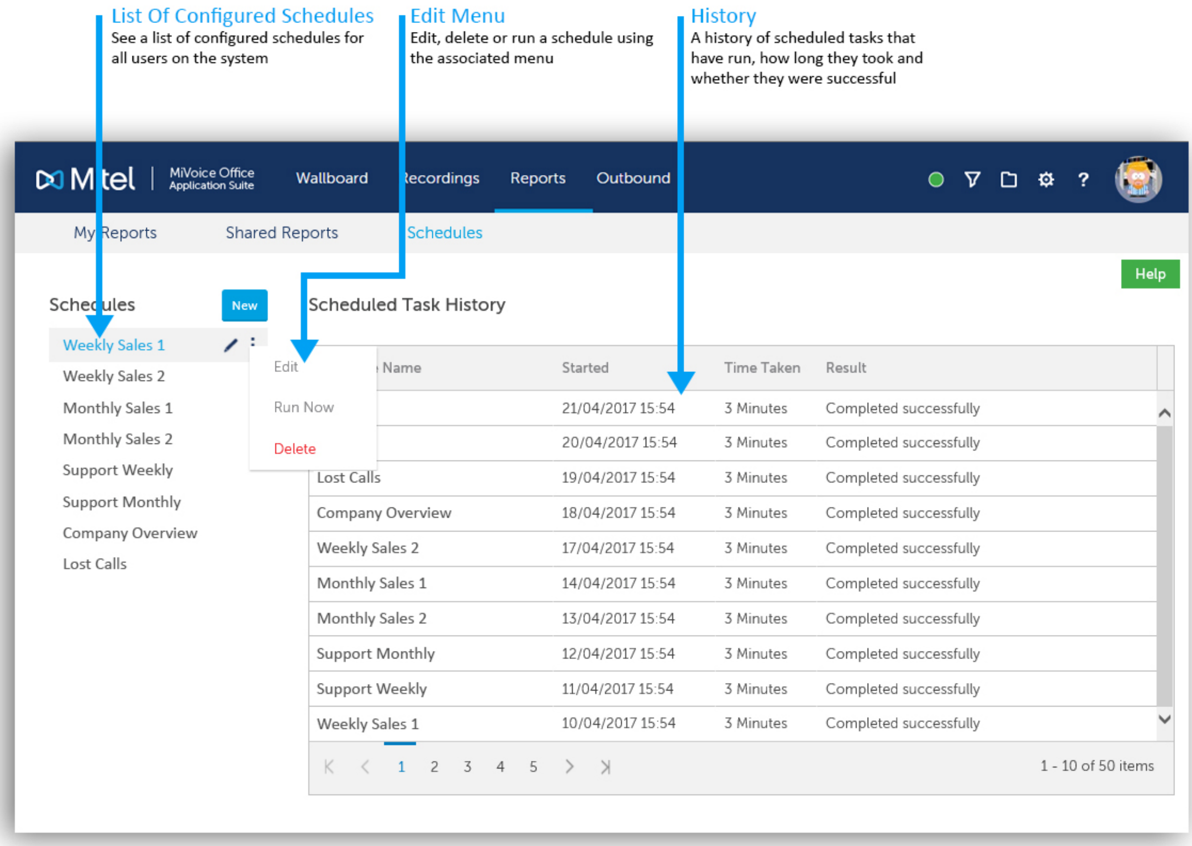
Filters

Select the default filter and date range to be assigned to a report when it is opened. This can then be overridden once the report is run using the date range and filter dropdown boxes on the report viewing page.

Sorting

Select the sort order for the report. Reports can be sorted by more than one column if required, but the sort direction (ascending or descending) will need to be the same for all sorted columns.

The optional scheduler can be used to automatically run reports on a regular basis and either deliver them by email or save them to a network share.

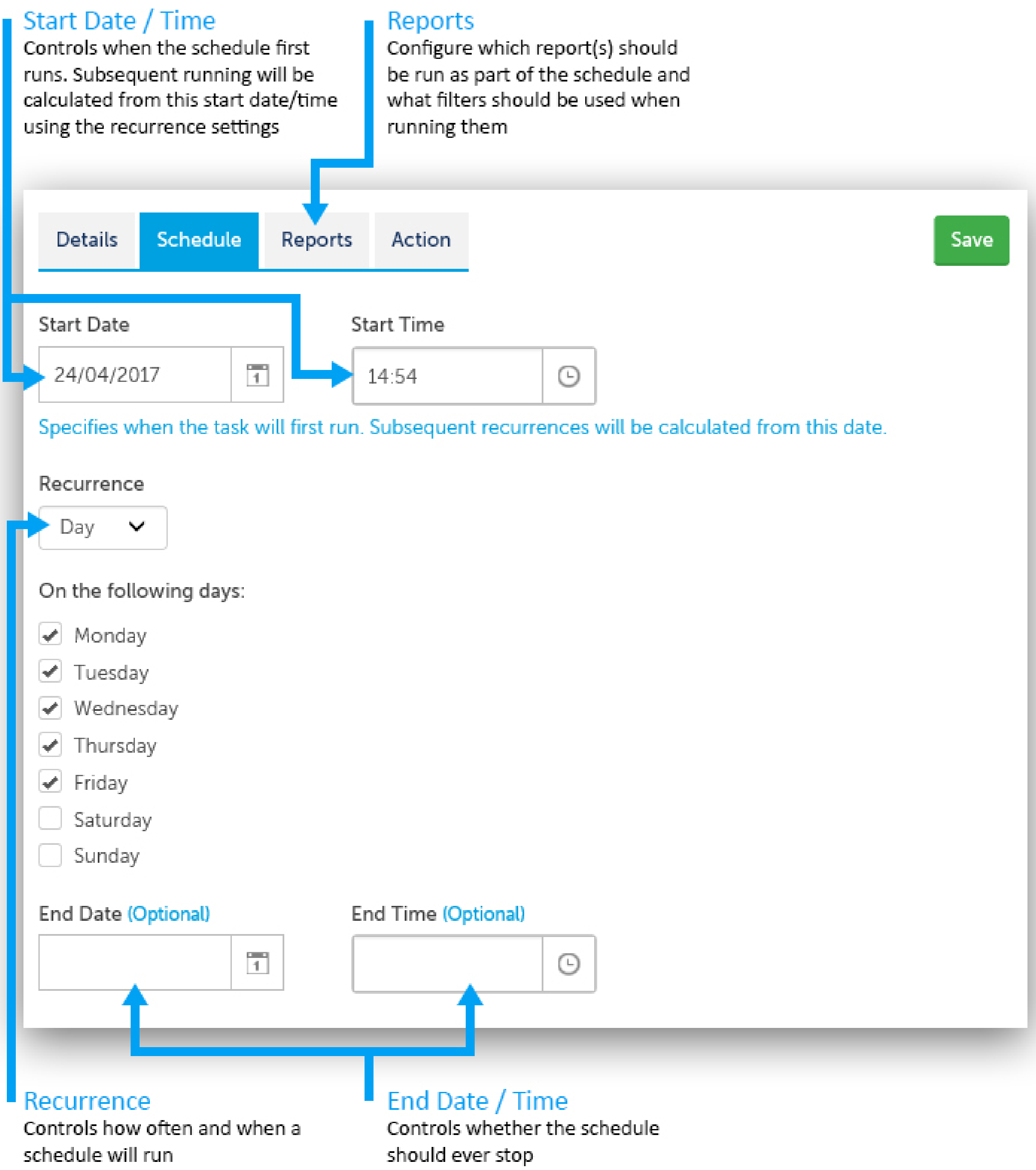


Using Schedules

The 'Schedules' page shows all schedules that have been configured on the system, regardless of the user that configured them. Any user with permission can add, edit or delete a schedule. The 'Scheduled Task History' table shows when the schedules have run and whether they were successful or not. Schedules can be run manually as a 'one-off' irrespective of the recurrence settings, by selecting the 'Run Now' option from the menu.

Shared Reports & Filters

Only shared reports and shared filters can be used in a schedule. This is because schedules are a system-wide concept that can be edited by anyone. Therefore the reports and filters being added to a schedule need to be visible to everyone.



Recurrence

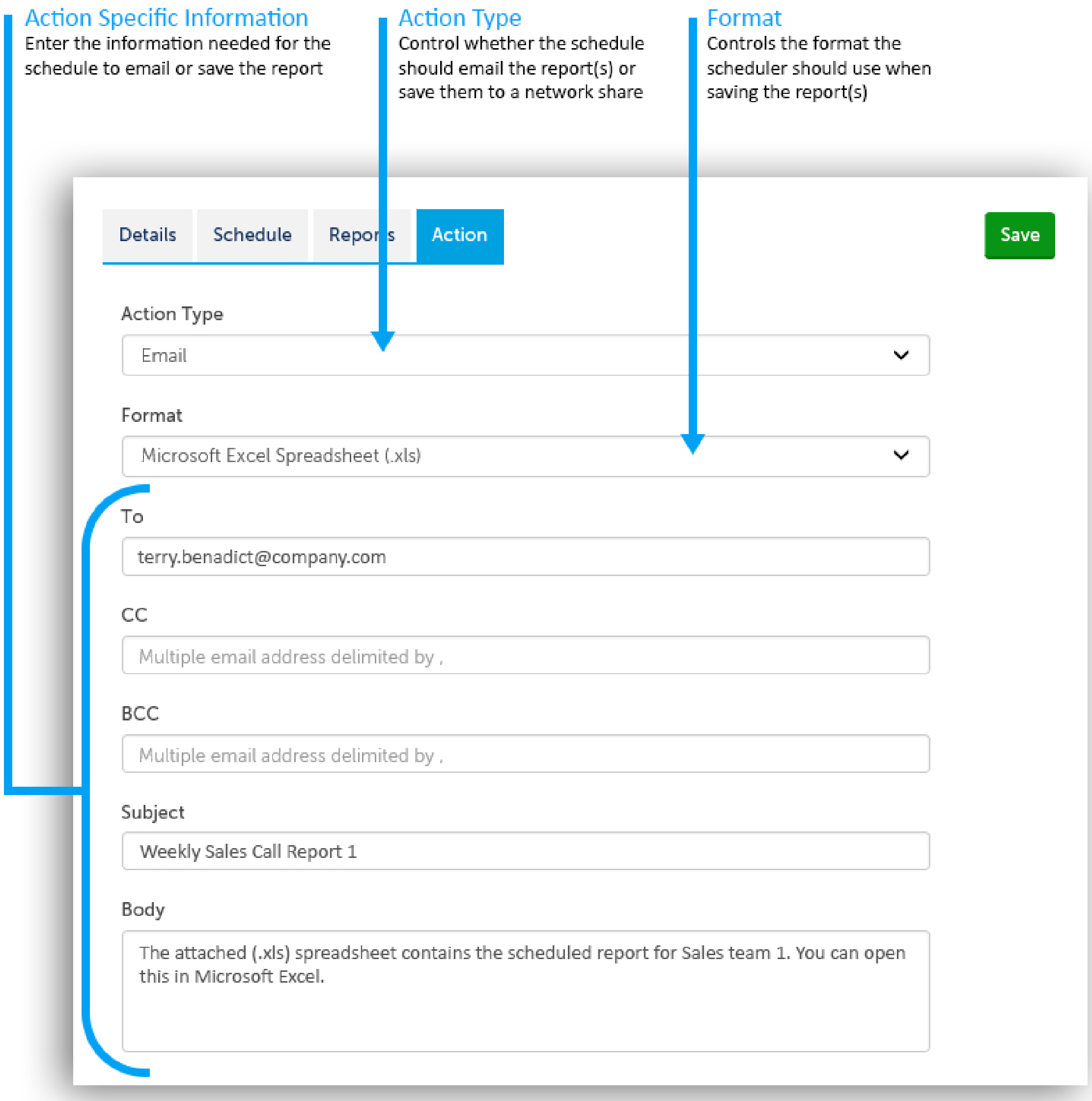
The 'Start Date' and 'Start Time' for a schedule is used to work out when a schedule will first be run. After this, the configured 'Recurrence' will be used to work out when the next schedule should be run. The table below shows the different options available for recurrence:

Recurrence	Description
Minute	Run every 'x' minutes (minimum 15 minutes). Select the days of the week to run and between what times.
Hour	Run every 'x' hours. Select the days of the week to run and between what times.
Day	Once a day at the time configured in 'Start Time'. Select the days of the week to run.
Week	Run event 'x' weeks at the time configured in 'Start Time'.
Month	Run every 'x' months at the time configured in 'Start Time'. Select the day of the month on which to run the schedule.

The 'End Date' and 'End Time' can be used if required to stop the schedule automatically.

Reports & Filters

Select the report(s) that will be run by the schedule and filter/date range to use for each one. When applying the date range it is advisable to use a contextual date range (this week, last week etc..). If a 'Custom' date range is selected, the date range will be fixed every time the report is run by the scheduler.



Action Type & Format

Reports can either be saved to a network share or emailed. In addition, the format of the report can be selected. Supported formats are Microsoft Word, Microsoft Excel and PDF.

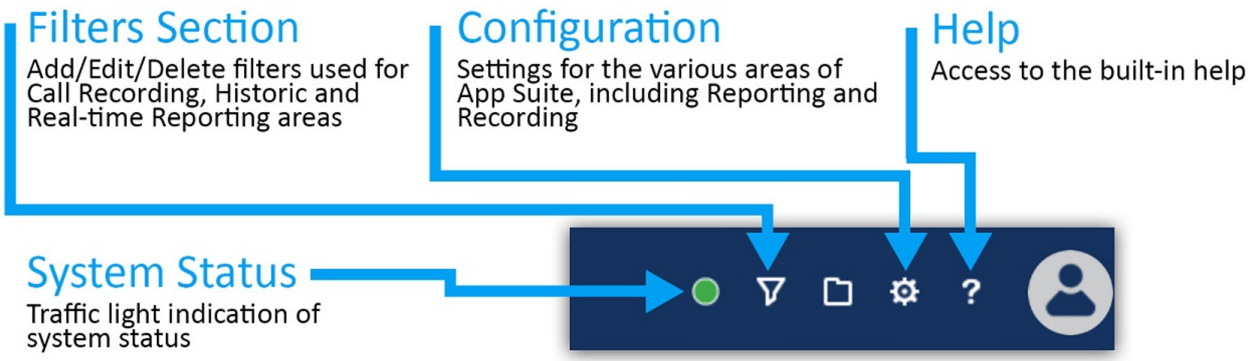
Emailing Reports

Reports can be emailed to one or more users of the system. Multiple email addresses can be added to any of the address fields (To, CC & BCC) using a comma separated list.

Saving Reports

To save the export to a network share, the details for the network share must first have been configured by the administrator of the system.

The title bar provides access to areas of the App Suite. The image below outlines each of the navigation icons:

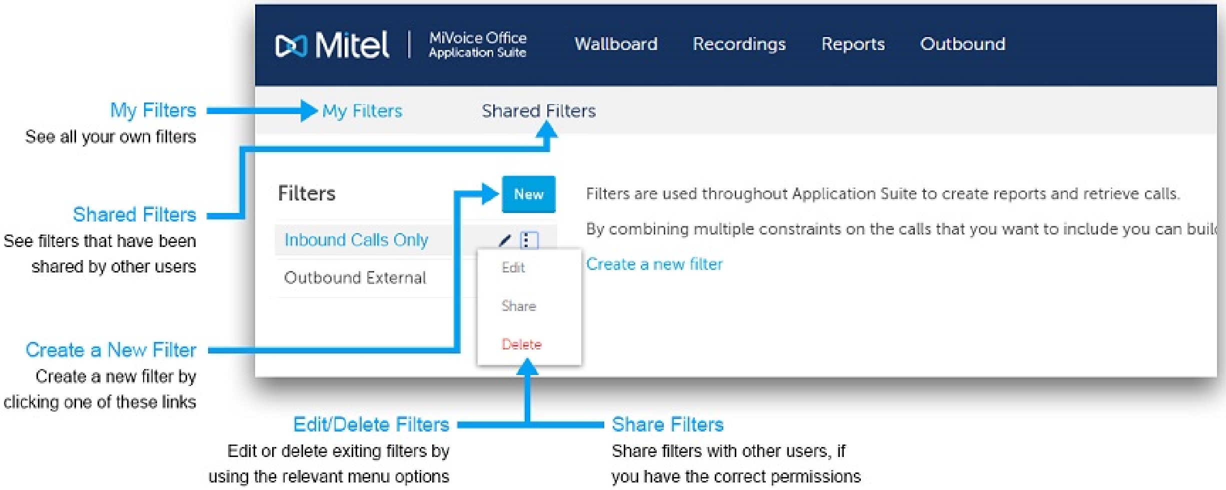


The configuration section and system status will only be visible with the correct permissions.

Filters

The 'Filters' section of the website is used to manage all the saved filters on the system. Filters can be used with reports or recordings.

Each user has their own 'My Filters' section that provides a list of all filters they have created.

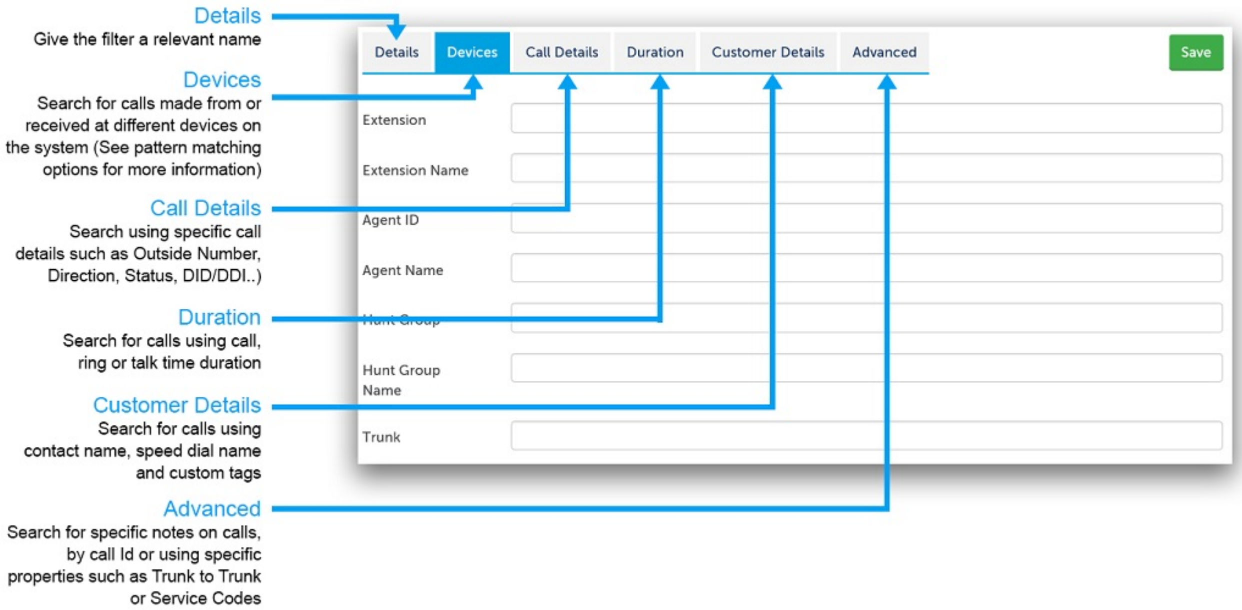


Shared Filters (Permission dependant)

Filters can be shared between users to avoid duplicating work and to allow administrative staff to set up filters that can be used by everyone.

Adding / Editing Filters

Each filter provides the ability to search on one or more details about a call. The details are grouped into tabs. The tabs are displayed with descriptions in the image below:



The use of special characters within the text boxes for a Filter enables the use of complex filter strings.

All Fields

The following characters are supported:

Special Characters	Description
Exclamation mark (!)	Not equal to
Percent (%)	Fuzzy matching (equivalent to a SQL LIKE %)
Underscore (_)	Fuzzy matching of a single character
Comma (,)	Can be used to search for multiple values at the same time

Device Fields

In addition to the special characters above, the following characters are supported when searching using a device based field (Extension, Agent, Trunk, Hunt Group):

Special Characters	Description
Plus sign (+)	Greater than or equal (e.g. 1000+ for extensions greater than or equal to 1000)
Hyphen (-)	Delimits a range of values to match (e.g. 1000-2000 for all extensions between 1000 and 2000 inclusive) or less than or equal to (e.g. -1000 for extensions less than or equal to 1000)

The example below shows what would be matched when entering combining multiple special characters using a comma:

- 1000-1005,!1003,1040,18%5,2000+

Matching endpoints: 1000, 1001, 1002, 1004, 1005, 1040, any that start with 18 and end with a 5, any with a value greater or equal to 2000.

> Device numbers are stored as text so when using greater than or less than, it is compared on an alphabetic level not a numeric level

5.2 Report Templates

Overview

The MCS has a series of report templates that can be used to create and run reports. Each report template contains the following information:

Data source (Call or configuration data for example)

This outlines when to get the data for the report from. Currently the two data sources available to the templates are

- Call Data
- Configuration Data

Columns

This outlines what columns are available to add to a report. Depending on the data source and grouping, the columns which are available to add to the report will change.

Grouping

This defines how the data in the report should be grouped (if at all). For example, a list of call records would usually have no grouping, each call and it associated properties can be viewed. If however the data is grouped by Telephone Number, aggregate columns become available such as Total Calls and Total Ring Time etc.

When creating a new report, a template must first be chosen before columns can be selected. Each template has a set of default columns which will automatically be visible, but can be added or removed by the user. When editing a report, if the template is changed, the selected columns will automatically be changed to the template's defaults.

> Refer to the Report Grouping section for more information on grouped and call list reports.

Available Templates

The following templates are available for creating reports:

Template Name	License	Description	Segmented Data
ACD Data - ACD Status List	Call Logging	A list of ACD state changes for all licensed agents. This template requires the ACD Reporter License.	N/A
Call Data - Call List	Call Logging	A list of call data records (not segmented*).	No
Call Data - Call List (Segmented)	Call Logging	A list of call data records which is segmented*.	Yes
Call Data - Calls by Account Code	Call Reporter	Call data grouped by Account Code, external calls only.	No
Call Data - Calls by Agent	ACD Reporting	Call data grouped by Agent, internal and external calls. This template requires the ACD Reporter License.	Yes

Call Data - Calls by DDI	Call Reporter	Call data grouped by DDI number, inbound external calls only.	No
Call Data - Calls by Extension	Call Reporter	Call data grouped by Extension, internal and external calls.	Yes
Call Data - Calls by Hunt Group	Call Reporter	Call data grouped by Hunt Group, inbound calls only.	Yes
Call Data - Calls by Start Time	Call Reporter	Call data grouped by Start Time, external calls only.	No
Call Data - Calls by Telephone Number	Call Reporter	Call data grouped by Telephone Number, internal and external calls.	Yes
Call Data - Calls by Trunk	Call Reporter	Call data grouped by Trunk, external calls only.	No
Call Data - Unreturned Lost Calls	Call Logging	A list of call data records (not segmented*), filtered to show unreturned lost calls only. External calls only.	No
Call Data - Inbound Call Summary **	Call Logging	Inbound call summary for external calls.	No
Config - ACD Agent List ***	Call Logging	Configuration data, a list of all ACD Agents MCS has imported from the telephone system.	N/A
Config - DDI Number List	Call Logging	Configuration data, a list of all DDI Numbers configured on MCS.	N/A
Config - Device List	Call Logging	Configuration data, a list of all Extensions MCS has imported from the telephone system.	N/A
Config - Trunk List	Call Logging	Configuration data, a list of all Trunks MCS has imported from the telephone system.	N/A
DND Data - DND Status List	DND Reporting	A list of DND state changes. This template requires the DND Reporter license.	N/A

* Refer to the Call Segmentation section for more information.

** The Inbound Call Summary template is not user selectable, it is fixed to the Inbound Call Summary Report.

*** MCS does not support ACD member hunt groups, only ACD Agent hunt groups.

> If '#ERROR' appears in any column, this is an indication of missing data. this can happen if the reporting service is stopped or loses connection to the telephone system.

Call List Limits

Each of the call list report templates (Call List, Call List (Segmented) & Unreturned Lost Calls) has a fixed limit of 5,000 rows of call data. If the date range for a report is configured and the resulting data would generate more than 5,000 rows, only the first 5,000 rows will get returned. When this happens, a warning messages will appear on the screen alerting to this fact. To remove the warning, reduce the date range the report is being run for or apply a filter to restrict the result set. Alternatively schedule the report to return all records.

Recording Playback

The Call List reports provide a 'Play' option against answered calls which allows the user to playback the recording if they have the necessary MiVoice Office Call Recorder features configured. Clicking the play link will open up the normal playback window.

If a call has not been recorded due to it being made on an unrecorded device or because it has been excluded, the play link will still appear but the user will be informed that the call was not recorded after pressing it.

> The prefix to each template ('Call Data', 'Config') refers to the data source the template is using.

> Refer to the Reporting section for information on licensing.

5.3 Report Grouping

The solution provides two types of call data report; lists and grouped reports. Lists provide a list of individual calls or call segments, grouped reports provide aggregated call data.

Call Lists

Call lists are not classed as grouped reports (see Non-segmented Reports section below for more information). This means they show data directly from the database with the addition of some computed columns like call duration.

Call lists are really useful for finding a specific call and information about it.

Grouped Reports

The MCS provides reports which are grouped by the following call information:

- Account Code
- Agent
- DDI
- Extension
- Hunt Group
- Start Time
- Trunk
- User

Grouped reports are really useful for assessing performance and getting an overall view of the number and types of calls being processed. Grouped reports contain Totals, Averages, Minimum and Maximum values of the majority of call data columns.

For example, a report grouped by extension can be used to see how many calls each extension handled and what their total talk time was.

> Refer to the Templates section to see more information on the grouped reports provided.

Non-Segmented Reports

Reports that calculate of full calls not segments of calls are effectively grouping by trunk line first before any other grouping (if there is any) is applied to the report.

When this grouping by trunk line occurs, the segmented calls data needs to be aggregated. The following section outlines the effect this aggregation has on a call's available columns.

Column Name	Aggregation Effect
Account Code	The last account code entered, on any segment.
Agent / Agent Name	If the call was answered, this will contain the details of the agent logged in if there was one. Other wise it will contain the agent details of the extension where the call first rang. If no agent was logged at all, these fields will be blank.
Answer Time	The time the call was first answered.
Call Answered	If any segment of the call was answered.

Call Duration	The cumulative call time of all segments.
Call Type	The call type of the first segment.
CallID	The call id of the first segment.
End Event	The end event of the last segment.
End Time	The end time of the last segment.
Extension / Extension Name	If the call was answered, this will contain the details of extension that answered the call. Otherwise it will contain the extension where the call first rang.
Hold Duration	The cumulative hold duration for all segments.
Hunt Group / Hunt Group Name	The details of the first hunt group the call passed through if applicable.
Rec ID	The Record ID of the first segment.
Ring Duration	The ring time of the call until it first got answered.
Start Time	The start time of the initial segment.
Tag Fields 1 to 5	The last valid entry in each field. For example, if field 1 was tagged on segment 1 and field 2 was tagged on segment 3 then both tag fields 1 and 2 would show on the report unless overridden with a valid tag in subsequent segments.
Talk Duration	The cumulative talk duration for all segments.
Transferred Agent From	Contains the agent details the first time the calls was transferred if applicable.
Transferred Agent To	Contains the agent details the first time the calls was transferred if applicable.
Transferred From	Contains the extension details the first time the calls was transferred if applicable.
Transferred To	Contains the extension details the first time the calls was transferred if applicable.
Username	If the call was answered, this will contain the details of the username that answered the call. Otherwise it will contain the username where the call first rang.

If a Call List column is not listed here then the aggregation will have no effect on it.

5.4 Report Creation

The following section describes the properties that can be configured against a report. The properties discussed here are displayed when creating a new report or editing an existing report.

To create a new report, press the 'New Report' button above the reports accordion\list on the reporting page. To edit a report, hover over a report and press the edit icon ( ) or press the more icon (⋮) and select Edit form the menu.

About the Report

Each report that is configured on the system requires a template to be selected. This template tells the report about the type of data that is being returned, the available columns for the report and whether the data is grouped or not. Once a template has been selected, the name and category properties must be configured before navigating to the columns section:

- **Name** - User definable name that will be used to identify the report for running or adding to schedules.
- **Category** - Defines where the report will appear on the website. Categories are used to group similar reports together to aid user access to them. Either select an existing category or type in the name of a new one.
- **Description** - User definable description, this can be used to store more detailed information about the report and what it is for.

> Changing the template of an existing report will cause the selected columns to change to the default ones for the selected report.

> To cancel the changes being made to a report simply navigate away from the current page without pressing the 'Save' button.

> Refer to the Report Templates section for information about each of the different templates available.

Columns

The column selection screen is split into three sections:

Available Columns

This section outlines each or the available columns for a specific report template. To add a column to the report, simply click on the column. Each of the columns available is displayed in a different category to group similar columns together and aid user navigation. Clicking on a category name will display the columns in that category. For a brief outline of what the data in the column represents, hover over the column with the mouse to get a tooltip.

Any columns that have already been added to the report will show greyed out and in italics.

> A maximum of 50 columns can be added to a report.

Chosen Columns

This section shows all the columns that will currently be displayed on a report. Columns will be displayed in the order in which they are visible in this list. To change the order of the chosen columns, simply left click on the a column and drag it to a new location in the list.

If the data returned by the report template is grouped in any way, the columns the report will be grouped on will be displayed in blue in the chosen columns list. These columns can be re-ordered but cannot be removed from the report. To remove other columns from the report simply press the red cross next to the column name.

To change the column on which the report is grouped, a different template must be selected.

Column Options

Each column has settings that can be configured including Header, Cell Width and in some cases Display As (display format).

The header setting is the name that will be displayed as the column header when the report is run. All columns have a default header name configured which is generally much shorter than the column's full name so that it will fit better within the report header.

The cell width option outlines the width the column should have within the report. All columns have been given a default width that suits the data type however these may need to be changed, especially if trying to fit a large number of columns onto a single report for exporting.

If a column contains a date or duration of some kind then the display format option will appear. The following date formats are available:

Call Time (Start Time, Answer Time, End Time etc..)

- Date and Time -> dd/MM/yyyy HH:mm:ss
- Date Only -> dd/MM/yyyy
- Time Only -> HH:mm:ss
- Week -> dd/MM/yyyy (Mon) (The date rounded to the previous Monday)
- Month -> MMM, yyyy

Duration (Call Time, Talk Time, Hold Time etc..)

- Hours, Minutes and Seconds -> HH:mm:ss
- Total Seconds

> Refer to the Report Grouping section for more information on these display formats and how they affect grouped reports.

> Refer to the Statistics section for more information on the columns available for each template.

Filters

The filters page provides a way to configure the initial filter and date range that will be used when the report is first run. These properties can be changed after the report is run using the ad-hoc date range and filter drop downs on the report viewer.

In addition, the time range on a day by day basis can be configured so that data outside this range is ignored.This is very useful for ignoring calls outside of working hours. For example, if a report is configured to run a display data over a week, the time range could be limited to between 9am and 5pm so any calls outside of these hours on any day of the week included in the report would not be shown.

Sorting

The sorting page provides a way to control which column(s) within the report are used to sort by when displaying the data. By default a sort column and direction will be defined in the template but this can be changed as required.

Reports can be sorted by more than one column by adding another column from the available columns list.

Saving a Report

Once all the properties have been configured, press the 'Save' button to implement the changes. If a new category has been entered for the report it will be created at this time.

If the report saves successfully it will be run immediately and display on screen. If there are any problems when saving the report, a message box will appear in red outlining the problem and suggesting changes that need to be made.

5.5 Using Reporting

The following section outlines the reporting user interface and how reports can be run, filtered and exported.

Default Reports & Report Categories

Each user with permission to run reports is automatically configured with a default set of reports. These reports are individual to the logged in user and can be edited/deleted as required.

These default reports are displayed in different categories to help navigate between different types of reports:

Category	Report Name	License	Description
Call Lists	Call List General	Call Logging	A list of all calls on the system (segmented, internal and external calls).
	Invalid Dialled Numbers	Call Logging	A list of outbound external calls that failed to complete.
	Lost Calls	Call Logging	A list of calls that were not answered (external calls only)
	Trunk to Trunk Calls	Call Logging	A list of trunk to trunk calls (inbound calls that were diverted or transferred externally).
	Unreturned Lost Calls	Call Logging	A list of lost calls that have not been returned or subsequently answered.
Call Performance	Call Performance By Day	Call Reporter	Overview of lost calls on a day by day basis.
	Service Level By Half Hour	Call Reporter	In depth breakdown of answered calls by half hour (call rate period).
	Service Level By Half Hour & Day	Call Reporter	In depth breakdown of answered calls by half hour and day (call rate period).
Calls By Device	Calls By Account Code	Call Reporter	Breakdown of external calls by account codes entered.
	Calls By DDI	Call Reporter	Breakdown of inbound external calls by DDI number.
	Calls By Extension	Call Reporter	Breakdown of all calls by extension number.
	Calls By Hunt Group	Call Reporter	Breakdown of inbound calls by hunt group.
	Calls By Trunk	Call Reporter	Breakdown of external calls by trunk line.
	Calls By User	Call Reporter	Breakdown of all calls by user.
	Detailed DND Status List	DND Reporting	List of DND state changes.
	DND Status By Extension	DND Reporting	Breakdown of DND status by extension.

	Unmatched Calls By Extension	Call Reporter	Breakdown of unmatched calls by extension.
	Unmatched Calls By User	Call Reporter	Breakdown of unmatched calls by user.
Calls By Number	Calls By Telephone Number	Call Reporter	Breakdown of calls by the number dialled/received.
	Calls For Service Codes	Call Reporter	Breakdown of calls made to service code numbers (see dial plans for more information).
	Top Dialled Numbers	Call Reporter	Breakdown of calls made by telephone number.
	Top Received Numbers	Call Reporter	Breakdown of calls received by telephone number.
Calls By Time	Call Summary By Day	Call Reporter	Breakdown of external calls by day.
	Call Summary By Month	Call Reporter	Breakdown of external calls by month.
	Call Summary By Week	Call Reporter	Breakdown of external calls by week.
	Calls By Half Hour	Call Reporter	Breakdown of external calls by half hour.
	Calls By Half Hour & Day	Call Reporter	Breakdown of external calls by half hour and day.
Calls/Status By Agent	ACD Status By Agent	ACD Reporting	Breakdown of ACD status by agent.
	Calls By Agent	ACD Reporting	Breakdown of calls made/received by agents.
	Detailed ACD Status List	ACD Reporting	List of ACD state changes for every licensed agent on the system.
	DND Status By Agent	ACD Reporting	Breakdown of DND state changes by agent.
	Unmatched Calls By Agent	ACD Reporting	Breakdown of unmatched calls by agent.
Other - Configuration	ACD Agent List	Call Logging	A list of ACD Agents imported form the telephone system(s).
	Device List	Call Logging	A list of extensions imported form the telephone system(s).
	DDI Number List	Call Logging	A list of DDI numbers configured on the MCS.
	Trunk List	Call Logging	A list of trunks imported form the telephone system(s).

These default reports can be deleted as required. The categories can be used to add additional reports or deleted as required.

Reports that are not licensed will be identified with a padlock symbol. In addition, some columns within reports may require an additional license, these will also be identified with a padlock symbol.

Inbound Call Summary

The inbound call summary report is a read-only report that gives a system overview of inbound external calls. This is the first report that is run every time a user browses to the reporting section of the MCS website.

This summary screen can be viewed on any system with a Call Logging license. It shows un-segmented call data for external calls coming into the telephone system. This screen is designed to provide a quick overview of system performance, for more information use one of the Call Performance reports.

Running Reports

Any existing report can be run by hovering over the report name with the mouse and pressing the play icon ( ). Each report has a default filter and date range which will be used when first running a report.

Filtering & Date Ranges

Once a report is on screen the date range and filter options above the report can be used to change, expand or restrict the data the report is displaying. When changing the date range or filter that is applied to a report, the 'Apply' button needs to be pressed to refresh the report.

The date range drop down offers a range of predefined date ranges (Today, Yesterday, This Month, Last Month etc..) that can be used to quickly change the call data being used to produce the report. If a specific date or date range is required then the 'Custom' option can be used to select the dates required. Refer to the Date Ranges section for more information.

The larger the date range the report is being run over, the longer the report will take to run. If a report is taking a long time to run, try reducing the date range. In addition, the UI is limited to displaying a maximum of 5000 rows of data.

The filter drop down can be used to restrict the data to only contain records that are specifically required (Caller ID, Extension etc..). The filter drop down will display all of a user's own filters along with any shared or built-in filters on the system. Refer to the Filters section for more information on creating and using filters.

Paging & Totals

Due to the fact that the reports are in a webpage, it is not feasible that all the rows returned from a report are displayed all at once on the screen. Instead, rows are displayed in pages which can be navigated using the following control:

The icons either side of the page number information can be used to navigate through the pages of the report. Clicking the far right icon takes you straight to the final page of the report.

If the report is grouped, there will be a total row at the end of the reports which shows totals of all columns where it is appropriate.

Cloning Reports

Copies of a report can quickly be made using the 'Clone' feature. To make a clone of an existing report, press the more icon (⋮) next to the report and select 'Clone' from the menu. A form will appear prompting for a new name for the report and the name of the category to store the report in.

Cached Reports

Due to the time it can take to run reports (especially when large date ranges are involved), the system will cache reports so that they can be re-used in the future without having to request the data again from the database.

If a report has previously been run with the same filter and date range then the system will use a cached version to speed up the running of the report. This does not apply to reports using the Today, This Week or This Month date range options because the data may have changed since the report was last run. Using any of these date range options will cause the report to be re-run each time.

> Reports that include large amounts of data should be run out of working hours to reduce the risk of resource contention with other users or other features of the system. Use Report Scheduling to run reports at times when the system is not in use.

> Cached reports are deleted when the MCS Reporting Service starts-up.

> Refer to the Report Creation section for information on creating and editing reports.

> Refer to the Statistics section for information on the columns available in each report.

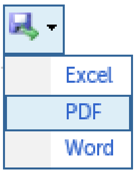
> Refer to the Exporting section for more information on exporting reports from the screen.

5.6 Exporting Reports

Any report viewed on the MCS website can be exported directly from screen. By default, all exported reports are in landscape format to maximise the page space available for columns.

Exporting

To export a report, run the report and then press the save button at the top of the report:



.

From the menu that displays, select one of the available export formats:

- Excel
- PDF
- Word

As soon as the export format has been chosen, the report will be exported in the required format and a standard browser download prompt will appear asking where to save the file to. The type of prompt received will differ from browser to browser.

> Applications that support Excel, Word and PDF formats are not required for exporting but will be required to open the exported files.

> If the number of rows in the report exceeds 1,000, the export option will not be available. To export more records than this you must use Scheduling.

5.7 Shared Reports

A shared report is visible to all users on the system that have access to reports. Shared reports can be run, edited and deleted by any user on the system. Shared reports are also the only type of report that can be added to a schedule.

Creating a Shared Report

Shared reports can be created directly from the Shared Reports section of the website or can be created by sharing an existing personal report.

To share an existing personal report, press the more icon (⋮) next to the report and select 'Share' from the menu. A form will appear prompting for the following information:

- **New Name** -> This will be the name given to the shared report.
- **Category** -> Choose a category for the shared report to reside in or enter the name of a new one.

Pressing the 'Copy Report' button will then accept this information and create the shared report. The shared report is effectively a copy of the existing report, the original will still be visible under 'My Reports' and any changes to the new report made by other users will not affect the original.

Shared reports have their own category structure which is system wide, any new category created in shared reports will be visible to all users.

Filters & Scheduling

Shared reports can be run directly on the website in the same way personal reports can. When running the shared reports in this way, personal or shared filters can be applied to the report.

Only shared reports can be added to a schedule to be run on a regular basis. When running a shared report through a schedule, only shared filters can be applied to it.

5.8 Scheduling

Scheduling provides a way to automatically run reports on regular basis. Access to the scheduling features of the solution is controlled by a single site-wide license. Once a system is licensed, any number of schedules and reports can be created.

A single schedule can be configured to run multiple reports using different filters and date ranges. when a schedule has run the reports configured, it can deliver them by email to one or more people or save the reports to a share on the network.

Permissions

Users can be given access to schedule reports through the security profile that has been assigned to their user account.

Once a user has been given access to schedules, they can create their own schedules as well as managing any other schedules created on the system.

Shared Filters & Reports

Only shared filters and reports can be added to a schedule. This is because schedules are a system wide entity and so to make sure that any user with permissions can access and edit schedules, they are restricted to using only filters and reports that are also accessible by all users.

If a filter or report that is currently being used in a schedule is deleted by a user, the user will first be alerted to the fact the filter/report is in use and will be given the opportunity to cancel the delete operation. If the filter or report is deleted, it will be removed from the schedule.

Schedule History

The schedule history is visible from the main schedule page on the website. It gives a list of schedules that have run with information on how long they took and whether they completed successfully or not. If the schedule fails, a guide to what caused the problem (Share access / email server connection failure etc..) should be visible.

Running Now

If required, a schedule can be executed immediately by selecting the more icon (⋮) and selecting 'Run Now' from the menu. Running a schedule in this manner will not change the automated schedule.

> Schedule history is kept for three months.

> Refer to the Schedule Creation section for information on configuring schedules.

5.8.1 Schedule Creation

To create a new schedule, navigate to the schedules section of the website (sub menu below Reporting) and press the 'New' button. The schedule management form will appear to guide the user through configuring the schedules. The same form can be accessed to edit an existing schedule by hovering over the schedule in question and pressing the edit icon ( ).

Details

The details section request a name and description for the schedule. The name will be used to identify the schedule and must be unique. The description is not required, but can be used to store information about what the schedule is for.

Schedule

Schedule section outlines when the schedule should be run:

Start

The time at which the report will first be run, subsequent recurrences will then be calculated from this initial time.

End Date & Time (Optional)

If the schedule does not need to be permanent then and end date for the schedule can be entered here.

Recurrence - Minute & Hour

Selecting a recurrence of minutes or hours provides an additional option to enter the interval number (15 minutes, 2 hours etc). If required, the recurrence can then be limited to run between certain hours of the day and on certain day\days of the week.

For example: Run every 15 minutes between 9am and 5pm Monday to Friday only, this allows a small interval between the schedule running but restricting reports out of working hours.

> The minimum recurrence value that can be entered is 15 minutes.

Recurrence - Day

Selecting a recurrence of day allows you to have a schedule that runs once a day at a certain time. As with the Minute & Hour options specific days of the week can be select so that reports don't run at weekends for example

Recurrence - Week

Selecting a weekly recurrence allows schedules to run once a week or less frequently.

Recurrence - Month

A monthly recurrence allows schedules to be run once a month or less frequently. In addition to selecting the number of months between running, the frequency options allows a specific day number (e.g. 1st) of the month to be selected or a contextual day like the first Monday of the month for example.

> If a contextual day of the month is selected for the frequency, this will occur in partial weeks. So if the first Friday of the month is selected and the 1st of the month is a Friday, the schedule will run on this day.

Reports

The reports section allows one or more reports to be added to the schedule. To add a report, press the 'Add' button and populate the form that appears.

Select a report form the drop down and then configure the following properties:

- Filter -> Select a shared filter from the list is required
- Date Range -> Select a date range the report should be run for

The filter and date range selected will be used instead of the report's default filter and date range. It is important to use contextual date ranges when running reports although a custom date range is configurable if required. Contextual date ranges are needed because the schedule will be running repeatedly so setting a specific custom date range will mean the same report is run each time.

If more than one report is added to a schedule it will run the reports one by one and then move onto the action to deliver all reports in one go.

> Only shared filters and shared reports can be added to schedules.

Action

The action section outlines what happens to the reports once they have been run by the scheduler. Reports can either be exported to a network share or emailed to one or more people. Select an action type using the drop down and then complete the necessary properties.

Whichever action type is selected, the same format options of .xls, .doc or .pdf are available.

> When exporting to '.xls', there is a limit of 65,536 rows enforced.

Email

All the standard email options are available. Multiple email addresses can be entered into each of the address properties (To, CC, BCC) using a comma (,).

> For schedules to be sent out by email, an SMTP server must be configured. The source email address configured for the MCS server will be used for scheduled emails.

Export

Reports can be exported to any of the network shares that the MCS server has been configured for. If no network shares are available to select from the drop down list then they must first be added in the configuration section (⚙) of the MCS website.

After a share is selected, a sub folder path can be entered. The scheduler will attempt to create the sub folder if it does not already exist. If a sub folder has already been added on the network share configuration then any sub folder entered here will be appended to that sub folder.

> Refer to the Network Shares section for more information.

6 System Status

The system status screen provides various indicators of the systems health. the system status screens can be accessed by click on the system status icon on the title bar of the MCS website. It is shown in the image below as a green dot:

If any of a server's status indicators are note green, this will be visible to the user by the dot on the title bar being yellow or red.

If there is an alert that has not been cleared, a yellow warning triangle will also appear on the title bar.

The site status screen displays activity over the entire system. It shows current and cleared alerts and has a historical log of events. There are 2 tabs that provide information on the status of the site.

Alerts

The *Alerts* tab shows important events that have happened in the Communication Service or on the PBX. They usually require some action to be taken.

> The alerts are shown until they have been cleared by clicking on the *clear* link or the *Clear All* button to clear all current alerts.

> Cleared alert entries are automatically deleted from the system after 90 days.

Events

The *Events* tab historically records key events that have happened in the system. This includes when key services have been stopped and started, failures to connect to a PBX connection etc.

Activity

The *Activity* tab displays a real time indication of the state of the devices that are currently being recorded and a usage graph to show previous activity.

> Hover over the status icons for Active Extensions to see information about the extension being recorded.

The server status enables the status of each server within the site to be monitored. To display the status of a specific server, click on the server name from the *Sites & Servers* navigation bar.

The *System Warnings* section shows the status of each component of the server using a traffic light system of colours to indicate the current status:

- Green indicates that everything is running ok
- Amber indicates a non-critical warning
- Red indicates immediate attention is required
- Unlit indicates the component is not configured or unavailable

The *Drive Information* section at the bottom shows the amount of free disk space available for each drive in the server. This includes any locally attached drives and any archive destinations that have been configured.

7 Filters

Filtering is used throughout the system to enable users to find specific calls or groups of calls. The system stores different types of information about each call which can be used to identify it. If any custom tagging information has been associated with a call then this can also be used in the filters.

Filters are created in the filters section of the MCS website and can be used when searching recordings and reports.

The MCS provides three types of filter:

Personal Filters

Any user on the system that has access to reports or recordings can create and manage their own filters. These filters will not be seen by other users of the system.

Shared Filters

Shared filters are visible by all users on the system (with the correct permissions). Shared filters can be deleted and managed by any user, not just the one that created it.

Refer to the shared filters section for more information.

Built-In Filters

Built-in filters are a type of shared filter that all users can see. They provide access to some commonly used filters and cannot be edited or deleted by any user. These built-in filters are used by many of the default reports provided to a user when they first login into the system.

Built-In Filters:

- Answered External Calls
- External Calls
- Inbound Calls
- Inbound External Calls
- Internal Calls
- Invalid Dialled Numbers
- Lost Calls
- Outbound Calls
- Outbound External Calls
- Service Codes
- Trunk to Trunk Calls

> Refer to the Filter Details section for information of creating and editing filters.

7.1 Filter Details

Filters can be edited/created in the Filters section of the website. To create a new filter, press the 'New' button at the top left of the screen. To edit an existing filter, press the more icon (⋮) next to the filter and select 'Edit' from the menu.

Each filter is split up into six sections:

- Details -> Contains the user definable name for the filter.
- Devices -> Options to filter by extensions, hunt groups, agents and trunks.
- Call Details -> Options to filter by call details such as direction, type, outside number etc.
- Duration -> Options to filter by call, talk and ring durations.
- Customer Details -> Options to filter by contact name, speed dial name, account codes or tag fields.
- Advanced -> Options to filter by Call ID, Service codes, Trunk to Trunk calls etc.
- Real-Time -> Options to filter real-time tiles only.

> Where the field has a text box entry, special characters can be used to search for patterns (%_,!). For more information, please refer to the Special Characters section.

> The following numeric fields also support filter ranges by using the + or - special characters:
>
> *Agent, Extension, Hunt Group, Trunk*

Details

The details tab just contains the user definable name for the filter. Nothing entered here will affect the filtering.

Name: This is the description that is used to reference this filter in other parts of the system. The name must be unique for the user or unique for the system if shared.

Devices

Filter calls by device.

Extensions: A specific extension or range of extensions. For multiple extensions separate each one with a comma and for a range use a dash. For example 1001,1002-1008,1010.

Extension Name: The name of the extension (This will be the extension's description if configured, otherwise it will be the extension's username).

Agent IDs: A specific agent id or range of agent ids. For multiple agents separate each one with a comma and for a range use a dash. For example 1001,1002-1008,1010.

Agent Name: The name configured against this agent id.

Hunt Group: A specific hunt group or range of hunt groups. For multiple hunt groups separate each one with a comma and for a range use a dash. For example 2001,2003-2008,2013.

Hunt Group Name: The name configured against this hunt group (This will be the hunt group's description if configured, otherwise it will be the hunt group's username).

Trunk: The trunk number that the call was connected on. This applies to external calls only.

> When apply filters to a Non-segmented report, the Extension/Agent filter options will also be applied to the First Rang, Last Rang and Answered on fields.

Call Details

Filter calls by the specific details of the call.

Outside number: The outside number presented for this call. For inbound calls this is the caller ID and for outbound calls this is the dialled number. Wildcards can be used to generalise the search, for example *09%,* any calls that have an outside number starting with 09 would be matched.

DDI: The direct dial number.

DNIS: The name associated with the direct dial number.

Direction: Was the call inbound, outbound or any.

Call Type: Was the call either internal, external or either.

Call Status: Is this call completed*, in progress*, recorded, not recorded or any of these.

Answered: Was the call answered or not.

> ⚠ Call details filter items cannot be used to filter the Agent or Extension Grid on a Real-Time Dashboard.

Duration

Filter calls by the call, talk or ring duration. Slide the bar from either end to increase/decrease the duration required.

Duration: The complete duration of time for the call, including ring, talk and hold time.

Talk Time: The talk time that the call was connected for.

Ring Duration: The time that the call was ringing.

Customer Details

Filter for specific customer related information.

Contact Name*: The MCS directory name associated with the outside number.

Speed Dial Name: The speed dial name associated with the outside number on the telephone system.

Account Code: The account code entered against this call. If more than one code is entered on a call, only the last one is saved.

Contact Match*: Was a contact matched in the MCS contact directories or not.

Field 1 to 5: Filter by the contents of the five custom tag fields.

Advanced

Notes*: Selects records that have had notes attached or if the notes contain specific words.

Serial*: The unique serial number of a specific recording.

Call ID: The id assigned to the call by the telephone system.

Logical Call ID: The logical call id used to link call segments together.

Global Call ID*: Call ID used to link CTI and Recording records in the database.

Trunk to Trunk*: Include or exclude trunk to trunk calls.

Invalid Dialled Number*: Include or exclude invalid dialled numbers. These are numbers where the external call attempt did not complete.

Service Codes: Include or exclude external calls to service codes.

Real-Time

Agent Status: Filter what is displayed on real-time grids. this can be used to hide logged out agents from the ACD grid.

Device Status: Filter what is displayed on real-time grids. this can be used to hide offline extensions from the Extension grid

> * Filter Items marked with an '*' are not applicable to Real-Time interfaces (Wallboard and Dashboard).

7.2 Shared Filters

Shared filters are accessible to any user on the system who has been given the correct permissions. These permissions are set via the Security Profile that has been assigned to a user's role.

For more information on shared filter permissions, refer to the security profiles section.

There are two ways to create a shared filter:

- Navigate to the Shared Folders section on the website and press the 'New' button. From this point follow the normal process of creating a filter.
- Share an existing filter by pressing the more icon (⋮) next to the filter and selecting 'Share' from the menu.

When creating a shared filter from an existing personal filter, a new copy of the filter will be created without affecting the personal filter. A new name for the shared filter will have to be provided by the user.

Shared Filters & Reports

Shared filters can be applied to both personal and shared reports when running them directly on the website. When running reports via a schedule, a shared filter must be used as personal filters cannot.

7.3 Special Characters

The use of special characters within the text boxes for a Filter enables the use of complex filter strings.

All Fields

The following characters are supported:

Special Characters	Description
Exclamation mark (!)	Not equal to
Percent (%)	Fuzzy matching (equivalent to a SQL LIKE %)
Underscore (_)	Fuzzy matching of a single character
Comma (,)	Can be used to search for multiple values at the same time

Device Fields

In addition to the special characters above, the following characters are supported when searching using a device based field (Extension, Agent, Trunk, Hunt Group):

Special Characters	Description
Plus sign (+)	Greater than or equal (e.g. 1000+ for extensions greater than or equal to 1000)
Hyphen (-)	Delimits a range of values to match (e.g. 1000-2000 for all extensions between 1000 and 2000 inclusive) or less than or equal to (e.g. -1000 for extensions less than or equal to 1000)

The example below shows what would be matched when entering combining multiple special characters using a comma:

- 1000-1005,!1003,1040,18%5,2000+

Matching endpoints: 1000, 1001, 1002, 1004, 1005, 1040, any that start with 18 and end with a 5, any with a value greater or equal to 2000.

> Device numbers are stored as text so when using greater than or less than, it is compared on an alphabetic level not a numeric level

8 Folders

Overview

Folders provide a way to manage the storage of documents, URLs, links to specific call recordings and audio files for use as Real-Time alarms. How the items are stored can be controlled by the user by creating their own sub folders and adding comments to indicate the reason and use of the item. Folders can be private to the user or they can configure them to be shared so other users can access the contents of the folder. Favourite links to call recordings can be stored so that frequently used calls can be accessed easily.

The use of folders can be beneficial for training by linking to or uploaded process documents on how to handle specific types of calls, and then specific examples of "good" and "bad" calls can be referenced to show how it should be done.

The Folders section is accessed by clicking the folder icon link on the title bar.

To create a new folder:

- See the Creating Folders section.

To create a new file:

- See the Creating Files section.

To create a link to a call recording:

- See the Creating Recording Links section.

Creating Folders

To create a folder:

1. Select the root folder to create the new folder in from the list in *My Folders* on the left hand side. Once selected the root folder will display in orange and the new folder will be created beneath this folder.
2. Select the *New Folder* button.
3. Enter a *Name* for the folder in the name field.
4. To make this folder and its contents available to all users check the *Shared* option if required.
5. Click *Save*

Creating Files

To create a new link to a file or upload a file to a folder:

1. Select the *New File* button.
2. Enter a *Name* for this file to reference it by and display to the users.
3. To upload a file select the *Upload* option.
    - Use the *Browse* button to select the file to upload.

      > When a user accesses this file they will need to have a valid application associated with the type of file uploaded to be able to view the file.
4. To link to an external file or website select the *URL* options.
    - Enter a URL to the file in the format "\\server\folder\myfile.doc", or enter a hyper link.
5. Click on *Save*.

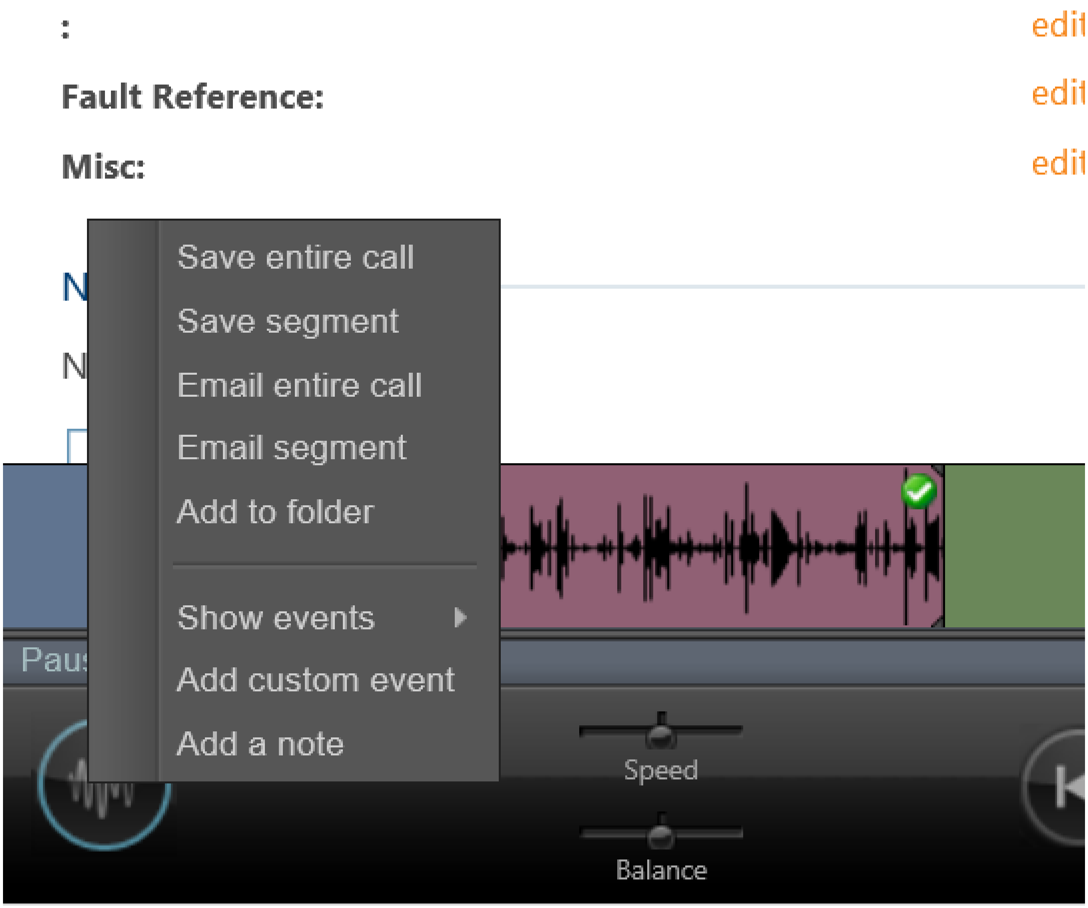
> The user is responsible for the contents and types of files uploaded. They should meet any company

> policies and be virus scanned before been uploaded.

Creating Recording Links

To create a new link to a call recording:

1. From the Recording screen find and open the recording to add.
2. Click on the playback start menu button (see image below) to show the menu
3. Select *Add to folder*, to display the list of the users folders.
4. Select the folder to add the link to.
5. Enter a *Name* for this recording to reference it by and display to the users.



6. Click *Ok*.

Sound Files From Alarms

The folders section can be used to store .mp3 files for use by the alarm notification features of the Real-Time Wallboard & Dashboard.

9 Site

Overview

The system is built on a modular design to provide scale up support when the limits of a single server are reached or specific environmental factors require different roles within the system to be performed by different servers (servers can be physical or virtual). Although roles can be performed by different servers each of them belongs to the same site and is managed through a single interface giving the user a single point to view the entire system.

Within each site there are several key roles that need to be performed. The roles need to be assigned to a specific server and a server can host and perform multiple roles.

- **WCF Server**: This is a required role for each server and provides core service processes
- **Database**: This role is for the server that hosts the Microsoft SQL Server database. There can only be a single server with this role
- **Licensing**: This role performs the license management and activation process for site. There can only be a single server with this role
- **Website**: This role is for servers that will host the website. There can be multiple servers with this role
- **Communications Gateway**: This role provides integration services for client applications
- **CTI Host Service**: This handles the CTI connection to the PBX for Phone Manager clients
- **Call Logging / Reporting**: These roles handle call logging information and historical reporting
- **Real-Time Reporting:** This role enables the services and features to support MiVoice Office Real-time Wallboard & Dashboard
- **Phone Manager Outbound:** If the Phone Manager Outbound dialler is to be run on this server, this role needs to be enabled.
- **Server Applications:** If Phone Manager or any of the Server applications such as Agent Hot Desking or IP SMDR are used, this role needs to be enabled.
- **Mobile Gateway:** If Phone Manager Mobile Softphones are being used, this role needs to be enabled.
- **Call Archiving / Recording:** These roles handle the MiVoice Office Call Recorder features. (Call Logging must also be enabled)
- **Mitel Handset Support:** This role enables the services that support the Mitel 6900 Series Handsets

In order to assign roles to a server navigate to Servers in the UI (Click on the word "servers"), then select a server from the grid and click Edit.

A site may need to be scaled up for several reasons:

1. The number of devices to log exceeds the capacity of a single server.
2. The management website needs to be accessed via the Internet and needs to be installed into a DMZ environment
3. The customer wishes to use a different SQL Database server.

For each server within a site the Site Settings applies to all servers within this site. If a server is required to have different Site Settings then the server will need to be moved to a different site. Multiple sites can be linked together, see the relevant section for a list of cross site supported features.

9.1 Features

Overview

The features section enables the configuration for the following parts of the system:

Section	Description
Contact Directories	Management of the global directory and any custom directories with the ability to be able to assign them to specific users.
Communication Service	The PBX configuration for Alarms, Agent Hot Desking, Group Messaging , Night Mode and IP SMDR.
Phone Manager	The Phone Manager configuration for Client Locations, Client Profiles, Macros, Call Banner Profiles, Client Toolbars, Call Recorder Integration and Meet-Me Conferencing.
Phone Manager Outbound	The PBX and database configuration for Phone Manager Outbound .
Call Recording	The configuration of Exclusion Lists, Inclusion Lists and Compliance Muting. For information on configuring call recording sources, see the Servers section.
Call Reporting	Configure the default settings for various reporting values such as Service Levels and report grouping durations.

9.1.1 Contact Directories

Overview

Contact information can be imported into the system to give more useful information about the outside party involved in a call and to provide directory search features to Phone Manager client users to help them find a contact to call. Multiple directories can be created and imports can be scheduled to run at a pre-determined interval so as to keep the data current. Directories can be created from different sources including text files (CSV format) and direct database connections.

Within Phone Manager there are several locations that can contain directory information. These include:

- Global contact directories, for example Microsoft Dynamics CRM, Salesforce.com etc
- Personal directories
- Microsoft Outlook personal contacts
- PBX Speed Dials

Depending on the type of contact then the information is populated in a different way.

Using the contact information a Phone Manager user can search the directory to find any matching contacts to dial. When an inbound call is received the relevant directories are searched automatically and the matching contact information is made available and displayed on the client toaster.

Central contact databases

For global contacts the information is stored and accessed from a single location. This can include a text file in CSV format or a direct database connection using ODBC or OLE DB. The contacts from these locations are imported into the system either manually or on a pre-configured schedule.

Each contact can contain up to 5 telephone numbers,10 custom fields (up to 1000 characters each) and a VIP flag and associated text. Each of the fields can be given a custom label to make it easier for the user, for example:

Field	Label
number1	Home Number
number2	Mobile Number
number3	Work Number
field1	Full Name
field2	Address 1
field3	Address 2
field4	Post Code/Zip Code

There can be multiple contact directories that are stored centrally and users can be assigned to one or more specified directories to allow them to access contacts that are applicable to them.

To assign directories to specific users see the Managing Directories section.

The global directories contacts can also have a VIP flag and text associated with them to allow for these entries to be highlighted on the Phone Manager banner as important contacts.

Personal Contacts

Personal contacts provide a user with their own personal contact directory. This works in a similar way to the global directory but only that user is able to search/add to this directory. These contacts are created by the users from the Phone Manager client software directly, not via the website. They are stored centrally on the server and will follow users as they move between computers.

Microsoft Outlook personal contacts

If a user has the "Download Outlook contacts" option enabled on their profile (see the Client Profiles section for details), personal contacts from within Microsoft Outlook can then be searched directly from the Phone Manager client.

> This requires Microsoft Outlook to be running within the same session as the Phone Manager client software. Only local contact folders are supported.

The contacts can be searched using the Home, Telephone or Mobile/Cell numbers as well as the first, last and company name fields associated with the Outlook contact. The only user that can then search and access these contacts is the PC user running both the Phone Manager client software and Microsoft Outlook.

PBX Speed Dials

The PBX contains its own directory in the form of system speed dials. These entries are configured from within Mitel Database Programming and the system will automatically download them directly from the PBX when connected. Each entry only has a name and number associated with them and either of these fields can be used to search.

Every user has access to search the system speed dials.

9.1.1.1 Managing Directories

Overview

Contact directories are managed from the '' -> Features -> Contact Directories section. Directories can be created, edited and deleted and imports can be run and scheduled. The status of each directory is shown with the number of contact records they contain and each directory can be searched to find specific contacts - see the Searching Contact Directories section.

Configuration

To add or edit a contact directory:

1. Access the Configuration -> Features -> Contact Directories section.
2. Click on *New* or *Edit*.
3. Select the **Details** tab.
4. Enter a **Name** for this directory.
5. Check the **Global** box to automatically assign this directory to any new Users created on the system.
6. If importing data into this directory then select the **Import source** from the drop down selection.
7. Configure the import source, see the Import sources section for details.
8. To schedule the import set the **Import interval** to the required value and the **Next import time** to when this should be run.
9. Check the **Delete unmatched records** if required
    - If checked, any records that no longer exist at the import source location will be removed
10. Select the **Field Names** tab.
11. Enter the custom labels for the numbers and fields.
12. Select the **Users** tab and add/remove the Users that will have access to this directory.
13. Click on *Save*.

Import sources

The system supports importing contact information from the following listed source types. Each import will require specific configuration:

- CSV File
- ODBC Query
- OLE DB Query

When importing contact data the following information needs to be provided:

- **id:** this must be unique and is used to identify the contact. This is used instead of the name or number as these are not always unique. This is also used to enable directory entries to be updated on an import as any fields that have changed will be updated as long as the id remains the same.
- **name:** this is the value that is used when the contact is displayed in search results and on the client toaster.
- **number1**, **number2**, **number3**, **number4**, **number5**: 5 different telephone numbers can be imported for a contact.
- **field1**, **field2**, **field3**, **field4**, **field5**, **field6**, **field7**, **field8**, **field9**, **field10**: 10 custom fields can be imported for a contact.
- **vip**: this flags the contact as a VIP and will be highlighted on any matches on the client toaster. If this is a VIP then set this value to true or 1, if this is not then false or 0.
- **vipText**: this is the text that will be displayed if the contact is a VIP match.

CSV File

This requires a text file that has been saved in a CSV file format. The first line of the file must contain the column headers, this allows any number and any order of columns to be used. All headers are case insensitive and will ignore any spaces.

> *id, name, number1, number2, number3, number4, number5, field1, field2, field3, field4, field5, field6, field7, field8, field9, field10, vip, vipText.*

Not all of the columns have to be provided, but there needs to be at least the *id, name* and *number1* present. The file must provide a unique value in the *id* column that can be used to identify this contact. Each of the columns must also be contained within double quotes. For example:

> id, name, number1, number2
>
> "1","John Smith","1233211231","6544566544"
>
> "2","Jane Doe","3699633696","2588522585"

If no value is available for a specific column then use a blank entry. Any additional columns will be ignored.

Set the **Import source** to be *CSV File* to configure the location of the import file. For scheduled imports this needs to be a file path location that is accessible from the **server**, for example on the local C:.

> UNC paths can be used but they require the Local System account on the server to have access to the file.

For one off or manual imports then the **File path** does not need to be configured as this will be prompted for when the import is run.

> There must be a single record on each line, no carriage return is allowed in any field.

ODBC & OLE DB Query

The configuration for the ODBC & OLE DB is the same. Set the **Import source** to be either *ODBC Query* or *OLE DB Query* and configure the **Connection string** that will be used to connect to the database.

This needs to be set to the DSN data source for the ODBC/OLE DB database in the format of “DSN=dbserver”. Alternatively a valid database connection string can be used and depending on the value an appropriate database driver may need to be installed on the server.

> For help in determining what the connection string should be this web page can be a useful reference (this is an external link, Mitel are not responsible for its contents): http://www.connectionstrings.com.

In the **Command text** field enter the T-SQL expression that will be used to retrieve the data. The query must provide a unique value in the first column that can be used as the primary key to identify this contact. The columns will be inserted into the directory in the following order:

> primaryKey, displayName, number1, number2, number3, number4, number5, field1, field2, field3, field4, field5, field6, field7, field8, field, field10, vip, vipText.

If no value is available for a specific column then use a blank entry. Any additional columns will be ignored.

> **Name Matching - what order is given to matching to display on call notifications**
>
> If the caller ID is less than or equal to the max extension length configured on the dial plan then all the users are searched that have this device associated and the first match is used (Displaying forename then surname). If no match is found then it will use the extension name provided in the SIP messaging.
>
> If the caller ID is greater than the max extension length configured on the dial plan then checks directory

> matches from (in order of preference):
>
> 1. Personal Contacts
> 2. Global Contacts
> 3. Speed Dials
>
> If no matches are found then the caller ID is used.

9.1.1.2 Searching Contact Directories

Overview

Contact directories can be searched from the website in order to check that the data imported is correct.

Searching

To search a directory:

1. Access the ''-> Features -> Contact Directories section.
2. Select the directory to search from the navigation pane on the left hand side or click on the directory's search icon in the Contact Directories grid view.
3. Enter a search term in the text box and click on the *Search* button.
4. All the records containing the search term will be searched and any matching entries will be shown below.
5. Select a matching entry and click on *View* to see all the fields for this contact record.

9.1.2 Communication Service

Overview

The Communication Service section enables the configuration for the PBX specific features to be managed. This includes:

Application	Description
Alarms	Used to send alerts generated by the PBX or CT Gateway to a configured list of email addresses or to Phone Manager Team Leader clients.
Agent Hot Desking*	Using Agent Hot Desking, agents can log onto any keyset and still receive direct dialled, intercom and hunt group calls.
Call Routing*	This feature s designed to monitor various devices on the telephone system and route any ringing calls according to rules.
CPN Substitution*	The feature is designed for organisations that have a national presence that wish to present the calling party number (CPN) and/or calling party name of a local branch, no matter which branch a call is made from.
Group Messaging *	This feature enhances Voicemail functionality so that a single message can notify more than one extension.
Night Mode	Night mode enables the PBX to automatically be placed into and out of night mode on a defined schedule.
IPSMDR*	IPSMDR provides a TCP/IP server feature to an external application requiring the SMDR data feed from the PBX.

* Some features may require additional licensing when used in a multi-node environment where there is more than one PBX.

9.1.2.1 Alarms

The Alarms section is used to send alarms that are generated by the PBX or Mitel CT Gateway to users to notify them there is an issue.

Alarm notifications can be sent out using one or more of the following methods:

- Email, alarms can be sent out to one or more email addresses
- 6900 Handset Display, alarms can be display as warning messages on the screens of 6900 handsets.
- Phone Manager Team Leader, alarms can be sent to Phone Manager clients and are displayed on a dedicated alarm notification form.

Alarm Profiles

Alarm profiles provide a way to send different types of alert to different locations. Each alarm profile created send out all alarms generated or can be filtered to only distribute a sub-set of alarms. This provides flexibility to send only specific alarms to specific people.

For example, IT employees could be notified about infrastructure of licensing issues and administration staff could be notified about emergency calls.

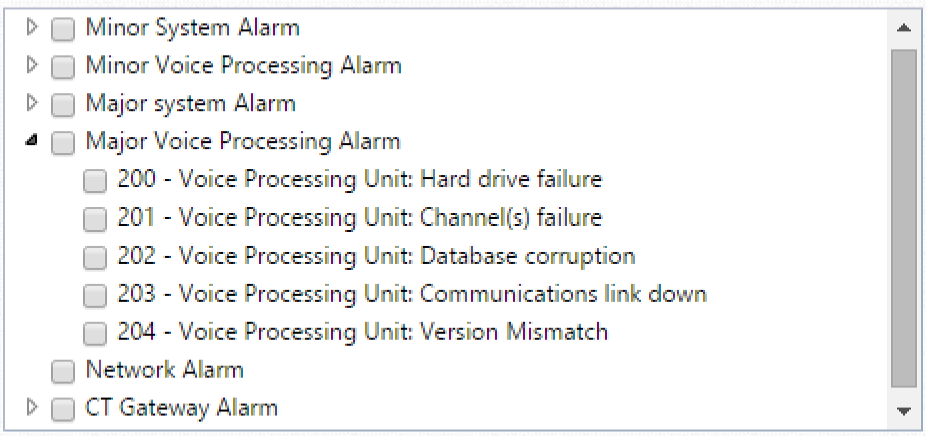
Configuration

To configure an alarm profile:

1. Access the Communication Service-> Alarms section.
2. Click on *New* to create a new profile or highlight an entry and click on *Edit* to modify an existing profile.
3. Enter a **Description** to describe what this alarm profile is for, this is used in the notifications to help the user determine what this alarm is for.
4. To alert for all alarms check the **Respond to all alarms** checkbox.

   > Responding to all alarms can generate a significant number of notifications.

5. To configure notifications for a specific set of alarms uncheck the **Respond to all alarms** and select the alarms from the list shown.

6. To send alarms via email, check the **Send email alerts** check box and enter the email address to send this to in the **To address** and **CC address** fields.

   > The system needs to have the email setting configured to send emails, see the Email section for details.

7. To send alarm notifications out to any Phone Manager Team Leader clients, check the **Alert Team**

Leader clients checkbox. This will cause a popup box to appear on any PC that is running a Phone Manager client licensed for Team Leader with the details of the alarm.

> If the Phone Manager Team Leader client is associated with an extension that is a Admin keyset then they have the option to clear the alarm and this will clear it from the PBX.

8. To display alarm notifications on the screen of Mitel 6900 handsets, check the **Alert 6900 Handsets** checkbox. Press the 'Select Handsets' button and then choose which of the phones should receive the messages.
9. Click on *Save* to save or update this profile.

Clearing Alarms

Depending on the type of alarm generated and it's source, the alarm may clear automatically or may need to be cleared by the user. To clear telephone system alarms, the relevant feature code must be entered on an administrative telephone extension (please refer to the telephone system manual for feature code information).

Alarms can be cleared by:

- Entering a feature code on a MiNET or Digital Handset
- Using the Clear Alarms key on 6900 Handset
- Using Phone Manager Team Leader client

Alarms that clear automatically will be removed from Phone Manager and 6900 Handsets automatically.

9.1.2.2 Agent Hot Desking

Overview

When users need to "Hot Desk" across multiple MiVoice Office nodes, "Agent Hot Desking" can be used as an alternative to the built-in Hot Desk feature. Using Agent Hot Desking, users can log onto any keyset using an agent ID with the feature code 328 and receive direct dialled, intercom and hunt group calls.

As well as inbound call routing, voicemail and keyset message notification will follow the agent as well as outgoing caller id (CLI) or Calling Party Number (CPN), username, description and class of service settings. When agents are logged out, calls can be forwarded to voicemail or any internal / external number.

The agent ID can simultaneously be a member of inbound ACD hunt groups and receive the associated calls as normal.

> Agent Hot Desking is not the same as the built-in hot desking feature 348 within the PBX. If multi-node hot Desking is required it can be used instead of the MiVoice Office 250 built-in hot desk feature.

How does it work?

Agent Hot Desking uses phantom extensions on the MiVoice Office 250 PBX to create a virtual keyset for each Agent Hot Desking user. Each phantom created has the same number as the associated hot desking agent ID. Agent Hot Desking agent IDs are then added to a dedicated ACD Hunt group configured on the MiVoice Office 250 PBX.

When an agent logs into an extension, the Mitel Communication Service will forward all calls from the user's phantom to the extension they have logged into. When the agent logs out, calls are forwarded to a "logged out destination" which can be configured by the user (the default can also be configured but is usually set to the Voicemail application on the MiVoice Office 250 PBX).

Any user specific programming needs to be done on the user's phantom extension; DDI, username, description, class of service, calling party number and mailboxes. The Agent Hot Desking feature will then apply these settings against any extension a user logs into.

What does it do?

- The username and description on the extension logged into will be changed to match the user's phantom device username.
- Any voicemails alerting the user's phantom device will be duplicated to the extension they are logged into.
- A Forward All Calls is placed on the user's phantom to direct calls to where they are logged in, this will forward any internal or external calls that ring the phantom.
- Optionally the class of service can be changed on the extension they logged into to match their phantom's class of service.
- Outgoing caller ID can be changed to match that set against the user in the website configuration.

What doesn’t it do?

The way Agent Hot Desking uses phantoms means that a few of the normal phone system features are changed:

- Extension Number – The extension number where the users logs in DOES NOT CHANGE
- DND – Works when using Agent Hot Desking, but DND Override will not work for a caller to the agent
- Reverse transfer – Has to be entered using the physical extension the agent is logged into. Attempting to Reverse Transfer the user's phantom will fail since the call is not ringing at the phantom. Using Phone Manager to reverse transfer alleviate this problem.
- System forwarding – When using Agent Hot Desking, inbound calls have followed a manual forward from the phantom to extension where the user logged in. This means any system forward placed on the users phantom extension will not be followed. To workaround this, Agent Hot Desking will remember

any manual forward placed on the extension when an agent is logged in and apply/remove this when logging in and out. (e.g. While logged in, if a user sets a FWD NO ANSWER to voicemail, calls will follow the manual forward rule. When the agent logs out the manual forward to voicemail will be removed returning the extension to its normal state. If the Agent then logs into a different extension, the FWD NO ANSWER to voicemail will automatically be "remembered" and applied to the new extension).

- Record-A-Call – The value for “Mailbox User-Keyed Extension” must be set to Yes for each extension that an agent could log into since at the time the user selects Record-A-Call they will not be associated with their phantom extension. The user must enter their own phantom extension mailbox number to record the call.
- DSS Console & Busy Lamp Fields configured on physical extensions – Buttons programmed up as phantom extensions will display no light status since the phantom is permanently in the free state and although the button can be used to dial the user, it will not be suitable for BLF. This is because the button will be showing the status of the phantom & not the extension where the agent is logged in. Instead use the Mitel Phone Manager software to display the status of an Agent Hot Desk user.
- System flags – camp on flags configured on the phantom cannot be used to provide busy conditions. These need to be configured on the physical extensions used by the Agent. Agent Hot Desking users should always have a logged out destination configured.
- UCD Hunt Groups - When using Agent Hot Desking UCD hunt groups cannot be used. If the Hot Desk user's phantom gets added to a UCD hunt group, any calls will follow the manual forward set on the phantom causing the call to stop ringing at the hunt group.

⚠	Ensure the customer knows the restrictions of the solution upon installation and allow them to make a decision on the benefits and restrictions of using native hot desking or agent hot desking

Agent Hot Desking Requirements

Agent Hot Desking requires the following capacity on the phone system:

- One phantom extension for each Agent Hot Desking user
- One extra phantom for the whole system if using default class of service features
- One ACD agent hunt group for Agent Hot Desk users to log in and out of
- When agents need to log in across nodes, the ‘Remote ACD Hunt Groups’ premium features must be enabled on all nodes Agent Hot Desking is required
- Ensure that all nodes are aware of each others message notification stations

Configuration

Configuration is required on both the MiVoice Office PBX and in the Mitel Communication Service user interface to enable Agent Hot Desking.

PBX Configuration

Open the Mitel Database Programming:

1. Create a phantom extension for each Agent Hot Desk user.
2. Create a corresponding agent ID for each user. (The phantom numbers and the agent IDs should be identical).
3. Program each phantom as if it were being used as the user's extension.
4. Program the username, description, calling party numbers, class of service and create a voice mailbox if required against the phantoms.
5. Point any DDI numbers to the phantom device.
6. Create a dedicated Agent Hot Desking ACD agent hunt group for the users.

7. Add the Agent Hot Desking agent IDs to this hunt group.
8. Add the agents to any other hunt groups they need to be members of for inbound ACD calls.

MCS Configuration

To configure Agent Hot Desking:

1. Access the Features -> Communications Service -> Agent Hot Desking section.
2. Select the **Enable** checkbox to turn on hot desking.
3. Select the hunt group that has been configured on the PBX from the **Hunt group** drop down selection.
4. Configure the options for when users are logged out, see the Logout Settings section.
5. Configure the options from the Advanced Settings.
6. Click on *Save*.

Logout Settings

The logout settings control the call behaviour when the users are logged out of the system.

Logged out destination: This is the default destination that calls are routed to when the agent is logged out. If users are allowed to override this destination then this initial logged out destination will be used until the user overrides it.

Allow manual forwards: If this option is checked then agents have the ability to override the logged out destination. To override this when the agent is logged in, a user will set a FWD ALL CALLS (default feature code 355) and enter the required destination. The user is automatically logged out of the extension and calls are immediately routed to the required destination. The new destination is now set to the default "logged out destination" any time this user is logged out.

Automatically log agents out: Enabling this option will automatically log out all Agent Hot Desking agents at the specified **Time**.

Forward messages when logged out: If the agent configures their logged out destination to be another extension, then the message waiting indications on the user's phantom will notify the logged out destination when they are logged out.

Advanced Settings

Change calling party number: This will automatically change the outgoing calling party number used for the calls to be the value configured against the user's phantom device. If **Reset settings on logout** is enabled the **Default calling party number** value will then be used to set the caller ID on the extension when the agent is logged out.

> For the MCS to be able to change the Caller ID programmed against an extension, it must be configured with the Extension Programming Password for each node.

> The outgoing calling party number can only be set to values supported by the PBX and by the network trunk line provider. Typically this will be configured as the user's DDI number.

Default calling party number: This is the calling party number that is configured on extension when an agents logs out of hot desking when using the **Reset settings on logout** option.

Change class of service (COS): This will change the class of service that is configured on the extension an agent logs into to match the COS configured on the user's phantom extension. This will enable the agent to only make calls that are permitted for their phantom extension.

Default COS extension: The class of service on this extension will be used when the agent is logged out of hot desking when using the **Reset settings on logout** option.

Change extension username: This will change the username and description of the extension to match their phantom when the agent is logged in. Intercom calls made by the user will therefore be identified for the receiving party.

Change station speed dials: This will change the station speed dials of the physical extension to match the user's phantom when the agent is logged in.

Reset settings on logout: This will clear the username and description on the extension when the agent is logs out and set the class of service and calling party number to be default. If not enabled, the extension will be returned to its original configuration (the configuration before an Agent Hot Desking user logged).

9.1.2.3 Call Routing

Call Routing is designed to monitor various devices on the telephone system and route any ringing calls in one of several ways:

- Route all calls based on the result of a database lookup using the DDI or Caller ID of the incoming call.
- Route calls that are queuing at the device (a busy Hunt Group for example)
- Route calls to the last agent that had contact with the caller

When routing calls, the target destination can be one of the following:

- A device on the telephone system (Extension, Hunt Group, CRA)
- An agent on the telephone system (DB return values only)
- An external number (Calling Party Number and Name can also be provided)

> An agent can only be used as a routing target when using the database lookup and when there is a device as an overflow.

Licensing

The call routing feature is a licensable feature within the MiVO Application Suite. If your system is licensed, the 'Call Routing License' should be visible within the Communication Service section of the Site License section of the website.

Call Routing Rules

The call routing engine monitors 1 or more rules that define how and where the engine should route calls to. Each rule has a 'Monitored Device' this device is an extension on the telephone system that the engine will monitor for incoming alerting calls. An incoming call will trigger the rule to be fired and the database look up to be made.

How Calls Are Routed

The routing process starts when a call starts alerting a Monitored Device. If the AlphaTag parameter and/or the AccountCode properties are populated for the rule, the call will first be modified using the _MD command. Once this command completes (the response has been received from the telephone system) or if neither the AlphaTag nor the AccountCode properties are set, the call will be routed to the target destination using the _MO (move call) command or the _DF (deflect call) command. The command used will depend on how the call is being presented to the Monitored Device.

If the command to route the call fails, the engine will attempt to route the call to the Overflow destination for the rule. If the target for the call is an agent and the agent is not logged in and in the free state, the call will also be routed to the Overflow destination.

Telephone System Configuration - Routing All Calls

To route calls using the Call Routing feature, the telephone system must be configured to send calls to the Monitored Device for each rule.

The monitored device can be a phantom on the telephone system or a physical extension. In addition to setting up the Monitored Device, it is advised to program a UCD hunt group on the telephone system for each Monitor Device for the following reasons:

- The Call Routing engine only has to deal with a single call per rule at any point in time. This means there is less chance of routing failures.

- The recall destination of the hunt group can be used to move the call on to an overflow if the call routing engine is failing or the MiVoice Office Application Suite is offline for any reason.
- There is less load on the target database because only one query per rule can ever been run at any point in time.

The Monitored Device should be added to the UCD hunt group and any calls to be routed should be pointed at this hunt group

> When routing calls to external numbers, the Class of Service of the Monitored Extension will be used by the telephone system when evaluating whether to allow the external call.

For more information, please refer to the following sections:

- Database Lookup
- Routing Queuing Calls
- Last Agent Routing

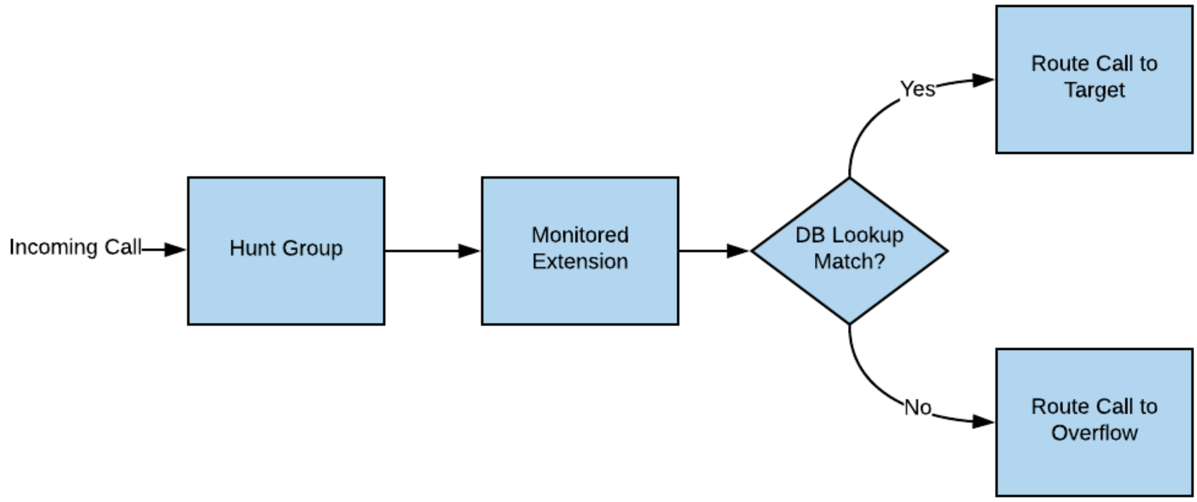
9.1.2.3.1 Call Routing - Database Lookup

Performing a database lookup to determine the target destination is the most common use of the call routing engine. To perform a database lookup, the following properties of the rule must be set:

- Select 'Database Lookup'
- Connection String -> Set to be a connection string for an ODBC compliant database*
- Stored Procedure -> Configure to be the name of the stored procedure to call on the SQL Server database

Routing Flow

The diagram below shows how the call routing should be configured when using a DB lookup rule. The monitored extension should be added to a UCD hunt group so that calls are presented to it one at a time. For each call that alerts the monitored extension, the call routing system will perform a DB lookup and either transfer the call to the resulting target or the overflow configured against the rule.



Connection String

An ODBC connection string is required to tell the routing engine how to connect to the database. Below are some examples of ODBC connection strings for commonly used databases:

SQL Server

The connection string below is an example connection string for an SQL Server database. The database, server, username and password properties must all be updated in the connection string to match those of the target database.

“Driver={SQLServer};Server=[server];Database=[database];Uid=[username];Pwd=[password];”

> If connecting to a specific SQL Server instance, it must be passed with the server property: servername\instancename.

> any ODBC drivers required for the database connection must be installed on the MCS sever manually.

Stored Procedure

The routing engine requires a specific stored procedure to be defined on the database it is connecting to.

The stored procedure must have the following parameter definition:

```
CREATE PROCEDURE [dbo].[ENTER_STORED_PROCEDURE_NAME_HERE]
(
 @cli as varchar(50),
 @ddi as varchar(50),
 @routetodevice as varchar(50) output,
 @alphatag as varchar(50) output,
 @accountcode as varchar(50) output,
@mailbox as varchar(50) output,
@cpnumber as varchar(50) output,
@cpname as varchar(50) output,
)
```

The @cli and @ddi parameters will be populated with the details of the call to be routed. If the call is internal, the @ddi parameter will be a zero length string.

The output parameters will then be used by the routing engine to route the call.

Route to Device

The @routetodevice can be one of the following:

- A device on the telephone system (extension, hunt group, CRA etc.)
- An agent on the telephone system
- An external number

To route the call to the overflow, pass back a null or zero length @routetodevice from the stored procedure.

To route to an agent, enable the 'Agent Return Value' options or prefix the return value with an 'A'.

> When routing to an agent, the system will check that the agent is logged in and is available to take a call. If not, the call will be routed to the overflow.

If the @routetodevice is an external number (any number longer than the 'Max Extension Length' configured in the dial plan will be treated as external), the Calling Party Number (@cpnumber) and Calling Party Name (@cpname) for the external call can be set.

> Only set the @cpname property if the trunk lines support it. Setting it when they don't will cause the routing of the call to fail.

Account Code

If the @accountcode property is set, the value will be entered on the call and will override any account code statically configured on the rule.

> Account Codes can only be set on external calls.

Alpha Tag

If the @alphatag output value is populated, the value can be used to change the outside caller name or trunk outside name on the telephone system for the call.

9.1.2.3.2 Routing Queuing Calls

The Call Routing engine can be used to route calls which are camped-on to a hunt group. These calls are in the 'Queuing' state on the telephone system because there are no free extensions or agents within the hunt group to be offered the call.

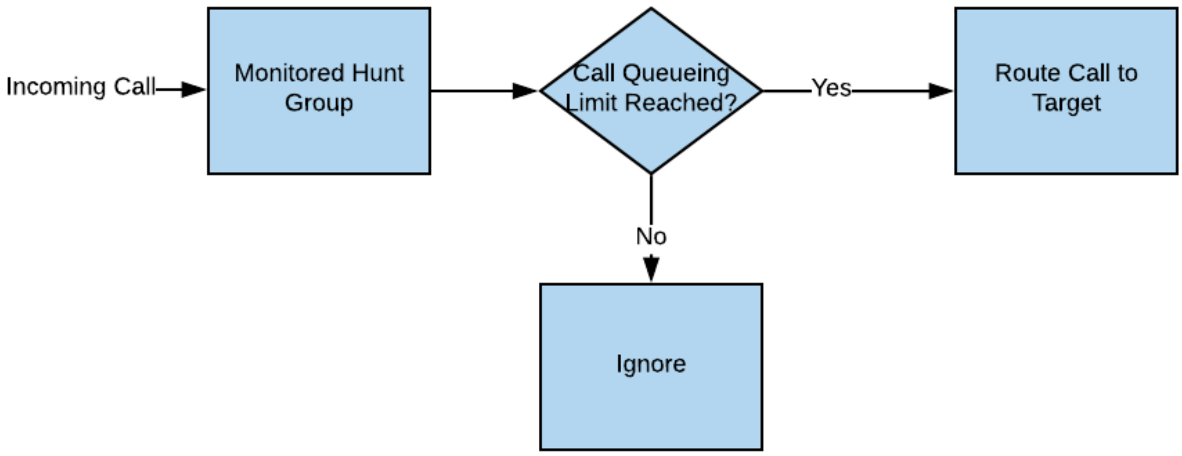
To use the system in this manner, the following properties of the routing rule must be set:

- Monitored Device -> This should be configured to be the hunt group to monitor for queued calls
- Queue Length -> 0 means route all queuing calls, Greater than 0 and only calls higher in the queue than the value set will be routed.
- Destination -> Should be set to the hunt group or device where the call should be routed to.

> When routing on Queue Events, a fixed destination must be provided. The database lookup can only be used when routing all calls.

Routing Flow

The diagram below shows how the call routing should be configured when using a 'Queuing Event' as a trigger. The monitored device should be a hunt group. any queuing events received from this group will be processed by the routing system. If the queue position triggers the rule, the call will be routed to the target destination, otherwise the call will be ignored.



9.1.2.3.3 Last Agent Routing

This feature uses the caller ID of an inbound call to attempt to route a call back to the last agent who handled a call from the same number. The feature works by attempting to locate the agent that last handled the call and then checks to see if they are logged in and available to take the call. Only calls that were answered by an agent are taken into account.

Configuration

The following settings apply to any call routing rule configured to route calls back to the last agent that handled the call.

Search Limit Type & Duration

The search limit type and duration specify how far back in time the system will look through the call history to find a caller ID match. The search duration is limited to a maximum of 48 days.

Include Outbound Calls

This settings controls whether the call history search includes outbound calls or just searches for inbound calls.

Overflow

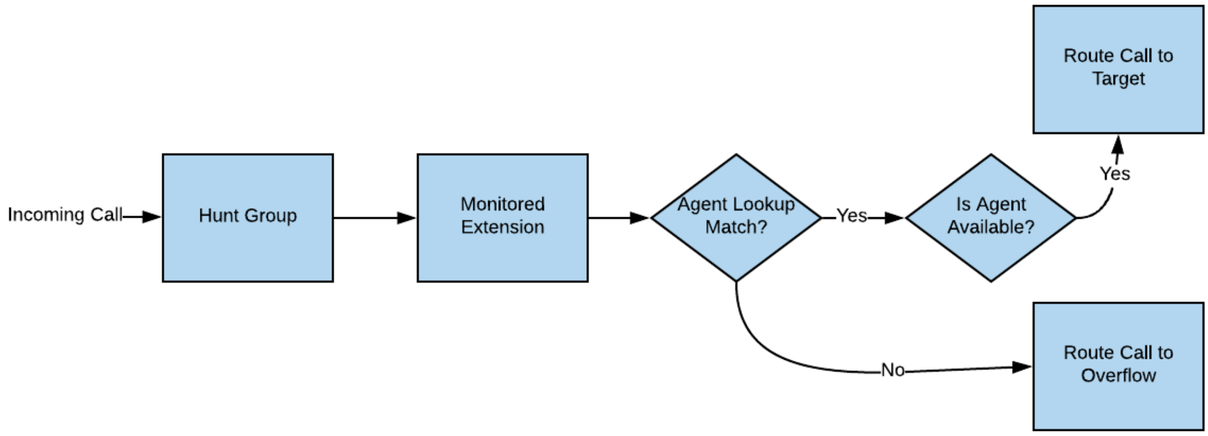
The overflow destination is used if no caller ID match is found or if a match is found but the target agent is not logged in or not available.

Minimum Talk Time

When search for call history matches, only calls that have had a talk time exceeding the minimum talk time will be included.

Routing Flow

The diagram below shows how the call routing should be configured when using a DB lookup rule. The monitored extension should be added to a UCD hunt group so that calls are presented to it one at a time. For each call that alerts the monitored extension, the call routing system will perform a call history lookup to find the last agent that spoke to the caller. If there is a match and the agent is available, the call will be routed to the agent directly. If not, the call will be routed to the overflow configured against the rule.



Once a call is routed, the call is no longer a hunt group call and must be answered by the agent. A forward on the agent's extension can be used to route the call back to a hunt group if they do not answer.

9.1.2.4 CPN Substitution

CPN Substitution is a new feature of the MiVoice Office Application Suite. The feature is designed for organisations that have a national presence that wish to present the calling party number (CPN) and/or calling party name of a local branch, no matter which branch a call is made from. The CPN Substitution feature looks at the number being dialled and the extension making the call and uses this information to perform a database lookup to find out which calling party number/name should be presented.

Licensing

The CPN Substitution feature is a licensable feature within the MiVO Application Suite. If your system is licensed, the CPN Substitution should be visible within the Communication Service section of the Site License section.

Enabling CPN Substitution

To use CPN substitution it needs to be enabled at system level but checking the 'Enabled' box and then on a per user level by using the Phone Manager Client Profiles.

Supported Dialling Methods

The following table outlines the scenarios in which it is possible for CPN Substitution to dynamically change the calling party number/name on a call being made.

Application / Dialling Method		CPN Substitution Supported?
Phone Manager Desktop	MiNET/Digital	Yes
	6900 Series	No
	Analogue / Generic SIP	No
	Softphone	No
Phone Manager Mobile	Calls via Desktop	Yes
	Calls via Office Link	Yes
	Calls via Softphone	No
	Calls via Mobile	No
Phone Manager Outbound	All	Yes
Handset	Manual calls from MiNET, Digital, Analogue or SIP (Including 6900 series)	No

If there is an extension programming password configured on the telephone system, MCS needs to know what this is to be able to change the Caller ID in some scenarios. Please refer to the Node Configurations section for more information.

> ⚠ If a call is made using a method that is NOT supported, the calling party name and number presented will depend on the telephone system programming for the extension making the call.

9.1.2.4.1 CPN Substitution Data

The system decides on which number/name to use on a call by using the number being dialled as a key to look up a record in the CPN Substitution table.

The CPN Substitution table consists of a mapping between area codes and the name/number that should be used when dialling them.

Populating the CPN Substitution Table

The CPN Substitution table can be found in the 'CallRecorder' database within the MCS SQL instance. The table is called – '_AS_AreaCodeMapping'.

Currently, there is no way to import data into this table automatically, data will need to be added manually by the customer.

Table Structure

Column	Description
[AreaCode] [varchar](15) NOT NULL	The Area Code to dialled numbers will be searched against.
[CallerID] [varchar](20) NOT NULL	The calling party number that will be presented when making the call.
[CallerName] [varchar](100) NOT NULL	The calling party name that will be presented when making the call.
[Idx] [bigint] IDENTITY(1,1) NOT NULL	Not currently used

The 'AreaCode' column can be populated with as many digits of a phone number as required. The stored procedure will find the match with the longest number of digits when using the dialled number to search. This allows for specific caller id's to be present for a specific target number at the same time as presenting a generic caller id for an area code.

For example, the following entries are in the mapping table:

AreaCode, CallerID, CallerName

1480, 4802221111, Area Based CPN

14809619000, 4801112222, Customer Based CPN

If a user is dialling 1-480-961-9000, a match will be found on the full number and the area code. The full number is longer so the customer based CPN will be used in this scenario. If a user is dialling 1-480-962-1000, the only match will be on the area based CPN.

> All entries in the CPN Substitution table's 'AreaCode' column must contain the toll digit and must not contain any non-numeric characters.

9.1.2.4.2 CPN Substitution Configuration

Once the CPN Substitution feature has been enabled, it will apply to all calls made on the telephone system that are made using a supported method.

> If CPN Substitution has been enabled and the license has been applied, it may require a restart of the MCS CTI Host service before the feature will work.

Using an Alternate Database

If required, the stored procedure that is called by the CPN Substitution feature can be changed. By changing the stored procedure being called, a custom stored procedure can be written to perform the CPN lookup on a different database if required by the customer.

To change the stored procedure used, the following configuration value must be changed in the '_Configuration' table within the MCS's database:

- ConfigurationName = 'Stored_Procedure'
- ConfigurationArea = 36

The default value for this configuration is '_AS_SearchAreaCodeMapping'.

The stored procedure that this is changed to, needs to have the following parameter structure:

```
CREATE PROCEDURE [dbo].[_AS_SearchAreaCodeMapping]
(
    @AreaCode as varchar(15),
    @SourceExtension as varchar(15) = '',
    @SourceAgent as varchar(15) = '',
    @CallingPartyNumber as varchar(20) = '' output,
    @CallingPartyName as varchar(100) = '' output
)
```

The *@CallingPartyNumber* and *@CallingPartyName* should be populated with the required values. If either of the values are set to null or blank, the number and name will not be set and the CPN details configured on the telephone system against the extension making the call will be used.

Command Timeout

When using the CPN Substitution feature, a default timeout of 2 seconds is used for any searches of the CPN Substitution table. If a query reaches this timeout it will fail and the calling party name/number configured against the extension will be used. The command timeout can be increased if required by changing the following configuration value in the '_Configuration' table within the MCS's database:

ConfigurationName = 'CommandTimeout'

ConfigurationArea = 36

ConfigurationValue = 2 <- this is the default value, in seconds

When the query is taking place it is blocking the dialling process for Phone Manager Clients and Phone Manager Outbound.

9.1.2.5 Group Messaging

Overview

This feature enhances Voicemail functionality so that a single message can notify more than one extension. An example of this is where the recall destination of a hunt group is set to Voicemail and typically the supervisor is the only extension with the notification of outstanding voicemail.

Group message notification will replicate the message notification on a list of additional devices as long as a message is outstanding on the primary device configured.

Remember that notifications will be sent for ALL outstanding messages at the source extension so if you intend only to send notifications for a specific hunt group, it may be necessary to create a dedicated phantom extension for the message notification configuration in the hunt group voicemail settings in MiVoice Office DB Programming.

Configuration

To configure a group message notification rule:

1. Access the Communication Service -> Group Messaging section.
2. Click on *New* or *Edit.*
3. Enter a **Description** used to identify this rule.
4. Enter the **Source extension** from where the message notification will be duplicated.
5. In the **Target destinations** select either **Hunt group** or **Extensions**. Then select either a specific hunt group or multiple extensions that will also be notified of the Voicemail message while the **Source extension** maintains an outstanding message notification.
6. Click on *Save* to save the rule.

9.1.2.6 Night Mode

Overview

The Mitel Communication Service Night Mode feature enables the PBX to automatically be placed into and out of night mode on a defined schedule and refers to the MiVoice Office 250 Night Mode feature. Without this the feature can only be activated manually by pressing a Night Mode button on an Administrator flagged extension.

Configuration

To configure the night mode schedule:

1. Access the Communication Service -> Night Mode section.
2. Select the **Enable** checkbox to turn on night mode scheduling.
3. Enter an Admin Extension - this needs to be an extension that has been configured in Mitel Database Programming with the Administrator flag. It will be used as the device to enable/disable the night mode feature on the PBX.
4. Enter the time schedules for each day of the week.
5. Click on *Save.*

The server will now automatically set day/night mode according to the time on the Communication Service server.

9.1.2.7 IP SMDR

Overview

If licensed, the server is capable of providing an IP based real-time SMDR server function for external applications such as call logging/call accounting software and tracks inbound and outbound trunk based calls.

The feature can work in two different modes. Push mode where the Communication Service connects to an application running on a remote computer and sends the SMDR information and Local mode where the remote application connects to the Communication Service.

Configuration

To configure the IP SMDR feature:

1. Access the Communication Service -> IP SMDR section.
2. Check the **General** -> **Enabled** option to enable the IP SMDR.
3. Set the **Local Port** to the TCP port number that the Communication Service will accept connections on, the default is 2007.

   > This port will need to be opened on any firewall software running on the server.

4. Configure the **Item padding character** to use to pad out any blank entries in the SMDR record to ensure that all records are provided in a fixed length, the default character is "0".
5. To enable push mode check the **Push connections** -> **Enabled** option.

   > Both push and local modes can operate the same time.

6. Enter the **Remote port** and **Remote IP address** that the Communication Service will try to connect to the remote application on.
7. Click on *Save*.

SMDR Format

Each SMDR line received over IP will contain the following fixed length elements in the order below:

Element	Element Location	Length	Description
TimeStamp	1	19	The timestamp of the message
Direction	2	5	The direction of the call, |IN | or|OUT|. This element is surrounded by | pipes
CallID	3	22	A unique identifier for the call that can be used to link events about the same call
Trunk	4	7	The device ID of the trunk the call is taking place at
Endpoint	5	7	The device ID of the endpoint the call is currently at
Source Endpoint	6	7	The device ID of the source endpoint on Transferred & Diverted events. This element with be empty on other event types
Caller ID	7	15	The Caller ID of the external party if provided
Contact Name	8	14	The Contact name for the external party if provided. This element is surrounded by | pipes
DDI (DID)	9	15	The number dialed by the external party if the call is inbound
DNIS	10	14	The name associated to the inbound call line. This element is surrounded by | pipes
Account Code	11	12	The current account code that has been assigned to the call
Event Type	12	14	The event type for the SMDR message. This element is surrounded by | pipes

A line of data ends with carriage return and line feed characters. Each element is separated with a space, this means that each line will be 162 characters long

Example Data: 2012-03-09 12:46:59 |OUT| 20120309004659821900470092808 0001843 0000000 0000079XXXXXXXX | | 000000000000000 000000000000 |RINGING |

Event Types The following event types can be received on the IP SMDR connection.

RINGING - Received when a call alerts a device. This can happen when the call first starts ringing on the system or when a call is transferred to ringing or when a call is put on hold and then recalls.

ANSWERED - This event occurs when a call first enters the CONNECTED state on the system. This message is effectively the first "CONNECTED" events - Any further events of this type will be reported as CONNECTED.

HOLD - Occurs when a call is placed on hold on the telephone system. This event will be followed by a CONNECTED event when the call is retrieved.

CALLCONNECTED - Occurs when a call enters the CONNECTED state at a device. This can occur after a transfer or after a call is put on hold and the retrieved.

DIVERTED - Occurs when a call moves from one extension to another when following a forwarding path. In this event the Source Extension will be populated.

TRANSFERRED - Occurs when a call is transferred by a user to another destination. Depending on the method of transfer this event may be preceded by a HOLD event and will be followed by a RINGING and / or CONNECTED event. In this event the Source Extension will be populated.

QUEUED - Occurs when a call enters a QUEUING state at a device. This occurs when a call is waiting at a hunt group.

CALLMODIFIED - Occurs when any of the following details of the call have changed: - Account Code - Caller ID - Contact Name

DISCONNECTED - Occurs when a call clears down from the telephone system.

Example Messages

Inbound Call Scenario

2012-03-09 01:20:40 |IN | 20120309012040520702640092108 0001843 0000000 0000079XXXXXXXX |CHRIS R

MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |RINGING |

2012-03-09 01:20:43 |IN | 2012030901204052070264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |ANSWERED |

2012-03-09 01:20:43 |IN | 2012030901204052070264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |CALLMODIFIED|

2012-03-09 01:20:46 |IN | 2012030901204052070264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |DISCONNECTED|

Outbound Call Scenario

2012-03-09 12:46:59 |OUT| 2012030900465982190047 0092808 0001843 0000000 0000079XXXXXXXX | | 000000000000000 000000000000 |RINGING |

2012-03-09 12:47:06 |OUT| 2012030900465982190047 0092808 0001843 0000000 0000079XXXXXXXX | | 000000000000000 000000000000 |ANSWERED |

2012-03-09 12:47:10 |OUT| 2012030900465982190047 0092808 0001843 0000000 0000079XXXXXXXX | | 000000000000000 000000000000 |DISCONNECTED|

Inbound Call Scenario – Call Held Then Retrieved

2012-03-09 01:20:53 |IN | 2012030901205303270264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |RINGING |

2012-03-09 01:20:54 |IN | 2012030901205303270264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |ANSWERED |

2012-03-09 01:20:54 |IN | 2012030901205303270264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |CALLMODIFIED|

2012-03-09 01:20:55 |IN | 2012030901205303270264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |HOLD |

2012-03-09 01:20:58 |IN | 2012030901205303270264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |CONNECTED |

2012-03-09 01:21:00 |IN | 2012030901205303270264 0092108 0001843 0000000 000007968543537 |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |DISCONNECTED|

Inbound Call Scenario – Call Transferred

2012-03-09 01:31:15 |IN | 2012030901311586070264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |RINGING |

2012-03-09 01:31:18 |IN | 2012030901311586070264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |ANSWERED |

2012-03-09 01:31:20 |IN | 2012030901311586070264 0092108 0001843 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |HOLD |

2012-03-09 01:31:27 |IN | 2012030901311586070264 0092108 0002560 0001843 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |TRANSFERRED |

2012-03-09 01:31:27 |IN | 2012030901311586070264 0092108 0002560 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |RINGING |

2012-03-09 01:31:27 |IN | 2012030901311586070264 0092108 0002560 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |CONNECTED |

2012-03-09 01:31:29 |IN | 2012030901311586070264 0092108 0002560 0000000 0000079XXXXXXXX |CHRIS R MOBILE| 00044161XXXXXXX |CHRIS DDI | 000000000000 |DISCONNECTED|

9.1.3 Phone Manager

To use Mitel Phone Manager (desktop or mobile) a user on the system must first have been assigned to a Client Profile. The client profile outlines which license users are entitled to use and which features of the Phone Manager(s) product they can see.

Once a user has been given permission to use Phone Manager, client specific features can be managed through Desktop or Mobile specific sections or through the general configuration sections referenced here:

Feature	Description
Client Profiles	Client profiles are used to control the configuration and features that a client has been assigned.
Client Locations	Presence profiles can be configured by users to control when and how calls alert their extension.
Call Recorder Integration	Configuration into a call recording system to provide features including pause/resume and direct playback.
Certificates	Certificates are used by Phone Manager Desktop & Mobile when connecting to the MCS server.
Telephone Formats	Configures the telephone formats that will be used by Phone Manager to identify phone numbers
Phone Manager Softphone	Outlines configuration options and usage of Phone Manager Desktop & Mobile Softphone.

9.1.3.1 Client Profiles

Overview

Client profiles are used to control the configuration and licensed features that a Phone Manager client user receives.

Performance options are available when running Phone Manager on lower powered computers to improve response times or reduce the processing requirements. This is beneficial in multi user and virtual desktop environments.

Configuration

To add or edit a client profile:

1. Access the '⚙' -> Features -> Phone Manager Desktop -> Client Profiles section.
2. The system will come with several pre-defined client profiles but its possible to create additional profiles that combine license levels with rule flags. Click on *New* to create a new profile or highlight an existing profile and click *Edit* to modify an existing one. The client profile configuration window is then displayed.

Setting	Description	Standard	Outlook	Professional	Team Leader
Name	To describe what this profile is for. (e.g. "Sales Team")	N/A	N/A	N/A	N/A
Description	To provide a more detailed description for this profile. (e.g. "Professional User with Application Support")	N/A	N/A	N/A	N/A
Desktop License	Select the **Desktop License** that will be assigned to clients using this profile. The valid license types are: ◦ **Standard**: This gives the user all the features of Standard client features (Not currently for sale, upgrading customers only). ◦ **Outlook**: This gives the user all the features of Standard plus Microsoft Outlook integration client features. ◦ **Professional**: This gives the user all the features of Outlook plus Professional client features such as CRM screen pop. ◦ **Team Leader**: This gives the user all the features of Professional plus Team Leader client features such as remote control of other users.	N/A	N/A	N/A	N/A
Phone Manager Mobile	When enabled, users connect from a Phone Manager Mobile application and consume a license if available.	N/A	N/A	N/A	N/A
Call Recorder Client	When enabled,the Call Recorder client can be run on a user's desktop. This can then be used to	N/A	N/A	N/A	N/A

	automate the pausing of recordings for compliance purposes.				
Enable Presence Profiles	Enables the user to use Presence Profiles. *Default Enabled*	✗	✓	✓	✓
Disable DEE & UCD when Hot Desk user is logged out	If the user is using Presence Profiles then these feature can be enabled. The features will only apply when the user's Primary Device is a Hot Desk devices.	✗	✓	✓	✓
Enable Chat	Enables the user to access the chat feature in Phone Manager. Without this the chat feature will not be shown (enabled by default).	✓	✓	✓	✓
Make this the default Client Profile	Use this profile as the default when new users are created.	N/A	N/A	N/A	N/A

3. Select the **Settings** tab to configure the options that will be made available to users with this profile. Depending on the type of license selected this will change what options are available.

Setting	Description	Standard	Outlook	Professional	Team Leader
Auto agent login/logout	Logs the agent ID associated with this user into all ACD groups programmed on the PBX when the Phone Manager client starts and out again when it closes.	✗	✗	✓	✓
Auto-answer hunt group calls	This will auto answer hunt group calls (UCD or ACD) for the user after the configured **Answer after** time in seconds, the default it 2 seconds. Phone Manager needs to be running for this to work.	✗	✗	✓	✓
Download Outlook contacts	Makes available the users local	✗	✓	✓	✓

	Microsoft Outlook contacts in their Phone Manager Contacts Directory to enable "Search & Dial" for those contacts. See the Microsoft Outlook Personal Directory section for details.				
Enable ACD control	Enables the user to manage their ACD status from Phone Manager. Without this the ACD control features will not be shown. (The user will still be able to make ACD changes directly on the handset).	✗	✗	✓	✓
Enable DND control	Enables the user to manage their DND status from Phone Manager. Without this the DND control will not be shown.	✗	✓	✓	✓
Enable UCD control	This allows the user control over their UCD state within Phone Manager. This does not prevent them from using the feature code on the handset.	✗	✗	✓	✓
Enable application support	Gives the user the options to configure the Computer Telephony Integration (CTI) plug-ins for the various applications supported, i.e. CRM screen popping, call history and calendar sync to applications such as Salesforce.com,	✗	✓ *	✓	✓

	Microsoft Dynamics CRM and many more.				
Enable macro editing	Gives the user the ability to create and publish VBScript and keystroke macros which provide the user with the possibility to integrate to a range of applications not supported by a dedicated plug-in. The macros created can be "fired" automatically (e.g. when a user answers a call) or assigned to a button on a toolbar so that the users can quickly navigate to a webpage or application if the call requires them to. See the Macros section for details.	✗	✗	✓	✓
Enable TAPI	Allows the user to enable the 1st Party TAPI driver for integration into applications that support TAPI. The **Ignore drop call** option will prevent Phone Manager from clearing the call when the TAPI application sends a clear call command. This is useful for when applications send this command when their own TAPI window is closed by the user. The default is disabled.	✗	✓**	✓	✓

	The **Ignore internal calls** option will prevent Phone Manager from sending information about internal calls to the TAPI application. The default is enabled.				
Enable CPN Substitution	Enables CPN substitution for the calls made by the user from Phone Manager.	✗	✓**	✓	✓

* Only applies to the Outlook Plugin
** TAPI licenses can be enabled when using an Outlook license for backwards compatibility with previous version of Phone Manager. TAPI licenses are currently only provided with Professional & Team Leader licenses only.

4. Select the **Phone Manager Outbound** tab to configure the Phone Manager Outbound specific options. This is only available with a Professional and Team Leader license.

Setting	Description	Standard	Outlook	Professional	Team Leader
Enable Phone Manager Outbound	Enables the user to be able to login to Phone Manager Outbound. The **Open on start up** option will cause Phone Manager to always show the Phone Manager Outbound window when Phone Manager starts, otherwise the user will have to open it manually from the main window icon. The **Can edit campaign records** option allows the user to edit the campaign record information directly within Phone Manager. Without this the *Edit* button is disabled.	✗	✗	✓	✓
Open on startup	This opens the Phone Manager Outbound window within Phone Manager each time the client starts.	✗	✗	✓	✓

	Note: This feature is designed for Phone Manager Outbound only users. Phone Manager will also shutdown if the Phone Manager Outbound window is closed.				
Can edit campaign records	This allows the user to edit Phone Manager Outbound records from Phone Manager Outbound window in Phone Manager.	✗	✗	✓	✓
Enable campaign record search	This allows the user to search for campaign records when taking inbound calls or when idle. Once a record has been found the user can then change the disposition.	✗	✗	✓	✓
Enable manual dialling	This allows the user to manually dial campaign records.	✗	✗	✓	✓
Enable call blending	This enables the user to work in call blending mode, i.e. this allows then to take inbound calls whilst also making automated outbound calls.	✗	✗	✓	✓
Call blending timer	The Call blending timer outlines how long the user will be left in the Free status after their Wrap Up has expired from the previous call.	✗	✗	✓	✓

5. Select the **Advanced** tab to configure the options to allow Phone Manager to run in reduced resource mode.

Setting	Description	Standard	Outlook	Professional	Team Leader
Enable timer columns	This option will enable timer specific columns to be updated at the interval defined in the **Refresh rate** field. This causes the columns such as "Time in status" or "Talk time" to automatically update their values. The default is enabled and refreshed every 5 seconds. With this disabled then timer columns will not update automatically and this will reduce the amount of resources required.	✔	✔	✔	✔

6. Click *Save*.

> Phone Manager Mobile can be used on it's own or in conjunction with any other Phone Manager Desktop license. 'enable Presence Profiles' must be enabled for users using Phone Manager Mobile.

9.1.3.2 Presence Profiles

Overview

Presence Profiles provide a method for users to control how they receive communications as well as inform internal users about their current availability. Presence Profiles is the default method for users to control their extension and is a requirement if they wish to use Phone Manager Mobile.

To use Presence Profiles, the user's Primary Extension **MUST** be a Dynamic Extension Express main device on the telephone system.

Presence Profiles control the following aspects of a user's Primary Extension's status:

- **Do Not Disturb:** Controls whether DND is enabled or not, which message is displayed and any additional text.
- **Forwarding:** Controls whether the user is forwarding all calls to another location or not
- **Dynamic Extension Express:** Controls which of the user's DEE devices are active
- **UCD Hunt Group Availability:** Controls the remove/replace feature of UCD *

(* Note: When users remove their extension from a UCD group with a profile they will also disable any group call pickups.)

To enable Presence Profiles for a user, edit their Client Profile and check the Enable Presence Profiles box.

Default Profiles

Each user is a given a default set of profiles that they can edit/delete or add to as they require:

In the office	Default profile, enables all of a user's DEE destinations, no DND, no Forwarding, Group Calls (UCD) enabled
Do Not Disturb	All DEE destinations enabled, DND set to on, prompt on selection. no Forwarding, Group Calls (UCD) disabled
Out of the office	External DEE destinations enabled only, no DND, no Forwarding, Group Calls (UCD) disabled
In a meeting	Only Voicemail DEE destination enabled, DND on, no Forwarding, Group Calls (UCD) disabled
Working from home	Only Voicemail DEE destination enabled, DND off, Forward Immediate with prompt for the destination, Group Calls (UCD) disabled
On holiday	Only Voicemail DEE destination enabled, DND on, no Forwarding, Group Calls (UCD) disabled

A user can delete any profile apart from the one they currently have selected. Any changes to a profile will have immediate effect if the profile is currently selected.

When are Presence Profiles Applied?

All profiles are implemented by the CTI Host Service. Changes are made when:

- the CTI Host Service starts up
- a user requests a profile change (from Phone Manager Desktop or Phone Manager Mobile)

- Phone Manager connects to or disconnects from an extension which is not the user's Primary Extension (see >What are Presence Profiles Applied to? section below)
- a user's Primary Device is also a Hot Desk device and they login/logout (see Hot Desking section below)

If the status of a device changes outside of these events then the change will stick until one of the event next occurs. For example, if a user manually puts their extension in DND then the change will be kept. This is important so that the server is not overwriting manual changes made by the user on their extension.

If at anytime the status of the extension does not match the current profile then the user will be alerted in Phone Manager.

What are Presence Profiles Applied to?

Presence Profiles are applied to the following devices:

- a user's Primary Extension
- any extension the user's Phone Manager client is connected to (This applies to DND, UCD & FWD properties only, no DEE changes will be applied to extensions other than the user's Primary one)

For example, if a user's Primary Extension is 1000 and they currently have Phone Manager connected to their softphone 1001 then their current profile will be applied to both of these extensions. If they shut down Phone Manager then any profile change will be removed from 1001 and left only on 1000.

Hot Desking & Presence Profiles

When a user's DEE main extension is also a Hot Desk device there are some extra checks MCS performs when applying profiles. If the 'Disable DEE & UCD when Hot Desk user is logged out' option is checked on the user's Client Profile then the CTI host service will remove the main device from any UCD groups and make it inactive as a DEE device if it is currently logged out. If the Hot Desk device is logged in, the CTI host service will re-apply the profile and re-enable UCD and make DEE active for that device again if applicable.

> When using Presence Profiles, DEE must also be used. Be aware that this can cause reporting issues on sites using MiCC Office (CSM) due the restrictions on DEE based reporting within the product.

> For more information about editing Presence Profiles, please refer to the Phone Manager Desktop Help.

9.1.3.3 Call Recorder Integration

Overview

Phone Manager can integrate into external call recording systems. This can provide the following features:

- Pause and resuming call recording for specific calls.
- Tagging call recordings with custom information.
- Playing call recordings directly back from within the Phone Manager client.

> The features available are dependent on the type of call recorder to be integrated with. Currently only Xarios Call Recorder is supported as an external solution. All of these features are supported with the MiVoice Office Call Recorder.

Configuration

To enable external call recording integration:

1. Access the Features -> Phone Manager Desktop -> Call Recorder Integration section.
2. Check the **Use external Call Recorder connection** check box.
3. Enter the hostname or IP address of the call recording system into the **Call Recorder hostname / IP address** field.
4. Click *Save*.

> When enabling Call Recorder Integration ensure that the Communications Gateway services have been configured to run against the server within both the MCS and Call Recorder websites.

9.1.3.4 Telephone Formats

Overview

The Telephone Formats section is used with the Phone Manager application support plugins to control the range of telephone number formats that are used when searching CRM applications. Often the CRM application that is being integrated with does not store the telephone number in a consistent format. For example there may be the following records:

Name: "John Smith"

Telephone: "+44 (123) 456 7899"

Name: Jane Doe

Telephone: "0123 45 6789"

To be able to try and match a contact record that has these telephone numbers then the exact format may have to be used when performing the search, including any non numeric characters, i.e. plus signs, brackets or spaces, or even toll digits.

From this section specific formats can be added in the form of regular expressions.

See http://en.wikipedia.org/wiki/Regular_expression for more information on regular expressions (external link).

The following formats are configured by default.

UK & International Telephone Formats			
08001831234	(0123) 4567890	44 (08001)831234	+44 (080)0183 1234
08001 831234	08001-831234	(08001)831234	(08001)-831234
080 018 31234	080-018-31234	080 0183 1234	080-0183-1234

The default formats for the US are shown below. This is based on the number 9876543210 been searched for.

US Telephone Formats			
9876543210	987.654.3210	+1 (987) 654-3210	19876543210
987-654-3210	(987) 654-3210	1-987.654.3210	1-987-654-3210
1(987) 654-3210	(987)654-3210	(987) 654-3210	

9.1.3.5 Phone Manager Softphone

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

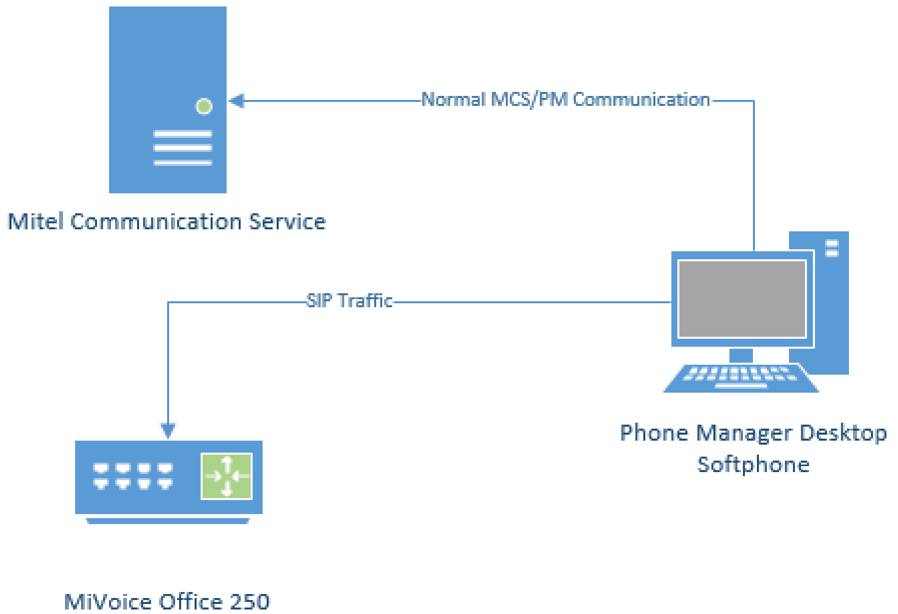
Requirements

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

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

Phone Manager Desktop with Softphone

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



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

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

Connecting from a Different Subnet

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

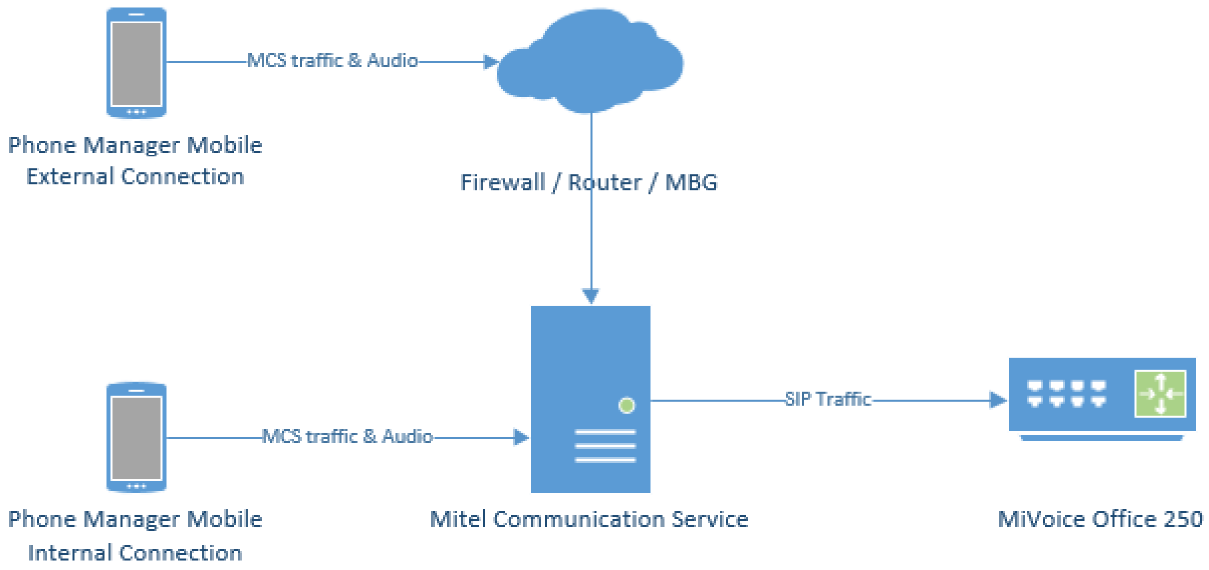
To work around this issue, Auto NAT Detection needs to be disabled on Phone Manager Desktop.

Phone Manager Mobile with Softphone

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

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

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



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

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

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

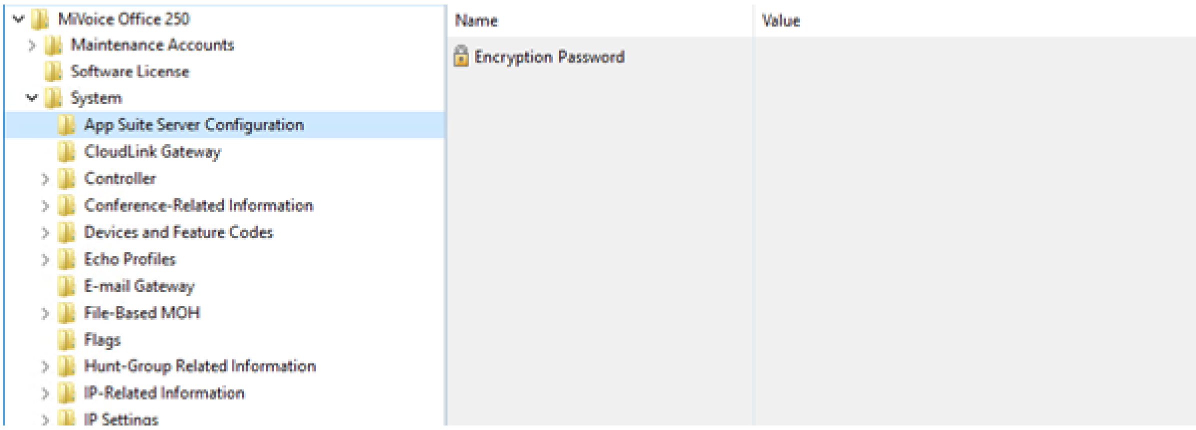
> ⚠ The SIP Proxy service must be on the same network as the PBX with no NAT in between the two.

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

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

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

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



Encryption Password

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

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

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

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

Node Configuration for SIP

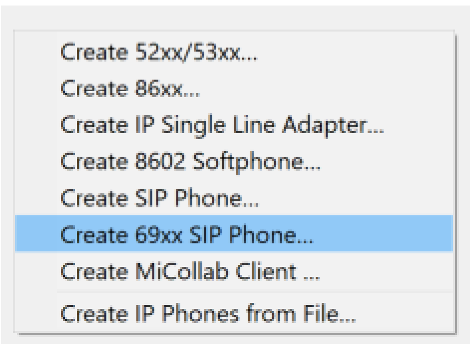
The MCS server needs to provide each 6900 phone and Phone Manager Softphone with the IP address of a SIP server to register with (the MiVoice Office 250). The IP address required will depend on which MiVoice Office 250 node the SIP extension is configured on and whether the phone is local or a teleworker.

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

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

69xx SIP Phone

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

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

SIP Phone Group

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

- Maximum Number of Calls = 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.

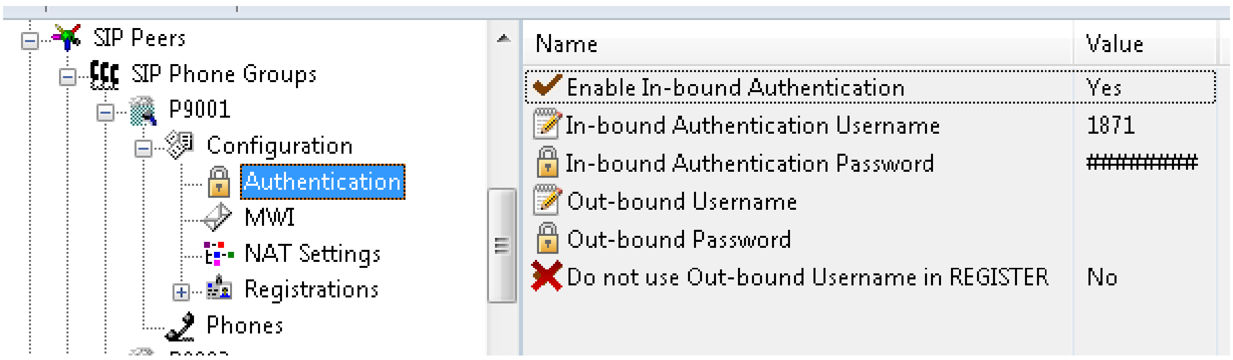
Manual Authentication Configuration

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

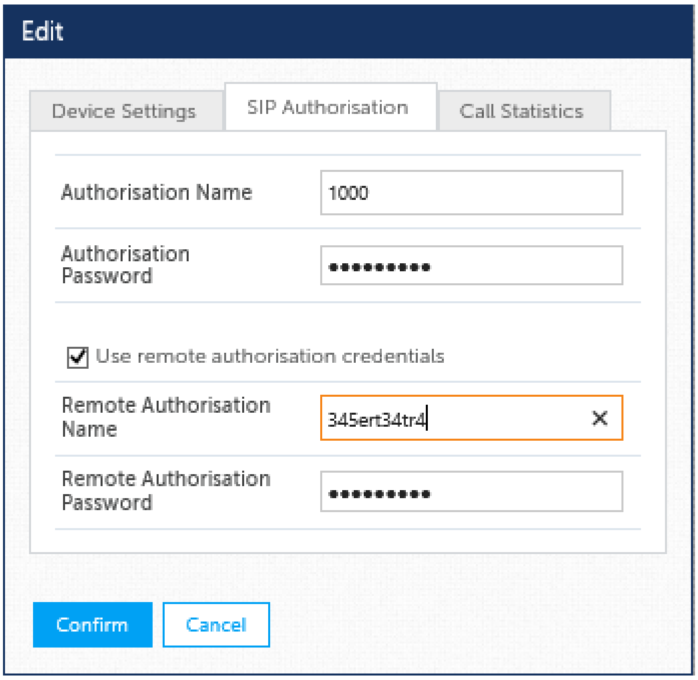
> If release 6.3 SP1 or higher is being used, check the App Suite Server Configuration section below.

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

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



This same username and password combination would then need to be set on the device configuration on the Communication Service for this extension.



For information on configuring Teleworker phones, please refer to the Remote Connections engineering guidelines.

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

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

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

Call Configuration

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

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

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

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

> It is important to connect only one softphone to each extension number on the telephone systems. Registering more 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.

9.1.3.6 Phone Manager Desktop

Overview

This section enables the configuration of Phone Manager Desktop client specific features to be managed. This includes:

Feature	Description
Macros	Client macros enable a custom VBScript macro to be assigned to a User that will be triggered on a specific call event or manually by the user.
Call Banner Profiles	Banner profiles control how the Phone Manager toaster popup is displayed when calls are received at the client.
Client Toolbars	Client toolbars are used to create and assign toolbars and buttons that are available for a User to perform common actions.
Meet-Me Conferencing	Configures the text field used by the Phone Manager Outlook integration feature for creating a calendar entry containing details of a user's Meet-Me conference settings.

9.1.3.6.1 Desktop Client Requirements

Phone Manager / Call Recorder Client 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 R2 Standard/Enterprise/Datacenter 32-bit/64-bit
- Windows 2012 R2 Standard/Datacenter 64-bit
- Windows 2016 Standard/Datacenter 64-bit

> Windows Server Core installations are not supported.
>
> Windows Server Small Business/Foundation/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 4.5.2

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.

9.1.3.6.2 Macros

Overview

Client macros enable a custom VBScript macro to be assigned to a User that will be triggered on a specific call event or manually by the User. For example, to screen pop a CRM application with the customer record when the Phone Manager user answers the call.

Users who have **Enable Application Support** can run macros that have been assigned to them and can set the rules for when a macro would "fire". Users who have the **Enable Macro Editing** option set on their Client Profiles are able to create and edit macros from Phone Manager.

This means that they have the Phone Manager client Macro option visible in the Settings area in Phone Manager and can create and publish macros to the server. Once a macro has been published by a Phone Manager user it is visible on the server and it can then be assigned to those users who have the **Enable Application Support** option assigned to their Client Profiles.

> For more detailed information on creating and publishing macros, see the **Phone Manager client help file** and the **Phone Manager API Reference**.

Assigning Macro Users

To assign or remove a macro to a User:

1. Access the '' -> Features -> Phone Manager Desktop -> Macros section
2. Select the published macro and click on *Edit*.
3. To assign a macro click on *Add* to search for Users to assign.
4. To remove a User from a macro assignment select the existing User and click *Remove.*

9.1.3.6.3 Call Banner Profiles

Overview

Call Banner profiles control the look and feel of Phone Manager Desktop's call banner (which is a toaster popup). This is displayed when calls are received/made at the extension associated to the Phone Manager client. The objective is to better inform a user about the nature of the call they are receiving and display customer data when the call rings, without taking PC focus away from the application the user is running.

Each banner profile is a combination of the following:

- Properties, Items on the call banner that will be changed
- Condition, Controls when the profile is applied to a call banner
- Priority, Controls which banners have priority over other banners

Properties

Each banner profile can be used to change one or more of the following call banner properties:

Fields

Each call banner can contain up to 10 fields of information. To change the fields displayed using a profile, check the 'Set fields' box and then use the plus icon (+) to add the required fields.

Title Bar / Text

To help the user identify specific types of call, the text and/or colour of the call banner's title bar can be modified. To change either of these properties, check the 'Set title bar text' or 'Set title bar colour' options and then enter the required information.

Header Text

The header text is the main piece of information on the call banner. This displays either the telephone number of the call or the contact name if there is a match. the profile can be used to alter the colour the header text is displayed in if required.

Conditions

The conditions configured against a call banner profile control when the profile is applied to a call banner.

The conditions that can be applied to a profile can be simple or complex to meet requirements. Any number of individual conditions can be grouped together and applied using 'All/None/Any' operators.

Individual Conditions

Each condition added to a profile's conditions has three constituent parts:

- Call Data Field, the call data field to be searched (Account Code in the image above)
- Search Value, the value to look for in the call data field (123 in the image above)
- Comparison Type, how the call data field and the search value should be compared (= in the image

above)

Each of these values can be changed by left-clicking on them with the mouse and then selecting a value from the context menu that appears.

The table below outlines the comparison types available and gives examples of how to use each one.

Comparison Type	Description	Example
=	Equals	DDI = 01617864350
≠	Not Equals	DDI ≠ 01617864350
<	Less Than	Account Code < 20
>	Greater Than	Account Code > 19
like	Like	DDI Like 0161
≤	Less than or equal	Account Code ≤ 19
≥	Greater than or equal	Account Code ≥ 20
in	In, used for matching multiple items	DDI in 01617864350,01617864351,01617864352
notin	Not In, used to negatively match against multiple items	DDI notin 01617864350,01617864351,01617864352

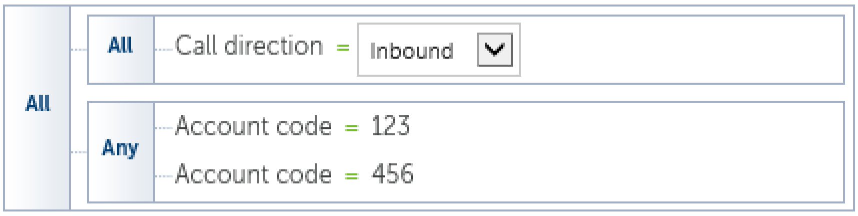
Multiple Conditions

Multiple conditions can be added to a single profile to ensure that it only gets applied based on specific scenarios. This can be useful if multiple call data fields need to be searched or if multiple values with in a single call data field need to be matched.

Each condition added can be grouped together with and operator of Any, All or None.

The image below shows an example of how multiple conditions can be grouped together. In the example, the call banner profile will only be applied if the call direction is inbound, and the account equals either 123 or 456.

Note how the operator on the group containing the account code conditions has been changed to 'Any' which means the account code can be either 123 or 456. Similarly, note how the parent group's condition is set to 'All' which means both the account code group and the call direction group must be valid.



Groups can be added/edited and operators can be changed by left-clicking on the with the mouse and selecting the relevant option from the context menu that appears.

To help create complicated conditions, they can be dragged and dropped between groups using the mouse.

For an example of how to configure call banner profiles see:

- Banner Profiles VIP

Matches On Multiple Profiles

When evaluating which call banner profiles to apply, multiple profiles may get a valid match against a call' data fields. When this happens the priority of the call banner profile comes into play. The properties of each matching call banner profile will be merged together and when two or more profiles are set to change the same property, the one with the highest priority wins.

For example, if a call gets a match on two profiles and they are both configured to change the title bar colour, the colour used will be that if the call banner profile with the highest priority (priority 1 overrides priority 5). If how ever one profile is set to change the title bar colour and the other changes the title bar text, both changes will take effect.

Default Call Banner

The properties of the default call banner profile will be applied to all calls. If there are no other profile matches for a call or if the other matches don't change some of the properties available, the properties configured against the default profile will take effect.

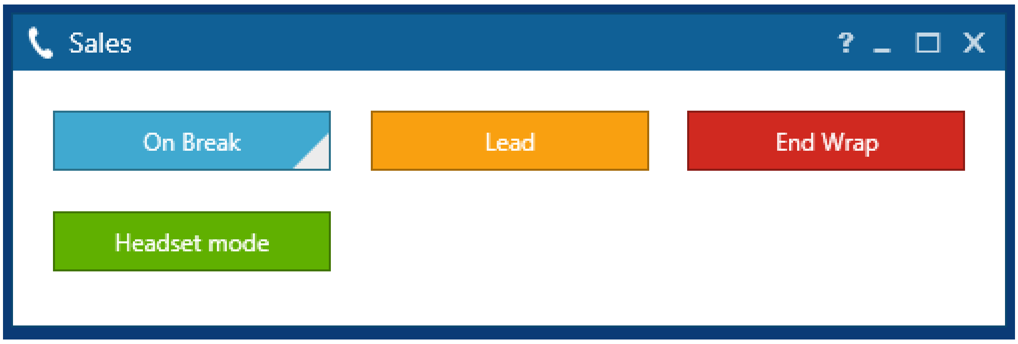
9.1.3.6.4 Client Toolbars

Overview

Client toolbars are used to create and assign toolbars to Phone Manager Desktop client users. These toolbars can be configured with the following items:

- Buttons -> Configurable buttons that are available to perform predefined common actions such as PBX features or speed dials.
- Wallboard Tiles -> Displays Agent based statistics about the currently logged in agent.

Multiple toolbars can be created with varying amounts of buttons, a button can have custom labels and colours to highlight or categorise specific types of actions, for example:



If a user has any toolbars assigned then they can open them using the toolbar icon from the main window in Phone Manager. If they have more than one toolbar assigned then a drop down window will be displayed when the click the button and they can select the toolbar to open.

> If there are no toolbars assigned to a user then the toolbar icon will not be visible in Phone Manager.

Licensing

There are multiple licenses on the system that control the functionality available on a toolbar.

Toolbar Access (Phone Manager Desktop Professional / Team Leader)

To have access to use a toolbar, the user must have either a Phone Manager Professional or Team Leader license. Toolbars are not available to Phone Manager Outlook (or standard) users.

Personal Wallboard Access (ACD Reporting Licenses)

In addition to the requirement of running a Phone Manager Professional or Team Leader license, to view wallboard tiles configured on a toolbar, the user must have an ACD Reporting license.

Editing a Toolbar

To create or edit a toolbar:

1. Access the '⚙' -> Features -> Phone Manager -> Client Toolbars section.
2. Click on *New* or select the toolbar and click *Edit.*
3. Select the **Details** tab.
4. Enter a **Name** that is used to identify this toolbar to the Phone Manager users.

5. Enter a **Description** to detail what this toolbar is for
6. Modify the Buttons and/or Wallboard tiles as required.
7. Select the **Users** tab and click *Add* (this will display the Business Units view). Select individual users that will have access to this toolbar.

   > Hold down the CTRL key to select multiple individuals.

8. Click *Add*
9. Then click on *Save* to complete the process.

> When a toolbar has been assigned to a user Phone Manager will require a restart for the changes to take effect. If changes have been made to an existing toolbar that is already assigned to a user then simply closing and re-opening the toolbar will apply the changes.

Toolbar Details

The following options are available for each toolbar:

Layout Style

Defines in which order the toolbar should display buttons/wallboard tiles or whether it will only display one or the other.

Always on Top

Controls whether the toolbar should display on top of other windows. This is a useful setting when the toolbar is not being docked. If not configured centrally, the user can configure this locally on the client.

Docking

Defines whether the toolbar should dock to the primary screen. If not configured centrally, the user can configure this locally on the client.

Editing Toolbar Buttons

If the layout of a toolbar has been selected to include buttons, the 'Buttons' tab will be available.

The '+' icon underneath the list box on the left hand side can be used to add a button to the toolbar. To edit an existing button, left-click on the button in the list on the left then press the 'Edit' button in the details pane on the right.

Each button added has the following options:

Label

This will be displayed on the button to inform the user what action the button performs.

Action

Selection an action for the button to perform from the available list. For a list of available actions, please refer to the Button Actions section.

Background Colour

Select the colour that will be used for the button's background.

Text Colour

Select the colour that will be used for the button's label.

Once the button has been configured, the 'Save' button can be used to apply it to the toolbar. Repeat the steps above for all buttons required.

Other options:

'x' - Delete a button from the toolbar.

'^' - Re-order buttons

Up to 30 different buttons can be added to a toolbar.

Editing Wallboard Tiles

If the layout of a toolbar has been selected to include statistics, the 'Wallboard' tab will be available.

The '+' icon underneath the list box on the left side can be used to add a tile to the toolbar. To edit an existing tile, left-click on the tile in the list on the left then press the 'Edit' button in the details pane on the right.

Each tile added has the following options:

Label

This will be displayed on the tile to inform the user what statistic is displayed on the tile. The label is automatically set when the statistic field is selected.

Statistics Field

Select the statistic field to be displayed on the tile from the available list. The following statistic types can be added to a personal wallboard tile:

- Any statistic that can be added to an Agent Grid
- External Data Source statistics
- Global Variable statistics

For information on the available statistics, please refer to the Statistics section.

Background Colour

Select the colour that will be used for the tile's background.

Text Colour

Select the colour that will be used for the tile's text.

Once the tile has been configured, the 'Save' tile can be used to apply it to the toolbar. Repeat the steps above for all tiles required.

Other options:

'x' - Delete a tile from the toolbar.

'^' - Re-order tiles

Wallboard Tile Alarms

Where the statistic is displaying a numerical value, one or more alarms can be configured on a tile to perform one of the following actions:

- Flash the tile
- Change the background colour
- Change the text colour

Each alarm configured has the following options:

Operator

Select how the statistic will be evaluated against the value provided, greater than (>), less then (<), equal to (=) or between.

Value

The value against which the alarm will compare the statistic currently displaying on the tile.

Actions

One or more actions that should be performed if the statistic matches the configured alarm's settings.

9.1.3.6.4.1 Button Actions

Overview

Both the centrally configured Client Toolbars buttons and the five user programmable buttons that come with the Softphone and Professional license (or above) can be configured to perform a range of features and functions.

Several of these buttons have pre-loaded actions that require certain parameters to be set for them to work.

Depending on which action is selected when adding the button, different parameters will be shown. Below is an outline of what each button will do and what parameters are required to be set.

Actions

Action	Description
ACD end wrap	This button will terminate Wrap Up for a user and functions in the same way as ACD Agent Wrap Up Terminate (Default feature code 329).
ACD status	The ACD Status button can be used to log the users associated ACD Agent ID in or out. The parameter that can be set for this button is a specified hunt group or groups. When Hunt groups are specified this functions the same way as ACD Agent Login/out (Default feature codes 326/327 on the PBX. If this parameter is left blank then the button will be used in the same way as ACD Agent Toggle (Default feature code 328) and will log the Agent ID in or out of ALL groups configured on the PBX.
Add call history	Used to create a call history record using a supported plugin for a third-party CRM.
Agent Help	Used to invoke the Agent Help feature on the telephone system. Use of this softkey requires the necessary PBX configuration to have been performed.
Answer call	This feature will simply answer a ringing call at the extension.
Change caller ID	Also referred to as the Calling Party Number (CPN), the Caller ID (CLI) is the number presented by the PBX when making an outside call. This number is usually configured in Mitel Database Programming against the extension associated with the user. With this feature it is possible to use a single button click to re-program that number via the server. Once set, the new CLI/CPN will remain in place until either re-programmed in DB Programming or if an additional button with a different CLI/CPN is clicked. This feature is limited to the scope of CLI/CPN numbers permitted by the Trunk network provider and if limited, it typically means limited to the range of DDI numbers configured on the PBX.
Change volume	This will increase or decrease the volume level for whichever state the extension is in at time the button is used. e.g. if the extension is idle it will change the ringing volume, if the user is connected to a call using a headset it will change the headset volume etc.
Clear call	This feature will simply hang up a connected call
Dial digits	This feature will simply dial the string of digits configured in the "Digits to

	send" field. If prefixed with the outside number digit and the extension is idle, it will make a call to the remainder of the digits. If already on a call it will send the digits as DTMF tones over the call.
Do not disturb (DND)	The Do Not Disturb button can be used to place the extension into DND. If the extension is already in DND it will remove it. Select one of the 20 pre-configured DND messages from the drop down menu and then set additional Message text if required. Multiple DND buttons can be created so setting specific DND states is a one click function.
DSS/BLF	The Create a DSS/BLF button for any extension hunt group, user or agent id on the system.
Feature code	The server will download a list of all the feature codes configured in the PBX and will make them available for selection from the drop down menu. Where applicable the additional parameters associated with the feature can be set. Remember that certain features are only possible if permitted in Mitel Database Programming PBX
Headset mode	This feature works in the same way as Headset on/off on the PBX (Default feature code 317).
Hold	This features works the same way as System Hold on the PBX (Default feature code 335).
Make call	This feature will make a call to the number configured in the Number to dial field. It differs from the "Dial Digits" feature in that if on an existing call, it will make an additional call whereas Dial Digits will send DTMF digits over the existing call.
Park Call Toggle	Create a key to park/pickup calls from a hunt group or phantom on the telephone system.
Pause / resume recording	If the system is integrated to an external Call Recording system, this feature will toggle between pause and resume the recording and can be used for PCI compliance purposes. This requires Call Recorder Integration and may not be supported by all recording solutions
Play prompt	This feature will automatically conference the call currently in progress to an external IVR so that the process of playing a script to a customer can be automated.
Record current call	This works the same way as the Record-A-Call feature and will create a voicemail message recording of the call in the specified mailbox. Remember that the extension needs to have the Record-A-Call application configured DB Programming on the PBX and the "User Keyed" flag needs to be set.
Redial	This feature will redial the last connected outside call. Remember that Phone Manager client software contains a call list of the last 1000 calls made and received with a one click dial button on the form.
Retrieve	The retrieve call button is used to retrieve a call that has been placed on hold at the extension. No parameters are required to be set for this button.

Run executable	This feature will run any program in Windows that can be called from the "Run" command line. e.g. to start Internet Explorer and go the Mitel home page, enter "iexplore" in the Exe path field and "www.mitel.com" in the command parameters field.
Run macro	With the Phone Manager Professional license, Once a macro has been published and assigned to a user, this feature will allow the user to "fire" the macro by clicking the button. As with the *Run Executable* feature, this can be useful when during a call the user needs to automatically store a pre-defined string of text in a field or to send a keystroke string into a given application to speed up the workflow
Screen-pop application	With the Phone Manager Professional license, this feature can be used to screen pop one of the many CRM applications where the integration is embedded in the corresponding Phone Manager plug-in. Supported CRM applications include Goldmine, ACT, Sage CRM, Salesforce.com, Microsoft Dynamics CRM, Tigerpaw, ZoHo, Sugar CRM etc.
Send to Voicemail	This feature will send a ringing call to the Voicemail application configured against the extension in Mitel Database Programming for users with a mailbox.
Set account code	This feature will set the Account Code - Optional feature (default feature code 390) with the configured account code. There are a maximum of 12 digits available and if no code is configured a blank field will pop up to enable the user to set a variable code on the call.
Set account code on monitor	If the user has the permission to silent monitor another extension, this feature will set the Account Code on the call being monitored.
Tag call	This feature will modify the display of the current call with the text in the Tag field. If no text is defined a blank field will pop up to enable the user to Tag the display with free text (up to 16 characters). This is useful when an operator tags the call with "Mr Jones" before a blind transfer to an extension. If the call returns to the operator unanswered, the display will indicate the caller's name and the operator can greet the returned call in a more professional way.
Tag recording	This will tag one of the custom tag field on the call recording record with the given value. This requires Call Recorder Integration and may not be supported by all recording solutions.
Toggle Macro Events	This will make a one step blind transfer to the destination specified in the Transfer target field.
Transfer	This will make a one step blind transfer to the destination specified in the Transfer target field.

9.1.3.6.5 Meet-Me Conferencing

Overview

Phone Manager contains integration to the Microsoft® Outlook calendar including a Meet-Me conference button that automatically creates an Microsoft® Outlook appointment with the users Meet-Me Conference details pre-populated.

The Meet-Me Conference feature is built into the PBX and permits Mitel users to create an audio conference bridge each with their own conference ID. The PBX installer then assigns an internal extension and external DDI number to access the bridge.

Configuration

To configure the template:

1. Access the Features -> Phone Manager Desktop -> Meet-Me Conferencing section.
2. In the **Appointment email template** box enter the internal extension and external DDI/DID number that routes to the conference assistant. In Users & Business Units, each user profile can be configured with a users Meet-Me conference ID and the @ACCESSCODE placeholder will automatically be replaced with this.

   Example Template

   ```
   To join the Mitel Meet-Me audio conference, please dial one of the numbers below
   and enter the access code:

   Internal: tel://1300
   External: tel://

   Access Code: @ACCESSCODE
   ```

   > If the telephone numbers in the template have the "tel://" prefix this will allow a Phone Manager user to just click the link at the time of the appointment and Phone Manager will dial the number automatically.

3. Click *Save*.

9.1.3.6.6 Software Deployment

To help with Phone Manager Desktop client deployments, 32bit and 64bit client installations can be uploaded to the server. Once uploaded, an invitation email can be sent to users on the system explaining how to install the software.

> For users to be able to install Phone Manager themselves, they require administrator permissions on their local computer.

Current Installation Files

A single version of Phone Manager Desktop software can be uploaded to the server at a time. Both 32bit and 64bit versions of the client installation are required.

To upload installation files, press the 'Browse' button and select the required file.

> Client installation files have to be manually uploaded and are not included with the server installation.

Invitation Email

The invitation email can be used to send installation instructions to new Phone Manager Desktop users. The email template can be modified as required and tailored to a specific environment.

The '[ADMINISTRATOR EMAIL]' section of the template should be replaced with the email address of someone who can provide help if users have problems during installation.

Dynamic Fields

The following fields should be left within the template at all times, they will be replaced by the system when the invitation email is sent:

- @USERNAME -> This will be replaced with the specific user's username
- @SERVER_IP_ADDRESS -> This will be replaced with the IP address/Hostname of the server configured in the Client Location section
- @INSTALL -> This will be replaced with a download link to the Phone Manager Desktop installation file

Sending Invitation Emails

To send the invitation email, press the 'Send Invitation' button. Choose from one of the following options:

- All Users -> Sends the invitation to all users on the system
- New Users -> Sends the invitation to all users who have never connected to the server with Phone Manager Desktop
- Custom -> Allows the manual selection of which users to send the invitation email to

9.1.3.6.7 Phone Manager Installation

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.

> ⚠ From release 5.0.12 of Phone Manager a new version of the Plantronics API is used for headset support. If you have previously deployed Phone Manager with Plantronics headset support then the Plantronics Spokes software must be uninstalled before upgrading Phone Manager.

> 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.

9.1.3.6.8 Unattended Installations

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 customise 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	User of Agent Hot Desking or

	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.	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 Manager starts up.	Users of Terminal Services or 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

9.1.3.7 Mobile Overview

Phone Manager Mobile provides many of the features of Phone Manager Desktop but for iOS and Android devices. Phone Manager Mobile can work on it's own or in conjunction with Phone Manager Desktop.

Features

Phone Manager Mobile offers the following features:

- Access to Favourites and Phone Manager Contacts including status visibility
- Control of Presence Status
- Access to their Call History
- Chat capability with other Phone Manager users
- Notifications of Missed Calls, Voicemails, Chat Messages and Call Routing
- A built in Softphone for remote working

Licensing

Phone Manager Mobile licensing works differently to Phone Manager Desktop licensing:

- Phone Manager Desktop - > **Concurrent** licensing, licenses are only consumed when users have Phone Manager Desktop connected to the MCS.
- Phone Manager Mobile -> **Persistent** licensing, licenses are consumed when a user first connects a Phone Manager Mobile client and are only released:
  - The user is deleted
  - The Phone Manager Mobile license permission is removed from the user's Client Profile
  - The user's license is revoked from the Mobile Clients page

Persistent licensing is used on Phone Manager Mobile because it does not have a permanent connection to the MCS. The mobile client only connects to the MCS when it needs an update/information.

A license is consumed for every device Phone Manager Mobile is installed on. If a user has Phone Manager Mobile installed on more than one device then they will consume more than one license.

> For details on supported operating systems and devices follow the link here.

9.1.3.7.1 Mobile Client Requirements

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

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

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

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

9.1.3.7.2 Mobile Clients

The Mobile Clients screen provides a way to manage Phone Manager Mobile users. The grid in the centre of the screen displays information about Phone Manager Mobile users, it can be filtered using the radio buttons at the top.

Filtering

Depending on the filter chosen, the Mobile Clients Grid will change to show users/sessions that match the filter:

- ***Users currently using a license*** -> Shows all the users that currently have a Phone Manager Mobile 'Session'. Each session represents a consumed license. If a users has more than one session (they are using the application on multiple devices) then they will be consuming more than one license
- ***All users allowed a license*** -> Shows all users that are allowed to request a license based on their Client Profile's settings
- ***Users never invited*** -> Shows all users that have not been sent an invitation email
- ***Users never connected*** -> Shows all users that are allowed to request a license but are not currently consuming one

Mobile Clients Grid

The following columns appear for each Phone Manager Mobile session:

User: The name of the user using Phone Manager Mobile session.

Device Model: Where possible this will store the hardware model of the device they are using.

OS Version: Where possible this will store the operating system version number the device is using.

Client Version: This shows the version number of the Phone Manager Mobile software that they have installed.

Last Connected: This shows the last time the application connected to the MCS server.

Diagnostics: Enables/disables diagnostic logging on the user's device. This will take effect the next time the user connects to the MCS.

Delete User Session: Pressing the cross icon against a user removes their current session and releases the license they are using. To stop the user opening another session remove the Phone Manager mobile license from their Client Profile.

> Deleting a user's session will stop them receiving notifications and will stop their softphone operating if they have one.

> The information shown in this view is valid as of the last time the user had a successful connection to the MCS. If they currently cannot connect then the information may be out of date.

Invitation Emails

Next to each user is a link to send them an Invitation Email. This can also be done to all users shown by the filter by pressing the 'Send Invitation to All' button to the top right of the grid.

Before sending invitation emails out check the email template first.

9.1.3.7.3 Mobile Client Installation

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

Server Side Configuration

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

MCS & PBX Configuration

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

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

For more information about why these configuration steps are needed please review the Phone Manager Mobile section.

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

Network Configuration

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

MCS Certificate Configuration

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

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

Mobile Client Installation

To install the Phone Manager Mobile client application please follow one of the platform specific guides:

- iOS Installation

- Android Installation

9.1.3.7.3.1 Mobile iOS Installation

iOS Installation

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

Installation Requirements

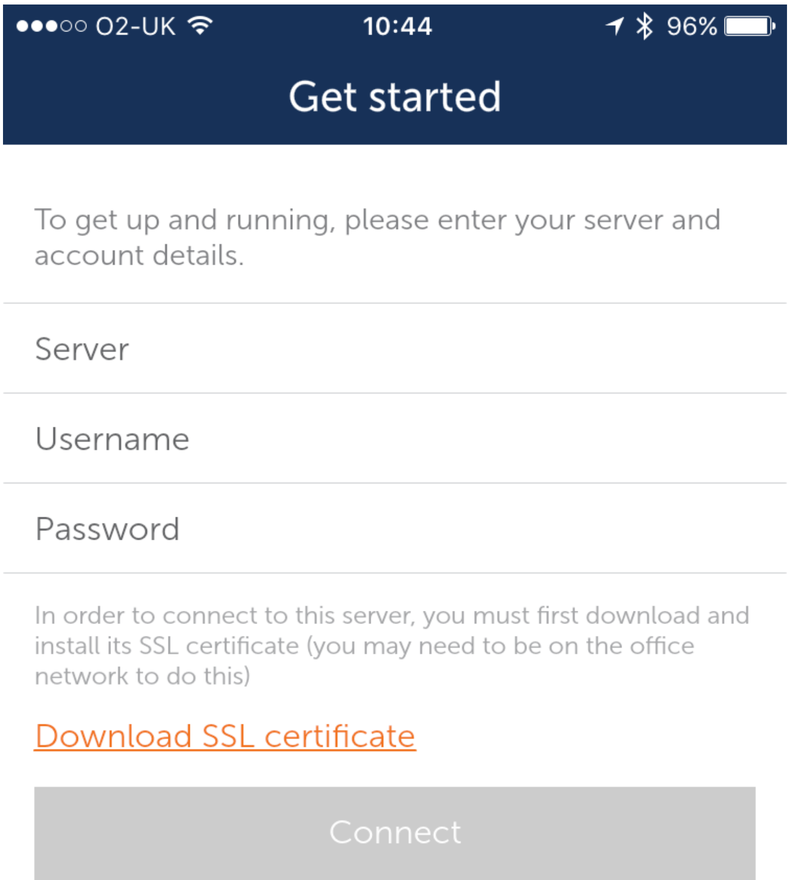
End-users will need the following information in their possession before they start the mobile client installation:

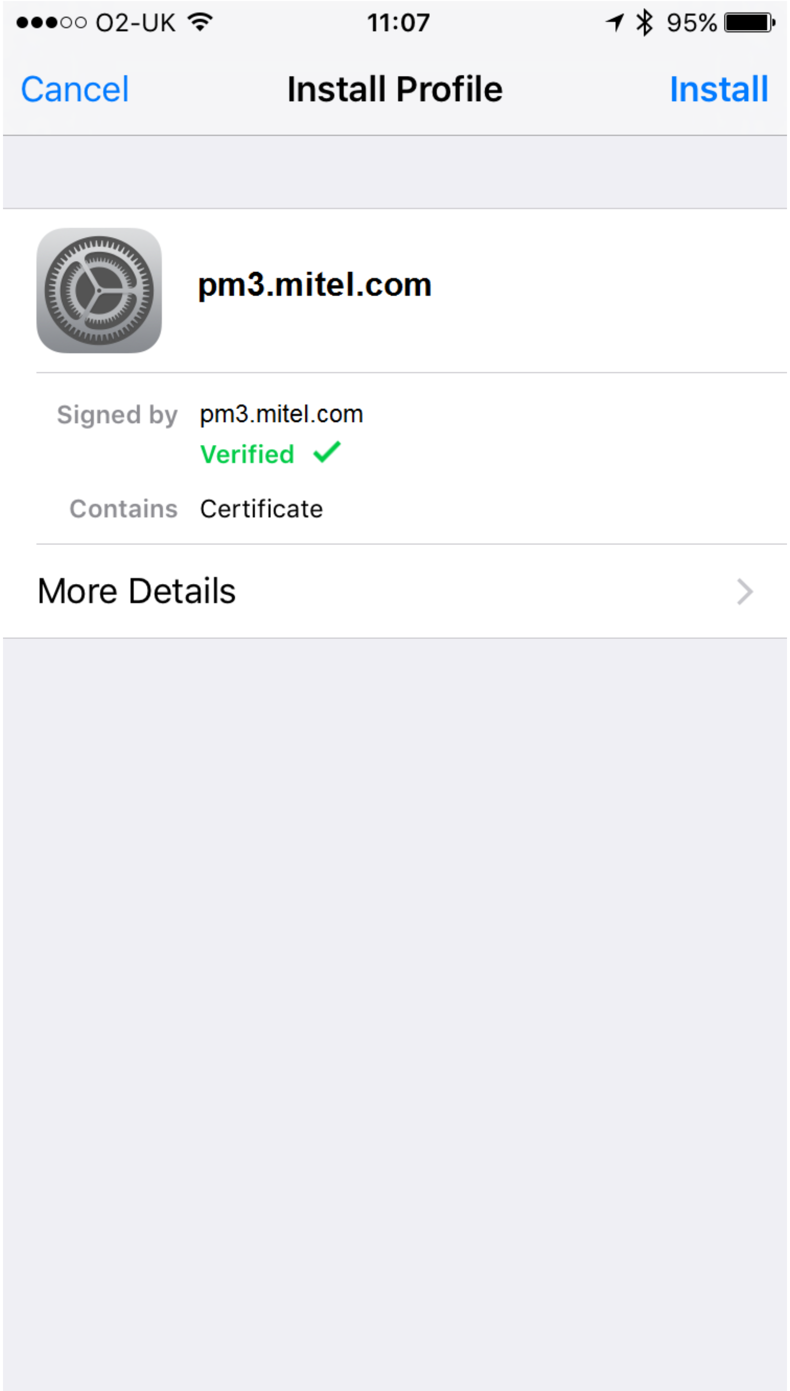
- Their username and password for accessing MCS. This may be their Domain user account (in format DOMAIN\username) or an MCS username and password.
- A valid network on their iOS device, Ideally they will be on the same network as the MCS Server.
- The IP address / Hostname of the MCS server. If connected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

Installation Steps

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

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


O2-UK
10:44
96%
Get started
To get up and running, please enter your server and account details.
Server
Username
Password
In order to connect to this server, you must first download and install its SSL certificate (you may need to be on the office network to do this)
Download SSL certificate
Connect



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

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

Troubleshooting

If the user has problems:

- They have not installed the self-signed certificate

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

iOS 10.3 Onwards

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

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

9.1.3.7.3.2 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

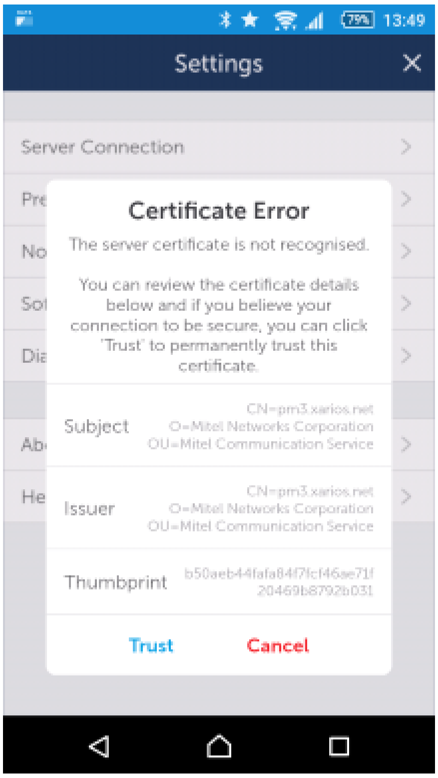
End-users will need to have the following information in their possession before they start the mobile client installation:

- 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.

9.1.3.7.4 Invitation Email

The Invitation Email page contains an email template that can be used to send users all the information they need to get Phone Manager mobile up and running. Once the email template has been altered as required, invitation emails can be send from the Mobile Clients page of the MCS website.

Dynamic Content Placeholders

The email template contains some dynamic content that will be populated by the system before sending to each user:

- @CERTURL -> This will be replaced by a URL to download the SSL certificate from the MCS
- @USERNAME -> this will be replaced by the user's full name
- @SERVER_IP_ADDRESS -> This will be replaced by the MCS's IP Address/Hostname from Client Locations
- @SERVER_REMOTE_IP_ADDRESS -> This will be replaced by the MCS's Remote IP Address/Hostname from Client Locations
- @USERLOGIN -> This will be replaced with the user's personal login name

It is important to leave all the placeholders for the dynamic content in the email template so the email is personalised for each user.

Administration Contact

A section of the email template has been reserved to enter the email address and/or contact details for an administrator who can help the end-user if they have problems. This should be manually configured before sending the invitation email to users.

Certificates

The MCS SSL certificate must be installed by iOS users before the Phone Manager Mobile application can connect back to the MCS. To try and simplify this process the email template includes a URL to the certificate and can attach the certificate to the email.

Unless port TCP 80 has been externally forwarded to the MCS server then the certificate URL will only work if the user is on the same network as the MCS server.

9.1.4 Phone Manager Outbound

Overview

This section enables the PBX and database details that are to be used with Phone Manager Outbound to be configured. This configuration section is generally only required on the initial setup of Phone Manager Outbound.

There is a separate website that is used for managing Phone Manager Outbound. This can be accessed from the 'Outbound' section on the main title bar of the application:

Configuration

PBX

Check the **Enable** option to enable the Phone Manager Outbound feature and set the **ACD agent Hunt Group** that Phone Manager Outbound will use. Make sure that the group number entered has been configured in Mitel Database Programming on the PBX to be an "ACD Hunt Group" with "Use ACD Agent IDs" enabled. Now when an agent logs into this hunt group on the PBX they will also be logged into Phone Manager Outbound.

Database

Phone Manager Outbound uses its own database to store its information. With the **Use default connection details** option set this will be hosted within the Communication Service instance.

Un-checking this is an advanced option allows a different database instance to be used. If a different instance is to be used then this needs to be a Microsoft SQL Server 2008 R2 SQL Server and the relevant database and archive databases will need to be created manually. The system will require a restart for this change to take affect.

Clicking on the *Test* button will validate the database details.

9.1.5 Call Recorder

Overview

The Mitel Communication Service has an embedded call recording engine that can be used to record all or a subset of telephone calls on the MiVoice Office 250 system. Calls that the system has recorded can then be replayed through the MCS website or through the Phone Manager Desktop Call History.

Licensing

The call recording feature is licensed based on the number of calls being recorded at any point in time. There are two licenses available for purchase on the MCS:

- MiVoice Office Call Recorder - Small Business License
- MiVoice Office Call Recorder - IP Extension License

> Check the Site license section of the website to see which licenses are available.

Small Business licenses can be used for either of the two recording sources outlined below, IP Extension licenses can only be used for recording IP/SIP extensions. It is important to ensure there are enough licenses on the system for the number of devices that are configured to be recorded.

Over Subscription

If more devices are configured to be recorded than there are licenses then there can be situations where calls are not recorded. When a call needs to be recorded, the system will check for a spare license, if there is one free it will consume it and record the call. If there isn't, the call will not be recorded. If more devices are configured to be recorded than there are licenses available then the calls will be recorded on a first come first serve basis.The system can be configured to only record external calls to reduce the licenses required. For example, if a system has 8 trunk lines and 32 extensions then an 8 device recording license can be purchased to record the external calls of all 32 extensions.

The sections below outline how each recording method is configured on the MCS:

Record-A-Call

Using the SIP Voicemail features of the telephone system, the MCS server can invoke the Record-A-Call feature and accept incoming SIP audio streams to record telephone calls. This method of recording calls provides a simple way of implementing call recording across a range of devices, including; Digital, Analogue and IP extensions.

For information on how to configure the telephone system to use this feature, please refer to the Record-A-Call section.

For information on configuring which extensions on the telephone system should be recorded, please refer to the Recorded Devices section.

> SIP Extensions (including Phone Manager Softphones) cannot currently be recorded using Record-A-Call. Use the IP/SIP Extension recording source for these device types.

> The trunk type does not have a bearing on the Record-A-Call recording source. As long as the extension type supports Record-A-Call, the trunk can be of any type.

IP/SIP Extension

Using a network interface card that is connected to a mirror port on the customer's switch, the MCS can intercept the SIP/RTP traffic for IP communications and record the calls. This applies to MiNET based extensions and SIP based extensions. This feature does not extend to SIP Trunks.

For more information on IP/SIP Extension recording, please refer to the IP/SIP Recordingsection .

> ⚠ Both Record-A-Call and IP/SIP Extension recording sources provide 'Extension Side' recording. Calls that are on hold, are at a call routing announcement or have been transferred externally will not be recorded.

> ⚠ Neither Record-A-Call nor IP/SIP Extension recording methods support the 'Multiple Ring In' type for trunk groups or call routing tables or the routing of external calls directly to a phone list. Ensure that UCD hunt groups are used instead of this ring-in type when using the MiVoice Office Call Recorder.

Recording Features

Other than selecting exactly which devices on the telephone system are to be recorded, the MCS provides a variety of ways to manage which calls are recorded and what happens to them after they are recorded. In addition, there are a number of recording specific permissions that can be applied to user accounts to control:

- Who has access to call recordings
- How they can access call recordings
- What they can do with the call recordings

The sections outlined below provide all the information on call recording related features:

Exclusion/Inclusion Lists	On most systems, there will be specific calls that should not be recorded. The Exclusion list can be used to stop the system recording calls that match an item listed. The Inclusion list is a back stop to this, and calls that match an inclusion list will automatically override an exclusion list.
Compliance Muting	When confidential information on a call should not be recorded, use Compliance Muting, e.g. Payment Details.
Retention Policies	Configure how long call recordings should be kept for.
Call Archiving	Configure where call recordings should be stored in the long term.
User Permissions	Configure who has access to the call recordings.

9.1.5.1 Record-A-Call

Overview

The Mitel Communication Service can record all extension* calls on the MiVoice Office 250 telephone system using the Record-A-Call feature.

> * Calls that route through a CRA and Hunt Group won't be recorded until they get answered at an extension. Trunk to Trunk calls are not recorded. Conference calls are recorded but not if they are transferred.

> It is not recommended to use the Record-A-Call recording source in multi-node environments, some calls scenarios such as cross-node conference calls are not supported.

MiVoice Office Call Recorder Configuration

To use the Record-A-Call recording source on the MCS, the software must first be licensed with MiVoice Office Call Recorder Small Business licenses. If these are present on the system, the following configuration must be performed:

- Devices that are to be recorded using Record-A-Call need to be added to the Recorded Devices section of the website.
- Any Exclusion / Inclusion options need to be configured
- For additional security, add the IP Address of the telephone system to the allowed addresses.
- Complete the MiVo 250 configuration outlined below.

> Once Record-A-Call devices are configured, the MCS will immediately being to invoke the Record-A-Call feature whenever they make a call. Ensure that the PBX configuration has been completed so that the MCS receives the Audio for the calls.

MiVoice Office 250 Configuration

To record the calls from the telephone system using Record-A-Call, the MCS needs to be configured on the telephone system as a 'SIP Voicemail'.

SIP Voicemail License

Before SIP Voicemails can be configured, they must be licensed on the telephone system. When purchasing the MiVoice Office Call Recorder - Small Business License, the necessary SIP Voicemail licenses for the telephone system are provided.

Ensure that these licenses have been added to the telephone system's AMC record and have been applied to the telephone system.

Once applied, they will be visible on the telephone system's license page. It is listed as 'SIP Voicemail Licenses In Use'. The number of licenses configured on the telephone system must be enough to record all the required calls on the system, the maximum supported at this time is 8.

SIP Voicemail & Record-A-Call Application

The MCS server must now be added as a SIP Voicemail on the telephone system. Open database programming for the telephone system and follow these steps:

1. Navigate to *'System\Devices & FeatureCodes\SIP Peers\SIP Voicemails'*
2. Right-Click in the right hand pane and select *'Create SIP Voicemail'*
3. If a message about *MiCollab Unified Messaging* appears, select *'No*'
4. Choose an extension number for the SIP Voicemail and then give it a name, for example *'MCS Recording'*
5. Navigate into the newly create SIP Voicemail extension, open the '*Configuration*' section and configure the following settings:
    - IP Address -> Set this to the IP Address of the MCS server (Note: This must be on the same NIC which the MCS is license is bound to)
    - Port -> 5060
    - Call Configuration
        - Choose a call configuration that uses G.711 (A-Law or MuLaw)
        - Set the Audio Frames/IP Packet to 2
    - Maximum Number Of Ports -> Set the maximum number of ports to be the same as the number of calls you wish to be recorded, the maximum supported at this time is 8.
    - Call Failure Threshold -> 500 (Set this as high as possible to reduce the risk of calls not being recorded).
    - Authentication -> Ensure in-bound authentication is enabled and that a secure username and password are applied.
6. Navigate to the *'Applications'* section. Right-Click in the right hand pane and select '*Create Record-A-Call*'
7. Give the new Record-A-Call extension and number and name

> ⚠ For security, ensure that the Inbound credentials against the SIP Voicemail are enabled and configured.

The SIP Voicemail configuration should now be completed. If the MCS server has MiVoice Office Call Recorder - Small Business licenses on it then the Operating State on the new SIP Voicemail added should say '*In Service'.*

> If there is a firewall in operation on the MCS server then the incoming ports for TCP 5060 may need to be opened for the MCS to accept connections from the telephone system.

> ⚠ The IP address used for the Record-A-Call SIP Voicemail connection must be on the same NIC which the MCS licence is bound to.

Ad-Hoc Conferencing Mode

The Ad Hoc Conference Type should be set to 'Advanced' when using the Record-A-Call recording source. When using Basic mode then Record-A-Call will be limited to a maximum of 4 concurrent calls and there is a higher risk of not being able to record a call because someone is using the resource for an ad-hoc conference.

> ⚠ Only one SIP Voicemail can be added to the telephone system by default. If you have Nupoint Messaging then the Record-A-Call via the MCS cannot be used without modifying the meta database on the telephone system.

Extension Record-A-Call Configuration

On each extension that is to be recorded, the Record-A-Call configuration settings needs updating to use the newly create Record-A-Call application on the SIP Voicemail.

On each extension to be recorded, apply the following configuration:

1. Navigate to the Record-A-Call configuration of an extension.
2. Update the '*Application'* section to be the Record-A-Call application on the MCS's SIP Voicemail
3. Set the *'Mailbox User-Keyed Extension'* to '*No'*
4. Repeat the configuration for each required extension

> If users are using Mitel Hot Desk devices than remember to configure the Record-A-Call configuration against the Hot Desk devices.

> If the '*Mailbox User-Keyed Extension'* is not set to '*No'* then the MCS will not be able to invoke a call recording when necessary

> Once an extension has been configured to be recorded via Record-A-Call on the MCS, its recording will be managed entirely by the MCS, the user will no longer be able to initiate Ad-Hoc Record-A-Calls.

Play Pre-Record-A-Call Message

One of the features available on Record-A-Call recordings is to play a message to the call informing them that the call is recorded at the start of the call. To enable this feature, browse to the main telephone system Flags in database programming and set the '*Play Pre-Record-A-Call Message'* flag to *'Yes'.*

To complete the configuration on the MCS and enable this feature, refer to the corresponding MCS Server Record-A-Call configuration.

9.1.5.2 IP/SIP Extension Recording

The MiVoice Office Call Recorder provides an IP/SIP Extension recording source that provides recording for MiNET handsets and generic SIP base devices (including Phone Manager Desktop and Mobile softphones).

This method of recording calls uses a network port mirror to capture the call audio. It can scale a lot larger than the Record-A-Call recording source and is the only way to record calls made on SIP based extensions.

To configure an MCS server to record this IP/SIP traffic, the following must be configured:

- A mirror port must be made available on the customer's network switch which provides a copy of data from the telephone system's network interface.
- A spare NIC must be made available on the MCS server to plugin the mirror port into.

Any RTP audio and SIP traffic that gets passed to the MCS down the mirror port can be recorded.

Once the mirror port(s) have been plugged into the MCS server, the following configuration must be completed to begin recording:

- Navigate to the Mirror Ports section of the website and tell the MCS which network cards on the server are providing the RTP/SIP data to record.
- Navigate to the Packet Filters section of the website and tell the MCS about the ports on which the RTP/SIP traffic can be found.
- Navigate to the Addresses section of the website and enter the IP address(es) of the telephone system.
- Add the devices to be recorded under the Recorded Devices section of the website.

> If the customer's switch does not support port mirroring then switches with hardware port mirrors could be installed between the telephone system and the customer's switch.

PS-1 & Multiple PBXs

It may be necessary to port mirror multiple network connections in order for the MCS server to receive all the required information.

If a MiVoice Office 250 has a PS-1 server installed then the network connections for both the Base Server and the PS-1 server need to be mirrored to the MCS.

If the MCS is recording calls for extensions on more than one PBX then each PBX's network connection(s) needs to be mirrored to the MCS.

For example, if an MCS is recording calls via the IP/SIP Extension recording method on 2nodes, each of which has a PS-1, the MCS will require 4 mirror ports to be configured.

> If there is more than one telephone system then multiple mirror ports can be plugged into the MCS server.

> ⚠ Each additional mirror port will require additional network interface card ports on the MCS server.

> ⚠ If you are having problems with setting up a mirror port, use Wire Shark or similar packet capture software to check that the RTP/SIP data is being sent to the MCS server.

Remote IP/SIP Extensions

Remote extensions (extensions that are not on the same LAN segment as the telephone system) can be recorded by the MCS server using IP/SIP Extension recording, but only in certain circumstances.

Remote SIP Extensions

SIP Extensions can always be recorded using the IP/SIP Extension recording source, no matter where they are located.The MCS interprets the SIP traffic between the telephone system and the extension to identify the extension involved in the telephone call. This is true even for SIP extensions that are connecting through a MiVoice border Gateway.

This applies to Phone Manager Softphones, both desktop and Mobile.

Remote IP Extensions (NAT'd through a firewall/router or Proxied through a MiVoice Border Gateway)

IP extensions that are connecting through a firewall/router or MiVBG can be recorded as long as each extension has a unique IP Address that can be seen by the MCS server. If there are multiple IP extensions connecting from the same remote location, the MCS server will only be able to see a single IP Address and will not be able to tell the extensions apart.

> If remote IP extensions are connecting through a MiVoice Border Gateway, the MCS must be told about the internal IP Address of the gateway. See the MiVoice Border Gateway section for more information.

Examples:

50 IP Extensions on a separate VLAN	Supported	The MCS will be able to see the IP address of each of the extensions.
10 IP Extensions home workers, each a different locations	Supported	The MCS server will see a different external IP Address for each extension.
10 IP Extensions at a remote office	Not Supported	MCS will see the same external IP address for all extensions.
A home worker with 2 IP Extensions	Not Supported	MCS will see the same external IP address for all extensions.

9.1.5.3 Exclusion List

Exclusion lists are used to discard recordings based upon a specific piece of meta-data that is associated with the call. For example, you can add calls to or from specific outside numbers to the exclusion list and they will not be recorded.

The following meta-data can be used to match a recording against an exclusion list.

- Account code
- Agent
- DDI / DID
- Outside number
- Endpoint
- Hunt group

> Some options may not be available for all PBXs

If a calls detail matches an item on the exclusion list, then it will not be recorded provided it does not match an Inclusion List entry. For example, if a senior directors calls should not be recorded then this could be configured for their endpoint.

As well as using the meta-data there is another rule that can be used:

Exclude internal calls: When extension side recording is being used then calls that are internal and do not involve an outside trunk line will not be recorded.

> ⚠ If the option for **Exclude internal calls** is enabled then the inclusion list will NOT override this and the call will NOT be recorded.

Configuration

To add a new exclusion list entry

1. Access the Site Settings -> Exclusion List configuration section
2. Click on *Add*, then select the **Type** of information to use to exclude this call.
3. Select or enter the value that this information must contain.
4. Enter a useful **Description** for this entry.
5. Select the level of persistence
6. Click on *Add* to save the entry.

Persist for Entire Call

Each exclusion list entry has the option to 'Persist for entire call'. This setting controls whether the exclusion entry should just take effect on the call segment that matches or on all proceeding segments on the call as well. If enabled, once there is an exclusion match on a segment of a call, if the call is transferred to another device on the phone system then the call would continue to be excluded.

Persistent exclusion list entries can be used in conjunction with a telephone system call routing announcement to ask the caller permission to record the call. By routing a negative customer response through a CRA with a persistent exclusion match, the call will not be recorded.

> If internal calls are being recorded, transfer announcement (enquiry) calls will still be recorded even if the call being transferred as a persistent exclusion against it.

9.1.5.4 Inclusion List

Inclusions lists override **ALL** other rules. If a recording matches any of the fields within the inclusion list, then it will be recorded – even if it is in the Exclusion List.

> ⚠ If the option for **Exclude internal calls** is enabled, the inclusion list will NOT override this and the call will NOT be recorded.

Configuration

To add a new inclusion list entry:

1. Access the Site Settings -> Inclusion List configuration section.
2. Click on *Add*, then select the **Type** of information to use to include this call.
3. Select or enter the value that this information must contain.
4. Enter a useful **Description** for this entry.
5. Select persistence level
6. Click on *Add* to save the entry.

Persist for Entire Call

Each inclusion list entry has the option to 'Persist for entire call'. This setting controls whether the inclusion entry should just take effect on the call segment that matches or on all proceeding segments on the call as well. If enabled, once there is an inclusion match on a segment of a call, if the call is transferred to another device on the phone system then the call would continue to be included, no exclusion list entry could override it.

9.1.5.5 Compliance

Businesses that record telephone conversations as part of normal business practice are often required to comply with industry specific or regional regulations which may dictate, among other things:

- How long recordings should/must be kept for
- What types of information can be recorded and what cannot
- Which parties involved in the telephone conversation need to be notified the call is recorded

Regulations that Affect Call Recording

Notification of Recording

Depending on the region the call recording equipment is installed in it may be necessary to notify one or all parties involved in a telephone conversation that the call is being recorded. In addition, some regions may require a continued audible notification that a call is being recorded.

The MiVoice Office Call Recorder is a passive recording device and has no way of adding audible notifications to a telephone conversation. To comply with regulations, the telephone system must be configured to provide the necessary notifications that the call is being recorded, usually through the use of a call routing announcement to incoming callers.

PCI-DSS Compliance

The payment card industry (PCI) has a set of regulations that apply to any organization that processes card payments. These regulations outline what information regarding payments and payment cards can be stored/transferred digitally by the organization.

For more information on how PCI regulations effect call recording, please refer to the PCI Compliance section.

GDPR

GDPR is the new EU regulations regarding the storage and transfer of the personal data within and crossing EU boundaries.

For information on how GDPR regulations effect call recording, please refer to the GDPR section.

MIFID II / FCA

Any organization that comes under the regulation of Markets in Financial Instruments Directive II / FCA will need to be aware of the requirements to record and retain recordings in relation to financial advice and transactions.

For more information on how MIFID II and FCA regulations effect call recording, please refer to the MIFID II section.

Compliance Features

The following features of the call recorder can be used to help comply with local regulations.

> Some of the features listed below require additional licensing to be used.

Pause / Resume Recording

The call recorder provides various methods to pause a recording to stop sensitive information being collected as part of a telephone conversation. In addition, the exclusion list rules can be used to instruct the recorder to dispose of a recording entirely if it matches certain criteria.

For more information, please refer to Pause / Resume section.

Recording Deletion

In response to data protection regulations, the call recorder provides access for specified users to be able to delete calls or calls segments that relate to a specific client or case.

For more information, please refer to the Recording Deletion section.

9.1.5.5.1 GDPR

The General Data Protection Regulation (GDPR) is an EU legal framework that set guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR sets out the principles for data management and the rights of individuals, it covers all companies that deal with data of EU citizens, even if the company is based outside of the EU.

What rights and controls do EU citizens have?

GDPR provides individuals with increased rights and control over how their data is used. GDPR includes the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making, including profiling

In addition, businesses wishing to record personal data will need to ensure that at least one of the following six conditions be met to legally record the data:

- Individuals involved in the call have given consent to be recorded
- Recording is necessary for the fulfilment of a contract
- Recording is necessary for fulfilling a legal requirement
- Recording is necessary to protect the interests of one or more participants
- Recording is in the public interest, or necessary for the exercise of official authority
- Recording is in the legitimate interests of the recorder, unless those interests are overridden by the interests of the participants in the call

How does this affect businesses?

Any business that processes personal data will need to ensure they have policies and processes in place to meet the rights of the individual's data they hold. In addition, they need to ensure they have a legal right to store the data, they are not storing data on minors, and that they have processes in place to report data breaches.

How does GDPR affect MiVoice Office Application Suite?

There are various features within the suite which can store personal data. These include:

- Contact Directory - Custom data fields can be inputted along with telephone numbers and other contact information
- Call Recordings - Personal data could be discussed on calls and stored in call recordings. Calls can also be tagged with custom data and notes
- Call Reporting - Telephone numbers can contact/speed dial names are stored within the call history system
- Phone Manager Outbound - Campaign data can contain personal information if imported in addition to the contact information

Any business that stores personal data (including recording telephone calls) will need to ensure that they have a legal right or requirement to do so. Where data storage (such as call recording) is not explicitly required by regulations (such as MIFID II), consent will usually be required.

Any personal data stored in the system will need to be documented as part of the business' GDPR policies, with specific references on how data can be identified and modified/removed if required.

How consent for data storage is sought, recorded and managed is of vital importance. The ICO has published a detailed guidance on consent under GDPR:

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

If existing forms of consent held by businesses do not meet the new requirements, they must be refreshed so that they meet the new GDPR requirements.

Employee User Data

The system will store limited personal data for users/employees. User accounts configured on the system will have an email address for the employee but no other specific information about the user. The system does store audit information about what users of have done; when they logged in, settings changed, recordings played etc.

In addition to usage data, any call recordings involving employees may contain personal data if discussed.

Customer Data

It is possible for the system to store the personal data of a company's customers in 3 locations:

- Contact Directory Data - *Imported into the system*
- Call Data - *Logs of calls to/from the customer including their phone number and possibly their name if there is a contact match. This could also include custom notes added or data tagged to a call using the API*
- Call Recordings - *Any information about the customer recorded on a call*

It is important to understand what information is being collected by the call logging/recording system to ensure that any customer requests can be responded to.

> Customer data can also be stored in the Mitel Phone Manager Outbound system. For information on this, please refer to the Mitel Phone Manager Outbound Technical Manual.

How to use the MiVoice Office Application Suite to help meet GDPR requirements?

The following sections outline how GDPR affects the system and how various features within the system can be used to help companies comply with GDPR requirements.

Document what is stored and ensure it contains no sensitive data

The previous section listed what types of personal data may be stored in the system. It is important to add to your existing GDPR documentation the data that is being stored in the suite. If any of the features listed are going to be used as part of the MiVoice Office Application Suite implementation (Contact Directories, Call Notes, Call Tagging, Call Recording, Phone Manager Outbound), the type of data stored must be documented.

> ⚠ The call data fields and contact data fields are not designed to store sensitive personal information. Ensure that any data imported into a contact directory or added in a note or tag field against a call is not classed as sensitive and does not relate to a Minor.

Consent / Provide callers with option to opt out of recordings

It is important to ensure that you have consent to record customer information (including recording calls) and that they have opted in. If required, Mitel can provide solutions to allow callers to opt in at the beginning of a telephone call. Contact your Mitel Sales Representative for more information.

Secure/Audit Access to the System

It is important to ensure that only the relevant users have access to the system and that they only have the minimum permissions that they require. In addition, ensure that the server the solution is installed on is appropriately secured and that no unauthorised users can gain direct access.

For more information on securing the server, please refer to the Best Security Practice section.

Tag recordings with Customer ID for Transparency

To ensure that customer records can quickly and easily be identified, the Communication Gateway API can be used to tag calls with a customer ID or other method of identification which offers improved searching over caller ID/telephone number searching.

Tools Available to Modify/Remove Data

Tagged data fields against call records and contact data can be updated or removed from the system. To remove call recordings themselves, they must be manually deleted from the storage medium at this time.

End-User Training

Ensure that all users of the system are trained on data protection and are informed that their own calls are being recorded (if applicable). Provide users with a non-recorded extension that they have access to so that they can make personal calls that are not recorded.

Update Internal Documents on where data is stored

When installing the system, ensure that your GDPR policy documentation is updated to make reference to any personal data that is being stored within the MiVoice Office Application Suite.

9.1.5.5.2 MIFIDii

The Markets in Financial Instruments Directive II (MIFID II) became live on the 3rd January 2017. It affects companies involved in financial services, including; inter dealer brokers, stockbrokers, financial advisors, corporate finance firms and venture capital firms, trading venues, DRSPs, banks, investment managers, tied agents and appointed representatives, trustee firms, OPS firms, depositaries, ICVCs, service companies, authorised professional forms and others.

For more information on the Financial Conduct Authority (FCA) MIFID II implementation, please review their policy statement - https://www.fca.org.uk/publication/policy/ps17-14.pdf.

MiFID II compliance includes an expanded requirement for comprehensive recording of transactions between clients and the company, irrespective of whether the transaction resulted in a sale of service.

MiFID II com plaice includes requirements for recording all client communications, including; face-to-face meetings, SMS, chat, email and telephone conversations. All transaction recordings must be detailed and stored for up to seven years, to provide evidence should a dispute occur.

MiFID II Call Recording

MiFID legislation requires comprehensive and evidence-proof recording and archiving of telephone calls that may result in transactions. The following requirements must be met:

- **Capture** -> Capture and store all communication is a high quality format. Recordings should be encrypted and secured.
- **Notify** -> Notify the caller that their conversations are being recorded
- **Store** -> Recordings must be time-stamped, indexed with effective tags and kept for up to 7 years.
- **Retrieve** -> Recordings and associated data must be quickly and easily accessible allowing a reconstruction of events in a timely manner.

Capture

Call recordings made by the system are digitally signed and encrypted to ensure that they cannot be tampered with. For information on this process, please refer to the Encryption & Authentication section.

Notification

MiVoice Office Call Recorder operates with a port mirroring interface and cannot interact with the telephone conversation. To notify the caller, the telephone system must be used or some other form of opt-in by the client. Using a Persistent Exclusion List entry and Call Routing Announcement, callers can be asked for permission to record at the beginning of a call. For more information on this, please contact a Mitel Sales Representative.

Storage

All recordings can be archived indefinitely at one or more locations with all the meta data relating to the call. This includes all the telephony data (Caller ID, DDI, start time, call duration, extension number, agent, user, account codes, hunt group etc.) as well as any custom tagged information such as customer reference numbers or order numbers.

Retrieve

An comprehensive search interface allows calls to be identified by all types of meta data, including any pieces of custom tag information like customer number. By using customer specific (or event order/transaction specific information if tagged to a call) it is easy to reconstruct communication between a client and an advisor.

9.1.5.5.3 PCI Compliance

The Payment Card Industry Data Security Standards (PCI-DSS) is designed to safeguard the security of customer's card based payment transactions by ensuring that sensitive card information is not stored and the staff do not have access to them.

How does PCI-DSS effect Call Recording?

If a business is processing MOTO (Mail Order/Telephone Order) payments then it is violation of PCI-DSS to store sensitive card data without proper protection in place, CVV/CV2 cards are never allowed to be stored.

Currently there are two ways supported by the MiVoice Office Call Recorder to avoid storing payment card information:

Process all payments at an unrecorded extension

A single or group of users can be designated as card processing agents. The extensions used by these users can then be added to the Exclusion List so that none of their calls are recorded.

Pause recording while payment card details are communicated

The other way to ensure that payment card information is not recorded is to pause the recording while the information is being communicated. This can be done manually by the user or automatically using the window and URL tracking capabilities of the Communicator Desktop client.

> Removing the payment card information from recordings removes the recorder from PCI-DSS security compliance. However, it is important to ensure that the telephone system itself is secured when transmitting payment card information.

9.1.5.5.4 Compliance Pause/Resume

In some circumstances it may be necessary to stop parts of telephone conversations being recorded. This is usually down to confidential information being imparted on the call that must not be stored. A prime example of this is payment card details being communicated which means the call would come under PCI-DSS compliance regulations if it was recorded to disk.

The call recording system provides the ability to be able to pause recordings while the confidential information is being communicated so that it is not recorded. This can be implemented in one of three ways:

Automatic Pausing using the Call Recorder Client

The call recording feature of the solution has a dedicated client that can be used to track applications that are open on a user's desktop and automatically pause a recording if certain parameters are met. The application can also track some web browsers and which URL a user is using.

For more information on how to configure and use the Call Recorder client, please refer to the Call Recorder Client section.

Manual Pausing using DTMF or Phone Manager/Call Recorder Client

If there is no way to automatically track when to pause a recording or the necessary licenses have not been purchased then recording can still be paused manually by the user. This can be done using DTMF on the telephone keypad (or programmable key) or by using the built in functions of the Phone Manager toolbar.

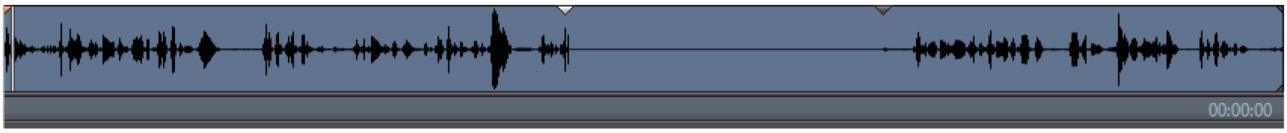
> DTMF Muting of recordings is not supported when using the Record-A-Call recording source.

Automated/Manual Pausing using the REST API

The system provides a REST based Web Service API that can be used to check the status of extensions and pause/resume recordings as required if there is a call being recorded at the time.

Paused Calls

When a call is paused, this is shown on the time line in the recording playback window with a flat line. There are also time line events at the start and end of the paused section to indicate when this has taken place.



9.1.5.5.4.1 Call Recorder Client

The Call Recorder Client provides automated muting of call recordings based on Windows applications that a user has open/or in current focus. As users open or close applications or switches between them, if the application is on a pre-configured list for do not record then the call recording will be automatically paused. Once the user has closed or changed the focus to another application the call recording will then be automatically un-paused.

The muting of call recordings requires no intervention by the user and can be configured so that there are no visible notifications to make them aware that this is happening. Alternatively notifications can be enabled to give feedback to the users when this is occurring.

The Call Recorder Client can be found as part of the Phone Manager install. It can be installed with Phone Manager or independently.

Connections

Each Call Recorder Client uses a user's' specific login credentials' when connecting back to the server. By default, it will try to use Windows Integrated login to find a user account on the MCS. Once connected, the client will monitor the user's Primary Extension for calls unless the user has a Phone Manager Desktop client running, in which case it will use whichever extension Phone Manager Desktop is associated with.

Configuration

The following settings control how the Call Recorder client operates and appears to the user:

S**how pause notifications**: Display a notification in the system tray that a recording has been paused.

Show status icon: Hides or displays the system tray icon that shows the client and call status.

Show settings menu: Make the settings menu visible to the users.

Enable debug mode: Enable the diagnostic options to the users, this includes showing the configured URLs/Window names that are to be matched and any pages that are open that do match.

Show desktop toolbar:Hides or displays the manual pause tool bar within the client application

Prevent client exit: Prevents the user from closing the application.

Enumerate Child windows: Specifies whether the Call Recorder Client should match on just parent windows or should search through child windows for matches..

Check Open Applications: When disabled (default), the client will only check the in-focus application and will recheck when focus changes. If Check Open Application is enabled then all applications are checked whether they are in focus or not. The application will then search based on a timer and not off focus changed events.

Tag With User: When enabled, the call in progress will be tagged with the current user. (Not required on MiVoice Office 250)

> ⚠ If Enumerate Child Windows & Check Open Applications are both enabled then the Call Recorder Client will be performing a lot of searching which may affect the client computer's performance.

Muting Calls Monitors

Each Call Recorder Client will monitor any rules created for a match with the name of any application/URL the user has in focus on their computer. While there is a match detected by the Call Recorder Client, any recording currently in place at the user's extension will be paused until the matching application/URL is closed or changes to something else.

Rules can be created on the Muting Rules page. Pressing the 'Add' button loads the' Add/Edit Monitor' page which has the following parameters:

- Input Type -> Plain Text or Regular Expression. As required, if using plain text the system will search for matches that start with the value entered
- Value -> The value to search for
- Active -> Enables or disables the rule. When disabled it will be ignored by Call Recorder Clients looking for matches.

Once a rule is entered here it will automatically be picked up by any currently connected Call Recorder Clients within 2 minutes.

Matching

The Call Recorder Client will try and match the following against the rules entered:

- Windows Heading
- Child Window Heading*
- Browser URLs
- Browser Tab Names

* Only get searched if the 'Enumerate Child Windows' options is selected.

Browser Matching

Call Recorder Client works with the most common browsers to provide URL and Tab Names where possible. Over time, changes to browsers may cause issues to the Client's ability to query the information it needs and may require an updated version of the Call Recorder client to be released.

The following information can be obtained from browsers:

Browser	Version	URL (In-focus Tab)	URL (Out-of-focus Tab)	Tab Name (In-focus Tab)	Tab Name (Out-of-focus Tab)
Internet Explorer	11	✓	✗	✓	✓
Firefox	46.0.1	✓	✗	✓	✗
Chrome	51.0.2704.84	✓	✗	✓	✗
Edge	20.10240.16384.0	✓	✗	✓	✓

When writing a rule to capture the correct moment to pause a call, use the Call Recorder Client's Logging page to see exactly what the client is tracking at the time and then write a rule to match it. For more information, refer to the Call Recorder Client Manual.

Plain Text Examples:

http://www.mitel.com -> This would pause any recording in progress if the user browses to any page on Mitel.com.

http://www.mitel.com/Products -> This would pause any recording in progress if the user browses to the products page on the Mitel website.

Regular Expression Examples:

^https:.*paymentsite.*card -> This would pause any recording in progress if the user browses to a URL that starts *'https:'* and then has the word 'paymentsite' followed by the word *'card'* somewhere in the URL.

9.1.5.5.4.1.1 Overview

The MiVoice Office Call Recorder Client tracks windows applications and matches window names to server configured rules to check whether any call recordings in progress need to be paused or not.

The application is an optional part of the Phone Manager installation. Once installed, the application automatically runs each time the user logs into their computer.

The application has two components:

- System tray icon -> Displays the status of the client and of any calls that may be in progress at the associated extension
- Toolbar -> Can be used to manually pause calls or to tag calls with customer specific information

Associated Extension

The Call Recorder Client monitors an associated extension and will pause any recordings on the extension when required. By default the client will monitor the user's primary extension unless there is a Phone Manager Desktop Client running on the same desktop. If there is, the Call Recorder Client will monitor the extension that Phone Manager is currently associated to. If the Phone Manager client is closed, the Call Recorder Client will revert back to monitoring the user's primary extension again.

If user's don't have a primary extension and are moving around then they will need to have Phone Manager Desktop client running for the Call Recorder Client to operate correctly.

> The Phone Manager Desktop Client can be configured to prompt the user for the extension they are sat at if they have no fixed primary extension. If the user is using Mitel Hot Desking, their primary extension should be their Hot Desk extension

System Tray

The system tray icon show the status of the application and provides access to the Settings of the application and the Toolbar. It can be hidden if required using server side configuration. Right-clicking the system tray icon displays the menu that gives access to:

- Settings -> Configure connection settings for the application
- Toolbar -> Manually pause/resume recordings
- Logging -> See real-time information of the applications the Call Recorder Client is tracking

The table below shows all possible states:

	Loading, this icon shows when the application first loads
	Connection Error, the application is not connecting to the MCS server correctly *
	Idle, this icon will display when the associated extension has no calls
	On a call, this icon will display when the associated extension has a call that is not being recorded. This occurs when the call is not on a recorded device (could be an internal call or on a trunk that isn't recorded)

	Recording, this icon displays when there is a call at the associated extension that is being recorded
	Paused, this icon displays when there is a call at the associated extension that is being recorded but is currently paused.

> * When the application is not connected to the MCS, the only option available on the right-click menu will be to access the Settings.

Toolbar

The toolbar provides the user with access to manually pause any recording that is in progress and to tag call record with customer specific information such as order numbers or ticket numbers.

For more information, see the Toolbar section.

9.1.5.5.4.1.2 Logging

The logging form provides a real-time view of the information the Call Recorder Client is tracking about the application that currently has focus. Depending on the server-side configuration, the following information can be shown:

- The Window Name of the in-focus application
- Child window names for the in-focus application
- URLs and Tab names for browsers*
    - Internet Explorer
    - Edge
    - Firefox
    - Chrome

The logging window is an ideal tool to use when configuring the match rules on the server. If there is a match on the current window then this will be displayed in the Logging window so that rules can be tested on the target clients.

Browser Matching

Call Recorder Client works with the most common browsers to provide URL and Tab Names where possible. Over time, changes to browsers may cause issues to the Client's ability to query the information it needs and may require an updated version of the Call Recorder client to be released.

The following information can be obtained from browsers:

Browser	Version	URL (In-focus Tab)	URL (Out-of-focus Tab)	Tab Name (In-focus Tab)	Tab Name (Out-of-focus Tab)
Internet Explorer	11	✓	✗	✓	✓
Firefox	46.0.1	✓	✗	✓	✗
Chrome	51.0.2704.84	✓	✗	✓	✗
Edge	20.10240.16384.0	✓	✗	✓	✓

9.1.5.5.4.1.3 Toolbar

It enable by the server, the Toolbar will be available to provide the following features:

- Show call state and allows recordings to be paused/resumeed manually
- Tag calls that are in progress with information

To load the Toolbar, right click on the system tray icon and select 'Show Toolbar' from the menu. Once the toolbar has loaded it can be moved, resized or docked to the corner of the screen as required.

Manual Muting/Unmuting

If there is a call recording in progress at the associated extension then the user can manually pause and resume the recording using the relevant button.

The LED on the button will change colour to show the status of the recording; Red -> Recording, Yellow -> Paused

If there is no call currently being recorded at the extension then the Pause/Resume button will be disabled.

Tagging Calls

Any call in progress at the associated extension can be tagged with additional information. This is most commonly used for adding information to the call records on the server which will make it easier to find later, for example:

- Customer reference numbers
- Order or ticket numbers
- Fault reference numbers

When there is a call in progress at the associated extension the Tag Call button will be enabled. Clicking the button will load a form that will prompt for the for the information along with a selection box allowing the user to select which of the 5 tag fields on the server they wish to add the information to.

9.1.5.5.4.1.4 Settings

The Settings form provides configuration of how to connect to the server and the associated extension.

> The Call Recorder Client shares it's connection settings with Phone Manager Desktop, changing the connection settings in either application will cause the other application the change.

Connection

The connection details outline how the client will connect to the MCS server.

Location

The application has two lots of connection settings, one for connecting to the MCS when on the local LAN and one when connecting from outside the LAN. If the software is installed on a laptop and will be changing locations then the software can be configured to prompt the user for their location on startup.

Connection Settings

The connection settings combine the Hostname/IP Address of the MCS server and the user credentials that will be used to connect. If the "Override login details" is not checked, the software will attempt to connect with the user's Windows Credentials.

User Preferences

The user can set there preferred language for the application here.

Diagnostics

If requested by technical support, diagnostic logging can be enabled here. The "Download Logs" button will zip together all required files and save them on the desktop of the local machine in a file named *CallRecorderClientLogs.zip.*

9.1.5.5.4.2 Manually Pausing Calls

DTMF Pause/Resume

The system can be configured to pause the recording of a call when a sequence of DTMF digits is entered by the user on the telephone handset. A second sequence can then be entered to un-pause the recording. This can be useful for compliance purposes if your staff are taking credit card payments for example. To make it easier for the user, the DTMF digits could be programmed under a programmable key on their telephone handset so that it is a more simple procedure.

To configure the pause and resume DTMF feature:

1. Access the Features -> Compliance Pause/Resume -> **DTMF Pause & Resume** configuration section.
2. Enter the sequence of digits to use for pausing a call in the **Pause DTMF** section.
3. Enter the sequence of digits to use to resume recording a call in the **Resume DTMF** section.

When configuring the DTMF sequence to use it is recommended to use a combination of tones, for example *123, as this will reduce the chance of this being activated when navigating though systems that require DTMF tone input.

> Licensing: Pausing calls using DTMF requires a DTMF Compliance license. Please check the system has this license before configuring.

> Due to no DTMF being received, DTMF Muting is not supported when using the following recording sources:
>
> - MiVoice Office 250 Record-A-Call

Pause/Resume with Phone Manager

If a Phone Manager user has an assigned toolbar or an integrated toolbar then a button can be configured to allow the user to:

- See the recording status of any call they are on
- Pause/Resume any recordings using the button as a toggle

For more information on using this toolbar feature, please refer to the Phone Manager manual or here.

9.1.5.5.5 Recording Deletion

The recording deletion features of the solution provide a way for users to be able to delete recordings that may contain personal information regarding customers and/or users. This feature is hidden from all users who do not have the 'Recording Deletion' role applied to their Security Profile.

For information on GDPR and how it affects call recording, please refer to the GDPR section.

Deleting Recordings

Recordings can be deleted from the standard 'Recordings' section of the solution if it is accessed using the 'Enter Recording Deletion Mode' button. Once the button has been pressed, the recordings section will be loaded with a banner displaying 'Deletion Mode Is Active' to warn the user that it is possible to permanently delete recordings.

Using the standard search methods available on the 'Recordings' section, the recordings to be deleted should be identified. Whole calls or call segments can be deleted but not sections of a call.

Using the check box on the left side of the recordings grid, one or more calls can be marked for deletion. Once all calls have been marked, the deletion process can be started by pressing the 'Delete Marked Items'.

Before the deletion process is started, a warning screen will appear asking the user to confirm the action.

Archived Recordings

Archived recordings can be deleted as long as the call recorder has write access to the media that the recording has been archived to. In these scenarios the recording path entry in the database will be deleted so that the recording can no longer be replayed through the call recorder.

> ⚠ Any recordings deleted from the system cannot be recovered. Please take care to ensure that you do not delete recordings that may be required.

9.1.5.6 Retention Policies

When using the Call Recording features of the solution, there are two types of information stored for each call:

- Call Data (CLI, DDI, Start Time etc) -> This information is stored in one of the SQL databases
- Audio Data -> This is the actual recording of the call audio itself. This is stored on the hard drive of the machine or on a network share if archiving is being used.

The audio data can take up quite a large amount of space and over time can fill up hard drives and network shares. If the audio data is not required after a set period of time then retention policies can be used to delete recordings once they reach a certain age.

This affects recordings that are on local drives and those that have been archived to network shares.

To enable the automatic deletion of recordings, check the box next to 'Delete old recordings' and then configure the 'Delete calls older than' setting accordingly.

> ⚠ Once the policy is configured on the system, recordings outside the policy age set will immediately be deleted and cannot be recovered. Ensure you have select the correct policy age and understand that recordings cannot be recovered once deleted.

9.1.6 Historical Reporter Overview

The MCS server provides access to the Call Reporting features of the MiVoice Office Application Suite. Call Reporting features include:

- The ability to run Call Lists and Grouped Reports
- The ability to configure schedules to automate reporting to email or a network share

This section outlines how the reports are licensed and how users can be given permissions to use reporting features. For information on running and using reports, please refer to the Reporting section.

There are a number of settings which affect how reporting data is calculated and presented. Refer to the Call Reporting Settings section for more information.

Licensing

There are 5 specific licenses that govern how reporting can be access and used:

Call Logging

The call logging license is a system wide license that enables access to the reporting section of the MCS website. This license provides access to run Call List reports, configuration reports and the Inbound Call Summary report.

Call Reporting Devices

For access to any type of grouped reports with aggregate data (Calls by Extension or Calls by Trunk for example), Call Reporting Devices licenses must be installed. The number of Call Reporting Device licenses required will depend on the number of extensions programmed on the telephone system(s) that the MCS is connected to.

If a system has Call Reporting Device licenses, users will be able to create and run grouped based reports.

> The Call Logging license is a prerequisite to having Call Reporting licenses.

> If a system has insufficient Call Reporting Device licenses to cover the number of extensions on the telephone system(s) then the system will go into license violation mode. Refer to the License Violation section for more information.

DND Reporting

The is a system wide licenses that enables the storage of and reporting on do-not-disturb (DND) events from the telephone system. Once enabled, the system will log DND status change events and provide access to DND status columns and DND event reports.

> DND events from the telephone system are not stored historically until the system has a DND Reporting license.

ACD Reporting

This is a per agent license that enables the storage of and reporting on automatic call distribution (ACD) events from the telephone system. Once enabled, every time an ACD agent logs in an ACD Reporting license will be consumed and the status change events for the agent will be historically logged in the database.

> ACD events from the telephone system are not stored historically unless an ACD Reporting license is available for the an Agent when it logs in.

Scheduling

The Scheduling license is a system wide license that enables access to create schedules for call reports. It can be applied to systems that only have Call Logging licenses or systems that have both Call Logging and Call Reporting licenses.

> Refer to the Report Templates section for more information on which types of report can be run with which license.

User Permissions

When a system has been licensed with reporting licenses, users can be given permission to run reports and create/manage schedules. This is done through the use of Security Profiles.

Other than giving users access to run/manager reports, there is no way to limit user access to specific report data. Once a user has access to reports they can run them on all historical data stored on the system.

9.1.6.1 Call Reporter Settings

The following settings are used when calculating data for the Call Reports. Settings changed here will affect all users.

General

Call Rate Period

The call rate period is used by the Calls by Start Time template when grouping calls together. Calls will rarely have the same Start Time, so to group them together to see call over time the Start Time is rounded down using the Call Rate Period. For example, with the call rate period set to 30, calls will be grouped in ranges of 30 minutes -> 08:30-09:00, 09:00-09:30. (Default: 30 minutes)

Short Call Threshold

Any call with a talk time (plus hold time) less than the value configured here will be classed as a Short Call. Using filters, these calls can then be removed from reports if required. (Default: 20 seconds)

Ignore Abandoned Calls

If this setting is enabled, any call with a ring time less than that of the abandoned call threshold will be excluded from reports. (Default: False)

Service Level

This setting is the target time in which inbound calls should be answered. This is used when calculating what % of inbound calls met the target service level. (Default: 10 seconds)

Daily Statistics Reset Time

This setting controls two things:

- When the Real-Time statistics for the Wallboard/Dashboard get reset to zero to denote the start of a day.
- When the Historical statistics calls a new day as starting. Any calls crossing this transition time will not be grouped together.

(Default: 02:00)

Reset Call Timers Only Once per Call

When enabled, the call timers will only be reset once per call. When disabled, call timers can be reset each time a call rings at a hunt group with the 'Reset call timers when a call rings this group' settings enabled.

(Default: Enabled)

Account Codes

When looking at a Calls by Account Code report, all calls with any type of account code on will be displayed. However, when viewing reports grouped by other items (Trunks, DDI, etc) then account code columns need to be added to the report.

The Account Code settings here represent the 10 account code columns that are added to these grouped reports. Any description given to the code here will be used in column headers on the reports so they make sense to the user.

Ring Duration Categories

The ring duration intervals configured here are used in grouped reports to show the break down of when calls were lost and answered.

Each ring duration is calculated as <= when calculating the call statistics.

For example, if a call was answered after 9 seconds, it would be counted in all but ring duration 1's statistics on a report.

(Default: 5, 15, 30, 60, 120, 240)

Call Statistics

Depending on the device type that is involved in a call, how the call is modelled and whether the call is treated as answered can be changed. Please refer to the PBX Configuration section for more information.

9.1.6.2 Call Reporter Global Variables

Global Variables provide a way to add data manually to one or more Real-Time Wallboard/Dashboard tiles. Data entered here can be added to any wallboard/dashboard by a real-time user.

Access to create, edit or delete global variables is controlled by Security Profile.

To create a global variable, press the 'New' button and populate the two required parameters:

- Name, this is the name real-time users will see when adding the data to a tile. This must be unique amongst global variables
- Value, this will be the data displayed on the real-time tile.

Global variables can be edited and deleted as required. Any changes made to a global variable will be reflected immediately on any Wallboard/Dashboard it is being displayed on.

9.1.6.3 Trunk to Trunk, Conference Calls & Dynamic Extension Express

Certain call scenarios can cause confusion when interpreting historical and real-time statistics. In general, these are calls that either include more than one trunk or there are more than two participants in the call.

- Trunk to Trunk Calls, calls that link two trunks together and are no longer connected to any internal extension
- Conference Calls, calls where there are more than two participants. This can be a mixture of internal and external participants
- Dynamic Extension Express Calls (DEE), these are personal routing calls where the phone system hunts around more than one of a user's extensions/external numbers to find them

The following sections outline how each to the call scenarios listed above affects the various aspects of historical and real-time reporting.

Trunk to Trunk

These are calls that connect to external parties together, with no internal device involved in the call.

Historical

Trunk to trunk calls have the following effect on historical reports:

Template Type	Description
Call List	When viewed in a call list, trunk to trunk calls will appear only once, but with details of both trunk numbers and outside numbers involved in the call.
Calls by Trunk	When viewed on a Calls by Trunk report, the call will be summarized against each trunk that was involved in the call.

Real-Time

Trunk to trunk calls have the following effect on real-time tiles & grids:

Statistic Type	Description
Active Call Statistics	• **Calls In Progress External**: Trunk to trunk calls will count twice in active external calls, once for the inbound leg and once for the outbound leg.
Call Totals	• **Calls Inbound/Outbound**: The call is accounted for in both the Calls Inbound and Calls Outbound statistics. This logic applies to all statistics that are calculated from these, such as % Calls Inbound/Outbound. • **Calls External/Calls Handled**: Trunk to trunk calls are counted twice, once for the inbound leg and once for the outbound leg.

Trunk Grid	Trunk to trunk calls will display twice on a Trunk Grid, once for each trunk involved in the call.
Call Grid	Trunk to trunk calls display as a single call on the Call Grid

Conference

Conference calls are calls which include 3 or more devices. These can be a mix of extension and trunks (external calls).

Historical

Conference calls have the following effect on historical reports:

Template Type	Description
Call List	When viewed in a call list, conference calls will appear only once, but with details of both trunk numbers and outside numbers involved in the call.
Calls by Trunk	When viewed on a Calls by Trunk report, the call will be summarized against each trunk that was involved in the conference. The trunks may be involved as inbound or outbound calls depending on how the conference was set up.
Calls by Extension	When viewed on a Calls by Extension report, conference calls will be counted against each extension that is involved in the conference.

Real-Time

Conference calls have the following effect on real-time statistics and grids:

Statistic Type	Description
Active Call Statistics	• **Calls In Progress**: Each participant of a conference will be counted within the active call statistics. External parties will be counted under 'Calls In Progress External' for example.
Call Totals	Each party of a conference will be counted within the call totals statistics.
Trunk Grid	Any external participants in conference calls will be displayed as a normal incoming or outgoing call on the trunk grid.
Extension Grid	Any internal participants in conference calls will be displayed as a normal incoming or outgoing call on the extension grid (and agent grid if an ACD agent is logged into one of the extensions).
Call Grid	A conference will shows as a single entry on the call grid, no matter how many participants are involved in the conference.

Dynamic Extension Express

DEE calls have a large impact on both historical and real-time data. When a user receives a DEE call, it is effectively a hunt group call which can be answered on any of the user's device. To make matters more complicated, DEE calls can be answered on external number such as a home or mobile number.

Historical

DEE calls have the following effect on historical reports:

Template Type	Description
Call List Segmented	When viewed on a segmented call list, each device which is alerted as part of a DEE call will be displayed. The hunt group parameter is populated with DEE to indicate why the extension was called. **Lost Calls:** On call list reports, unanswered DEE calls that have alerted an external device will appear twice as a lost call, once for the unanswered inbound leg, and once for the answered outbound leg.
Calls by Trunk	When viewed on a Calls by Trunk report, the call will be summarized against each trunk that was involved in the call. If the DEE call originated externally, it will be counted against the incoming trunk. If the call alerted or was answered externally, it will be counted against the outgoing trunk.
Calls by Extension	When viewed on a Calls by Extension report, DEE calls will be counted against each extension that the calls rang at and will be classed as answered on the extension it was answered on and missed on all other extensions it rang at.

Real-Time

DEE calls have the following effect on real-time statistics and grids:

Statistic Type	Description
Active Call Statistics	• **Calls In Progress External**: External DEE calls will be displayed in active call statistics. If the DEE call originated externally, it will display as a trunk to trunk call would. If it originated internally, the external leg will appear as an external outbound call.
Call Totals	**Calls Outbound/Outbound (DEE)/Calls External/Calls Handled:** Externally answered DEE calls are excluded from the normal Call Total statistics. They are not calculated as part of the Calls Outbound/External or Handled statistics. Instead, a dedicated statistic named Calls Outbound (DEE) is provided for these externally

	answered legs.
Trunk Grid	Externally ringing/answered DEE calls will display as a normal outgoing call on the trunk grid.
Call Grid	DEE calls will display as a single call on the call grid, event when ringing multiple numbers

9.1.6.4 Call Reporter External Data

External data sources can be used with the Real-Time elements of the MiVoice Office Call Reporter to display information from data sources external to the call/status logging platform. It provides a method for displaying important information on a Real-Time Wallboard/Dashboard that hasn't come from the telephone system. Some examples of the data from external data sources might be displayed:

- Sales information such as targets or orders processed
- Support information such as open tickets or escalated tickets

The external data feature can be used to query information from any ODBC or OLE DB compliant database. Data returned from these queries can be displayed on single statistic, multiple statistic and ticker tiles.

Licensing

The external data feature is a licensable feature within the MiVO Application Suite. If your system is licensed, the ‘External Data Sources' should be visible within the MiVoice Office Call Reporter area of the Site License section of the website.

Once the feature has been licensed, any number of external database connections can be configured.

Configuring an External Data Source

This section outlines the steps involved in configuring a connection to an external database and pulling back one or more pieces of data. The connection string and command details will vary depending on the type of database being connected to.

> To connect some databases, additional drivers may need installing on the operating system running the MCS server. For more information, please review the documentation of the target database.

Connections

The connection is the first step in configuring MCS to communicate with an external data source. The following properties need to be configured:

- Name, used to uniquely identify the connection to anyone managing the MCS website
- Type, ODBC or OLE DB. Select the connection type required by the target database
- Refresh Interval, how often the MCS will requery the external database for updated information (minimum 5 minutes)
- Connection String, this provides all the information necessary to connect to the external database including location and authentication

The connection string will vary depending on the target database's type and location. To help in setting up a connection, some example connection strings are provided. In the examples below, the parameters myServerAddress, myDataBase, myUsername & myPassword need substituting with the actual values for the target database. Once the connection string has been entered, it must be successfully tested before the website will allow the command details to be configured.

SQL Server ODBC

Driver={SQL Server Native Client 11.0};Server=myServerAddress;Database=myDataBase;Uid=myUsername;Pwd=myPassword;/p>

SQL Server OLE DB

Provider=SQLNCLI11;Server=myServerAddress;Database=myDataBase;Uid=myUsername;Pwd=myPassword;

MySQL ODBC

Driver={MySQL ODBC 5.2 UNICODE Driver};Server=localhost;Database=myDataBase;User=myUsername;Password=myPassword;Option=3;

MySQL OLE DB

Provider=MySQLProv;Data Source=mydb;User Id=myUsername;Password=myPassword;

IBM DB2 ODBC

Driver={IBM DB2 ODBC DRIVER};Database=myDataBase;Hostname=myServerAddress;Port=1234;Protocol=TCPIP;Uid=myUsername;Pwd=myPassword;

IBM DB2 OLE DB

Provider=IBMDADB2;Database=myDataBase;Hostname=myServerAddress;Protocol=TCPIP;Port=50000;Uid=myUsername;Pwd=myPassword;

Command

The command is used to query information from the target database once a connection has been established. The command can be in the form of an SQL select statement (Text) or a stored procedure call.

Once the command has been entered, pressing the 'Test' button will execute the command on the target database. If successful, the 'Data Fields' tab will be enabled and will be populated with results of the command.

Data Fields

The data fields represent the data returned from the external database. The grid displays the resulting data from the test command with the index and field name of the columns returned.

The 'Display Name' is the name that will be displayed to Real-Time users when selecting external data to add to a tile. This is pre-populated with the field name returned from the database but can be overridden if required.

Once all display names have been updated as required, saving the external data source will make it available for Real-time Wallboard and Dashboard users.

9.1.6.5 Automatic Agent Logout

This feature provides a method to schedule the automated logging out of agents from one or more hunt groups on the telephone system. If agents forget to logout when leaving the office, call reporting statistics can be skewed and calls can be offered to agents that are no longer sat at their desk.

> Access to this feature is controlled by the ACD Reporting license.

Rule Details

Each rule has the following settings:

Name & Description

Give the rule a name and description that will uniquely identify it from other rules.

Hunt Groups

Select one or more hunt groups which the rule will fire against. Any agent logged into the hunt groups selected will be logged out when the schedule occurs.

> If no hunt groups are selected, agents will be logged out of ALL hunt groups when the schedule occurs.

Rule Schedule

The schedule controls when the agents are logged out of the configured hunt groups.

Start Date & Time

Specify the time and date the schedule will first run. The recurrence setting will then be used to evaluate all further executions of the rule.

End Date & Time

Optionally configure and end date and time for the schedule to stop executing.

Recurrence

Select how often the schedule should recur.

Day Selection

Select which days of the week the schedule should execute on. Any days not selected will be skipped by the recurrence.

9.1.7 Mitel 6900 Handset Support Overview

The MiVoice Office Application Suite is the core configuration server for Mitel's premium 6900 handset range when used on the MiVoice Office 250 telecommunications platform.

The 6900 phones operate as a SIP phone, connecting directly with the telephone system (or via MiVoice Border Gateway for Teleworkers) for audio and call control features. The MCS server acts as configuration server for the phones, providing the following features:

Administrative Features:

- Firmware Updates
- Feature Configuration
- Keymaps
- Centralised Background Images & Screen Savers
- Page Zone Management

End-User Features

- SIP Hot Desking
- Server based feature keys including; UCD, ACD, DND, Forwarding etc
- Presence Profile visibility and control
- Alarm Notifications
- Speed Dial and Intercom Directory Access

Licensing

Each 6900 handset that uses the MiVoice Office Application Suite as a configuration server will consume a license. There are two levels of license available:

- Basic, provides access to all 6900 server based functionality apart from specific softkeys.
- Enhanced, required to access specific softkeys -> CLI Change & Recording Pause / Resume.

If there are no licenses available when a handset connects to the MCS server, a licensing message will be displayed on the screen.

Enhanced Licences

Each handset requires a 'Basic' licence in order to be provided with configuration and keymap updates from the MCS. An additional 'Enhanced' licence is required to access some of the softkey features. Any handset that is associated with a user that has been assigned a Phone Manager Professional or Team Leader licence will automatically request an 'Enhanced' licence.

6900 Features

The following sections provide information on configuring various aspects of the support for 6900 handsets:

1. General Settings
2. Phones
3. Handset Firmware & Models
4. SIP Configuration
5. Keymap Profiles
6. Softkey Features
7. Configuration Profiles
8. Configuration Options
9. Image Handling

10. Screen Savers
11. SIP Hot Desking
12. Page Zones

In addition, there are some engineering guidelines available for the 6900 on the following subjects:

- Handset Rollouts
- Network Architecture & Resiliency
- SIP Hot Desking
- Teleworking with 6900 Handsets
- Multi-Node 6900 Installations

9.1.7.1 6900 Handset Models

The MCS server supports three different models of 6900 handset. The models supported are listed in the table below with a brief description of the difference in features:

Model No	Screen Size	Softkeys	Bluetooth
6920	320 x 240	• Softkeys - 18 • Top Softkeys - 20	No
6930	480 x 272	• Softkeys - 24 • Top Softkeys - 44	Yes
6940	800 x 480	• Softkeys - 30 • Top Softkeys - 48	Yes

Configuring 6900 Handset Models

The Model configuration page shows a list of models support and provides an edit form to configure the following properties:

- Firmware
- Keymap
- Configuration

Firmware

When a handset requests new firmware, the MCS will check the model to see which firmware should be provided. This allows a different firmware to be run on different models of handset if required.

> Firmware can be overridden at handset level if required. Please refer to the Firmware section for more information.

Keymap

Optionally, each model can have a specific keymap applied. When a handset requests a keymap, the *[Default]*, model and phone assigned keymaps are applied. For more information, please refer to the Keymap Profiles section.

Configuration

Optionally, each model can have a specific configuration applied. When a handset requests configuration, the

[Default], model and phone assigned configurations are applied. For more information, please refer to the Configuration Profiles section.

9.1.7.2 6900 Handset Phones

The 6900 Handset Phones section displays each physical handset that has been configured to use the MCS server as a configuration server.

If required, handsets can be added manually by pressing the 'New' button and filling out the required parameters. Otherwise, a the MCS will automatically add a new handset to this section the first time it sees a request from it.

Handset Information/Configuration

The following is a list of information and configurable options for each physical handset:

Parameter	Description
Model Number	This is the model number of the handset. Models 6920, 6930 & 6940 are currently supported.
MAC Address	This hardware address for the handset. It is used by the MCS to uniquely identify the handset. Note: To swap out a handset with another, the MAC Address of the handset can be updated.
IP Address	This displays the current or last known IP Address of the handset. If the handset is remote (Teleworker), this will display the address of the internal address of the MiVoice Border Gateway.
Status	This displays the current status of the handset. Possible states are: • Offline, the phone is not currently in contact with the MCS Server • No SIP, the phone is successfully connected to the MCS Server but is not connected to the telephone system. • Online, the phone is operating normally. Both SIP and Configuration connections are online.
Firmware	This displays the current the version of firmware that the handset is currently running.
Extension	This shows the Extension number of the SIP device on the telephone system that this handset is mapped to.
Keymap	This displays the name of the keymap profile assigned to the phone (if any).
Configuration	This displays the name of the configuration profile assigned to the phone (if any)
Mode	This displays the mode the phone is configured to run in. Possible modes include: • Not Initialised, the phone has not yet been assigned a SIP extension • Fixed, the phone has a fixed SIP extension assign. • Mixed, the phone has a fixed SIP extension but also allows Hot Desking

Last seen	Indicates when the server last had communication with the phone.
Programmable Key Modules (PKMs)	Each 6900 handset can have up to three programmable key modules connected. If a handset has PKMs connected, they will be displayed here.
Remote	Indicates whether the phone is currently remote.
Diagnostics	Displays whether or not the handset has diagnostics enabled or not
Effective Keymap	Select this option to see the combined keymap that will be sent to the phone (System, Model, Phone & User)

Rebooting Handsets

If a handset is not offline, the reboot button can be used to force it to restart. Restarting a handset is useful for forcing it to request new configuration files and firmware.

> ⚠ If any calls are in progress on the handset when it is rebooted, they will be cut off.

9.1.7.3 6900 Handset SIP Configuration

6900 handsets operate in SIP mode when connected to the MiVoice Office 250 telephone system. SIP extensions need provisioning on the MiVoice Office 250 and Cat-F licenses need providing for each 6900 phone.

For information on how to configure the SIP extensions on the MiVoice Office 250, please refer to the Softphone/6900 Support section.

9.1.7.4 6900 Handset Firmware

The MCS server provides 6900 series handsets with firmware updates as part of it's configuration server role. The firmware configuration page provides an interface to see which firmware files are currently loaded onto the system and provides a utility to upload firmware updates.

MCS can manage multiple versions of firmware at the same time. Having multiple versions of firmware allows new firmware to be evaluated on a subset of handsets and/or models before it is rolled out system wide.

The table on the 6900 Firmware configuration page shows the firmware currently loaded. The table shows the following information:

- Version, the version number of the firmware in the format 'x.x.x.x'
- Phone Types, a list of models which the system has this firmware version for

Managing Firmware

New Firmware

New firmware is automatically added to new releases of MiVoice Office Application Suite and are automatically installed when upgrading. If firmware is released outside of a MiVoice Office Application Suite release then it may be necessary to upload new firmware.

New firmware will be provided in the form of a ZIP file. The name of the ZIP will correspond to the version number of the firmware and there will be a firmware file inside the ZIP for each model of handset.

> Please speak to your system maintainer about getting access to firmware updates.

To upload a new zip file, press the 'Upload Firmware' button. Press the 'Choose Files' button and browse for the new firmware ZIP file. When the upload has completed, the new firmware files will be copied to the following location:

"[ProgramData]\Mitel\Mitel Communication Service\Net Store\Firmware"

The table should automatically refresh and show the new firmware has been updated.

Deleting Firmware

When old firmware is no longer required, it can be deleted from the system. To do this, select a firmware from the table, then press the 'Delete' button. Firmware can only be deleted if it is not currently assigned to a model of handset.

Rolling Out Firmware

Firmware can be assigned at two levels:

- Model
- Phone

By default, all phones will be supplied with the firmware that matches the model number unless the firmware version has been overridden at phone level. Overriding firmware at phone level can be useful for testing a new release on one or a subset of handsets before rolling it out system wide. To override firmware at phone level, edit the required phone from the 6900 Phones configuration page.

Handsets will request new firmware at the following times:

- During the start-up sequence
- Upon resync (if configured)

The resync process is controlled by the 'Auto Resync Mode' and 'Auto Resync Time' configuration options. If set, the handsets will request new configuration files and firmware at the configured time.

If auto resync is disabled, handsets will need to be rebooted to force them to request new firmware.

> Firmware is provided over https to all handsets accept in initial configuration when a 6900 handset with MiNET firmware requests and update over TFTP. For more information on the initial configuration and rollout of 6900 series handsets, please refer to the 6900 Engineering Guidelines.

9.1.7.5 6900 Handset Keymap Profiles

Keymap profiles are used to control the softkeys that are displayed on each handset. Once a key has been configured centrally via a keymap profile, it cannot be configured by the user.

Keymap profiles can be assigned to handsets in three different ways:

- Default Keymap, assigned to all handsets by default
- Model Keymap, assigned to all handsets of a specific model
- Phone Keymap, assigned directly to a phone or Hot Desk Device

When a handset is provided a keymap, the Default (system-wide) keymap and any model or phone keymaps are merged together. Keys set at model level will override any set at Default level and keys set at handset level will override those at model level.

Keymaps are not model specific, they can be assigned to any model of handset. This simplifies the process of having departmental keymaps for users with different model handsets. It also allows users to hot desk into any 6900 Handset and get their assigned keymap.

If there are more keys configured in the keymap than the handset allows, it will just show as many as is possible.

> Any softkeys that have not be configured using a Keymap Profile can be configured by the user, all other softkeys will be read-only to them. Users can program softkeys themselves from the User Keymaps section.

SoftKey Types & Locations

Each handset has three different types of key available:

- Softkeys, Run along the bottom of the screen
- Top Softkeys, Display in the main area of the screen
- Expansion Module Softkeys, If fitted with one or more programmable key modules (PKMs), like top softkeys but do not support images.

The softkey features available can differ depending on location. For example, Line keys cannot be programmed as Softkeys.

Depending on the handset model, there will be a different number of Softkeys and Top Softkeys available. Please refer to the 6900 Handset Models section for more information.

If more softkeys are configured than can fit on the handset's display, they will be paged out by the phone and one of the softkeys will become a screen-page button (not applicable to the 6940 where the touch screen allows navigation between pages without a screen-page button).

By default, the handset will compress any configured softkeys so that any blank entries are removed. For example, if a Top Softkeys 3, 6 & 8 are programmed in a keymap. The handset will render these in locations 3,4,5 (Top Softkeys 1 & 2 are reserved for Line keys by the handset) so that no spaces are displayed. This behaviour can be changed if required. Please refer to the Configuration Options section for more information

Editing Keymap Profiles

Each keymap profile has the following sections:

- General, Provide a description for the keymap to make it easily identifiable
- Softkeys, Configure any softkeys along the bottom of the handset
- Top Softkeys, Configure any softkeys in the main display area.
- PKM (1,2 & 3), Configure softkeys for any programmable key modules.

For each location tab (Softkeys, Top Softkeys, PKMs) there is a list of softkeys which are numerically ordered. To add a softkey, configure the following properties:

- Type, select the type of key to add to the handset
- Label, select the label that will display against the key (some labels are controlled by the software/handset)
- Value, this will be different depending on the key type

For information on the different softkey types available, please refer to the Softkey Features section.

> Use the 'Clone' button to quickly create a copy of a keymap profile that can then be edited rather than creating a new one from scratch.

Call States

For softkeys that run along the bottom of the phone's screen, a 'Call State' option can be selected. This controls when the softkey is displayed.

By default, when a softkey is added, it will always be displayed. If required, one or more of the following call states can be selected:

- Idle - The phone is not being used
- Connected - The current line is in an active call (or is on hold)
- Incoming - The phone is ringing
- Outgoing - The user is dialling a number, or the far-end is ringing
- Busy - The current line is busy because the line is in use.

For example, the 'Queue' softkey could be set to only display when the phone state is busy.

> The call states can be used in conjunction with the 'Collapsed Context User Softkey Screen' & 'Collapsed More Softkey Screen' configuration options to move softkey buttons onto the main screen when on a call.

Assigning Keymap Profiles

Once a keymap has been configured, it can be assigned to a Model or Phone/Hot Desk Device. To assign the keymap to a certain model, use the Models configuration area.

To apply a keymap to multiple phones and/or hot desk devices at the same time, press the 'Assign' button in the keymaps grid next to the keymap. A device selection form will then be loaded allowing multiple phones and/or hot desk devices to be assigned or removed from a keymap.

Any changes to a keymap or assignment will have an immediate effect on handsets that are online.

Enforced Softkeys

Some of the softkeys are essential to the operation of the handset. Where softkeys are essential, the MCS will automatically add them to a handset's keymap if they have not been added anywhere else.

Currently there are two types of key which are essential to handset operation:

Hot Desk Softkey

For handsets that allow hot desking or have hot desk devices currently logged in, the Hot Desk softkey is an essential key. If the Hot Desk key does not appear anywhere where it is required, one will automatically be added to softkey position 1. If there is another key programmed in this position, it will be overwritten.

Line 3 & 4 Softkeys

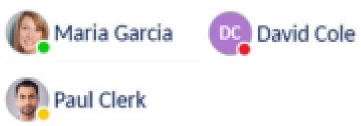
To control up to 4 calls on a 6900 handset from Phone Manager Desktop, softkeys for lines 1 to 4 are required. By default, all handsets are configured with softkeys for line 1 and 2. If there are no softkeys configure for lines 3 and 4, these will automatically be added to the last 2 topsoftkey positions available. If there are no topsoftkey locations available, the last two topsoftkeys will be overridden.

9.1.7.5.1 6900 Softkey Features

The following table lists all the different softkeys that are available to add to a 6900 handset. The features behind each softkey are either provided by the phone itself or by the MCS server.

> Phone based softkey features are processed locally on the phone, Server based softkey features are processed by the MCS server and will communicate to the server when pressed.

Softkey Type	Feature Description	Softkey Examples	Phone or Server
Account Code	Used to set optional accounts on any external call that is in progress at the handset. Parameter: Enter an account code or leave blank to prompt the user at runtime. Enter a comma separated list to give the user a choice at runtime.	OFF No call, no account code or account code does not match call ON Account code on call matches parameter	Server
Account Code Following	User to set account codes on all external calls made from the handset until the feature is toggled off. Parameter: Enter an account code or leave blank to prompt the user at runtime. Enter a comma separated list to give the user a choice at runtime.	OFF No account code following or account code following set does not match parameter ON Account code following set matches parameter	Server
ACD End Wrap	If there is an Agent ID logged on to the handset, this softkey will allow the user to end wrap-up status early if required. No parameters.	No in the Wrap-up state Agent in Wrap-up state	Server
ACD Toggle	Provides support to log ACD agents onto and of off the handset. Parameter: Enter a hunt group or comma separated list of hunt groups. Leave blank to provide the user a list of hunt groups the agent is a member of at runtime. Use * as the parameter to control all hunt groups without prompting the user. *Note: If an Agent ID has been assigned to the MCS user the phone is associated with, it will be pre-populated into the Agent ID dialog when the user press the ACD Toggle key.*	Logged Out Logged In/Free Busy Wrap-up	Server

Agent Help	Allows the user to invoke the Agent Help feature on the telephone system. No parameters.	OFF Agent help not in progress ON Agent help in progress	Server
BLF - Extension	Shows the status of an extension on the telephone system and provides one-click dialling. Parameter: Select an extension from the telephone system.	Idle Busy Do-not-disturb Wrap-up Offline	Server
BLF - Hunt Group	Shows the status of a hunt group on the telephone system and provides one-click dialling. Parameter: Select a hunt group from the telephone system.	Idle/Calls Ringing Calls Queuing No free agents Offline	Server
BLF - Trunk	Shows the status of a trunk on the telephone system and provides one-click access. Parameter: Select a trunk from the telephone system.	Idle Busy Offline	Server
BLF - User	Shows the unified status of a Phone Manager based on all their associated devices.User BLF softkeys will display a user's avatar image where possible and will show initials if there is no avatar.  Parameter: Select a MCS user.	Idle Busy Wrap-up Do-not-disturb	Server
Call History	Provides access to the Call History page on	Refer to the 6900 User Guide/Quick	Phone

	the local handset. No parameters.	Reference Guide.	
Caller's List	Provides access to the list of inbound callers on the local handset. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
CLI Change	Provides the ability to change the calling party number programmed against the handset on the telephone system. Parameter: Enter a CLI or comma separated list of CLIs for the user to choose from at runtime. Leave blank to allow the user to type in the CLI manually. ***Note: This softkey type requires an enhanced 6900 license on the MCS server.***	Caller ID on the phone does not match the parameter Caller ID on the phone matches the parameter	Server
Conference	Start a conference using the built in features of the handset. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
DEE On/Off	Toggles the Dynamic Extension Express feature of the extension in the telephone system No parameters.	Dynamic Extension Express is disabled Dynamic Extension Express is enabled	Server
Directory	Provides access to the built in directory features of the handset. This includes accessing the System Speed Dials & Intercom directory from the telephone system. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Discreet Ringing	Enables discreet ringing on the local handset. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Do-not-disturb	Shows status and provides access to control the DND status of the handset. Parameters: Selected a DND message from the list or let the user select at runtime. If no DND Text is provided, the user will be prompted at runtime. *Note: If enabled, it is advised that DND is controlled using Presence Profiles.*	Do-not-disturb is disabled Do-not-disturb is enabled	Server
Door Relay	Activate the door relay on the telephone system.	No status displayed	Server

	No parameters.		
Empty	Programs an empty key on the keymap. This is useful when the configuration for collapsing the keys is enabled. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Feature Code	Provides the ability to enter supported feature codes on the telephone system Parameter: Select the feature code to apply when the key is pressed. Only a limited number of feature codes are supported at this time.	No status displayed	Server
Forward	Provides control of the handsets manual forwarding on the telephone system Parameter: Select a manual forward type or let the user select at runtime. If no destination is provided, the user will be prompted at runtime.	OFF Local forward is disabled or does not match the softkey parameters ON Local forward is enabled and matches the softkey parameters	Server
Group Pickup	Shows the status of a hunt group on the telephone system and provides one-click pickup. Parameter: Select a hunt group from the telephone system.	Idle (When LED flashes, calls are ringing at group) Calls Queuing No agents free OFF Offline	Server
Hand Off/Pull	When using Dynamic Extension Express (DEE), this softkey can be used to push active calls from an internal extension and pull back calls currently active on an external DEE call. Calls that have been 'Pushed/Pulled' will divert back to alert the primary DEE device so that they can be answered again. No parameters.	OFF Feature Inactive ON Call is available to push/pull to the primary DEE extension	Server
Hook Flash	Provides access to invoke a hook flash on a SIP call. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone

Hot Desk	Provides access to SIP hot desking features and the ability to log into or log out off a handset. No parameters.	OFF No hot desk user logged in ON Hot desk user is logged in	Server
Intercom	Provides access to direct SIP paging to another 6900 handset. Parameter: Enter an IP address or an extension number of another 6900 handset (or SIP Hot Desk extension) If an extension number is entered, the MCS will dynamically swap this for the relevant IP address when the keymap is applied to the handset.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Line	Displays call activity on the handset and provides outgoing access. Parameter: Enter a line number from 1 to 24.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Mobile	Displays mobile call activity for any mobile phone connected via Bluetooth to the handset. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Night Mode	Toggle night mode on or off on the selected node. Parameter: Select a telephone system node from the list.	OFF Night mode is off for the configured node ON Night mode is on for the configured node	Server
Outgoing Access	Dials the outgoing access digit on the keypad to initiate an outgoing call. Parameter: Leave blank to dial the outgoing access digit or enter the number of a trunk/trunk group number.	No status displayed	Server
Paging (PBX)	Provides access to the page zones on the telephone system to page non-6900 handsets. Parameter: Enter a page zone extension number or leave blank to allow the user to select one at runtime. *Note: The parameter must be a page zone extension number and not a page zone id.*	No status displayed	Server
Paging (Phone)	Provides access to the SIP paging features of the handset to page other 6900 handsets. Parameter: Select a SIP Page Zone from the list.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone

Park/Pickup	Park or pickup calls from designated hunt groups or phantoms/devices on the telephone system. Parameter: Enter the number of a hunt group or phantom/device on the telephone system.	No call parked Call parked	Server
Phone Lock	Lock or unlock the phone. To unlock the phone, the user will need to know the PIN that has been locally configured. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Presence Profile	Shows the current active profile for the user and provides the ability to switch between profiles. No parameters. *Note: This feature requires the handset to be associated to an MCS user, either as a primary, secondary or DEE device.*	Label will display current profile selected.	Server
Queue	Toggle queue requests on and off. Queue requests can be requested when dialling someone. Once in place they can be cancelled at any time. No parameters.	No queue requested Queue requested	Server
Recording Pause / Resume	Pause or resume an a call recording that is in progress on a MiVoice Office Call Recorder or linked Xarios Call Recorder. No parameters. ***Note: This softkey type requires an enhanced 6900 license on the MCS server.***	No call Active call, not recorded Active call, recording paused Active call, recorded	Server
Reverse Transfer	Enables the reverse transfer feature so that the user can press an Extension/Hunt Group or User BLF key to pick up a call. No parameters.	OFF Reverse transfer mode disabled ON Reverse transfer mode enabled	Server
Speed Dial	Dial a number programmed behind the button. Parameter: Enter the number to be dialled by the handset when the key is pressed. A # can be used to indicate the end of the number to dial, commas and digits can then be used to dial DTMF on the call after it has been dialled. For example, 1300#,,1000# could be used to dial the conference bridge on extension 1300, pause and then enter 1000# as DTMF to log directly into a specific	Refer to the 6900 User Guide/Quick Reference Guide.	Phone

	conference.		
Speed Dial Conference	When on a call, conference in another number directly. Parameter: Enter the number to be dialled by the handset when the key is pressed.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
Speed Dial Transfer	Transfer a call straight to another number Parameter: Enter the number to be dialled by the handset when the key is pressed.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
System Speed Dial	Dials a speed dial bin configured on the telephone system. Parameter: Enter a speed dial bin number or leave blank to let the user choose at runtime.	No status displayed	Server
Transfer	Places a local call on hold to begin a transfer. No parameters.	Refer to the 6900 User Guide/Quick Reference Guide.	Phone
UCD	Toggle the handsets availability in any UCD hunt groups on the telephone system. No parameters.	OFF UCD calls disabled ON UCD calls enabled	Server

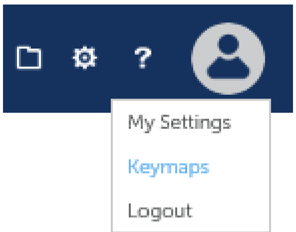
Any softkey implemented by the phone will continue to operate if the link to the MCS server is down. Any softkey implemented by the server will only work when the MCS server is online.

9.1.7.5.2 6900 User Keymaps

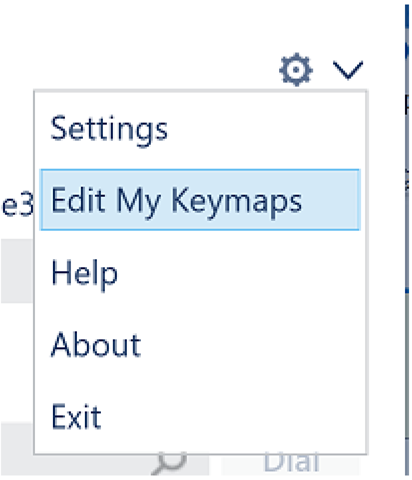
This section of the website provides a way for users to configure any available softkeys on any 6900 handsets they are using.

There are two ways for users to access the keymap configuration, directly through the MCS website or by using the hyper link from within their Phone Manager Desktop client:

Access through MCS:



Access through Phone Manager:



If a Phone Manager Desktop user is remotely connected to the MCS, they will not be able to access the User Keymaps page if the website port has not been forwarded through. User Keymap editing should be performed when on a local connection or through a firewall.

Editing User Keymaps

A list of 6900 extensions assigned to the user will be displayed in the grid. If there are no extensions displayed there are no 6900 handsets associated with the user's account, please refer to the Users & Business Units section for more information.

To edit a keymap, press the edit icon (✎) next to an extension. The keymap for that extension will be displayed. Any softkeys that have been configured centrally (either System, Model or Handset level) will be displayed on the keymap for the user to see but will be read-only. Any softkey that has not been configured centrally can be manually configured by the user.

For information on the features available, please refer to the 6900 Softkey Features section.

9.1.7.6 6900 Handset Configuration Profiles

Many of the features normally controlled by the telephone system (such as House Phone, Headset Mode, Time zone etc) are instead configured directly on 6900 series phones. Configuration profiles provide a way to configure the handsets centrally.

Configuration profiles can be assigned to handsets in three different ways:

- Default Configuration, assigned to all handsets by default
- Model Configuration, assigned to all handsets of a specific model
- Phone Configuration, assigned directly to a phone or Hot Desk Device

When a handset is provided a configuration, the Default (system-wide) configuration and any model or phone configurations are merged together. Configuration options set at model level will override any set at Default level and configuration options set at phone level will override those at model level.

Please refer to the Configuration Options section for information about each options available.

Default Configuration

To help with the initial rollout of handsets, the default configuration is pre-populated with commonly configured items.

The table below shows the options that are enabled by default and what they are configured as.

Option	Default	Description
Call Deflect	Enabled	Enables the display of the 'deflect' softkey when an inbound call is alerting the handset
Collapsed Context User Softkey Screen	Enabled	Causes Softkeys to collapse onto the first page if there is space when on a call
Collapsed More Softkey Screen	Enabled	Causes the More button to be removed if there is the exact number of keys to fit on the screen.
Collapsed Softkey Screen	Disabled	Causes Top Softkeys to retain their position and not move up to empty spaces
Conference/Transfer In Live Dial Mode	Live Dial Mode (With Dial Plan Matching)	When a user initiates a conference call or transfer, they hear a dial tone before dialling begins. The phone automatically dials out if the number matches the local dial plan or if it reaches the set digit timeout.
Goodbye Key Cancels Incoming Call	Disabled	When disabled, the 'Goodbye' key will instead clear the call in progress.
Date Format	Depends on region	• UK / Canada - DD MMM YYYY • US - MM DD YYYY
Idle Screen Mode	Secondary	Secondary mode displays the extension name and number on the main idle area of the screen.
Link Layer Discovery Protocol	Disabled	Disable Link Layer Discovery Protocol which is rarely used and speeds up the boot time of the handset not waiting for it.
Live Dialpad	Enabled	Enables real-time validation of the SIP dial plan so that calls are made without having to press the 'dial' key. This mimics normal MiNET/Digital handset behaviour.
Mask SIP Password	Enabled	Enables the enhanced security feature whereby a user's SIP account password is hidden/masked in the server.cfg and local.cfg files (downloaded from the IP phone's Web UI troubleshooting page for debug purposes).
Picture Refresh Timeout	1	Indicates the timeout in hours for a downloaded picture.
SIP Intercom Allow Barge In	Disabled	This stops the phone putting calls on hold when a page occurs.
SIP Intercom Type	Phone	This enables the 6900 intercom feature (direct page)
Time Format	Depends on region	• UK / Canada - HH:mm • US - hh:mm
Time Zone Name	Depends on region	• Canada - CA-Eastern • UK - GB-London • US - US-Eastern

Restricted Configurations

Some of the configuration options that are available on the handsets are not accessible through a configuration profile. These are designated as 'Restricted' options because they are provided to the phone automatically by the MCS server and are key to the normal operation of the phone in conjunction with the MCS server.

The following options are restricted and cannot be changed by profile or manually on the phone:

Area	Option	Description
SIP Configuration (Device)	SIP Auth Name	These settings are automatically populated with the relevant information based on the handset's fixed extension or logged in hot desk device. • 'Display Name' is set to the extension number. • 'Screen Name' is set to the mapped user's name unless there is no user, in which case it is set to the extension description. • 'SIP Vmail' is set to the extension's message retrieval extension
	SIP Display Name	
	SIP Password	
	SIP Screen Name	
	SIP Screen Name 2	
	SIP User name	
	SIP Vmail	
SIP Configuration (Server)	SIP Proxy IP	These settings are automatically populated with the SIP configuration details for the node of the handset's fixed extension or logged in hot desk device. This information can be configured against the relevant node in the Phone Systems section.
	SIP Proxy Port	
	SIP Registrar IP	
	SIP Registrar Port	
	SIP Registration Timeout Retry Timer	30
	SIP XML Notify Event	Enabled
Configuration Server	Firmware Server	Set to the 6900 Handset Server Address
	Image Server URI	Set to the 6900 Handset Server Address
	Download Protocol	https
	Https Path	config
	Https Port	8202
	Https Server	Set to the 6900 Handset Server Address
	Https Validate Certificates	Enabled
	Upload System Info Server	Set to the 6900 Handset Server Address
	Web Interface Blacklist Duration	0
	XML Application Post List	Set to the 6900 Handset Server Address
Phone UI	Idle Screen Avatar	Set to enabled to show the user's profile image on the handset
	Softkey Selection List	Limits the softkeys the user can configure through the UI: *speeddial,lcr,speeddialxfer,speeddialconf,directory,callers,redial,conf,xfer,icom,phonelock,paging,discreetringing,callhistory,empty*
Diagnostics	Log Module XML	If Diagnostics are enabled against a handset in the 6900 Phones section, this will be enabled.
	Log Server IP	If Diagnostics are enabled against a handset in the 6900 Phones section, this will be set to the 6900 Handset Server Address, either local or remote. Note: For logging to operate, the 6900 Handset Server address must be an IP Address, not a DNS name.
	Log Server Port	514
Action URIs	Action URI Connected	Actions URIs configure the phone to update the server with information about call events. This is required for Phone Manager to be able to track phone status and provide call control
	Action URI Incoming	
	Action URI Disconnected	
	Action URI Registered	
	Action URI	

	Registration Event	
	Action URI Offhook	
	Action URI Onhook	
	Action URI Outgoing	
	Action URI Startup	
	Action URI XML SIP Notify	
Directories	Directory 1	This directory is automatically populated with the telephone system intercom directory.
	Directory 1 Name	
	Directory 1 Enabled	
	Directory 2	This directory is automatically populated with the telephone system speed dial directory for the node the handset is on.
	Directory 2 Name	
	Directory 2 Enabled	
Dial Plan	SIP Dial Plan	This option is automatically populated with information from the Dial Plan configured on the MCS unless it has been overridden in the 6900 General Settings.
Paging	Paging Group Listening	This option is automatically populated with multicast addresses based on which pages zones (6900 Handset Page Zones) that handset has been placed in. For more information, please refer to the 6900 Paging section.
Phone Lock	XML Lock Override	This option is automatically set to 1 to ensure that the configuration server can post softkey & configuration updates to the handsets even when they are locked.

9.1.7.6.1 6900 Handset Configuration Options

The following table outlines the different 6900 handset configuration options that are made available through configuration profiles. Not all the configuration options available on the handsets are directly supported by the MCS server. For information on how to apply a configuration option which is not directly supported, please refer to the Custom Configuration Options section.

> Some configuration options require a reboot of the phone to take effect. Please refer to the table below for information about specific options.

> For detailed information about each configuration option, please refer to the Mitel 6900 SIP Administration Guide

Option	Description	Requires Phone Reboot
Admin Password	Allows you to set a new administrator password for the IP phone.	No
Audio Mode	Allows you to configure how the "handsfree" button on the IP phone operates.	No
Auto Resync Mode	Enables and disables the phone to be updated automatically once a day at a specific time in a 24-hour period. This parameter works with TFTP, FTP, and HTTP servers.	No
Auto Resync Time	Sets the time of day in a 24-hour period for the IP phone to be automatically updated. This parameter works with TFTP, FTP, and HTTP servers.	No
Background Image	Specifies the location of the background image for the idle screen on phones.	No
Backlight Mode	Allows you to turn the backlight on the LCD, Off (always off) or Auto. The “Auto” setting sets the phone to turn off the backlight after a period of inactivity. You can set the amount of time before the backlight goes off using the “Backlight on Time” option (“bl on time” parameter).	Yes
Backlight On time	Allows you to set the amount of time, in seconds, that the backlight stays ON before turning OFF because of inactivity.	Yes
Brightness Level	Specifies the brightness level when the phone is active.	Yes
Call Deflect	Enables or disables the ability to deflect a call to another number during a ringing state.	Yes
Call Hold Reminder	Enables or disables the reminder ring splash timer to start as soon as you put a call on hold (even when no other calls are active on the phone). When enabled, the phone initiates a reminder ring splash periodically for the single call on hold. When disabled, no reminder ring splash is audible.	Yes
Call Hold Reminder During Active Calls	Enables or disables the ability for the phone to initiate a continuous reminder tone on the active call when another call is on hold. For example, when the call on Line 1 is on hold, and the User answers a call on Line 2 and stays on that line, a reminder tone is played in the active audio path on Line 2 to remind the User that there is still a call on hold on Line 1. When this feature is disabled, a ring splash is heard when the active call hangs up and there is still a call on hold.	Yes
Call Hold Reminder Frequency	Specifies the time interval, in seconds, between each ring splash sound on the active line. For example, if a call comes into Line 1, and then a call comes into Line 2 and you answer Line 2, Line 1 is automatically placed on hold. While on the active Line 2, after 7 seconds, a ring splash audio sounds on the line reminding you that the call on Line 1 is still on hold (determined by the “call hold reminder timer” parameter), and then the ring splash is heard again after 60 seconds (determined by this parameter).	Yes
Call Hold Reminder Timer	Specifies the time delay, in seconds, that a ring splash is heard on an active call when another call was placed on hold. For example, if a call comes into Line 1, and then a call comes into Line 2 and you answer Line 2, Line 1 is automatically placed on hold. While on the active Line 2, after 7 seconds, a ring splash audio sounds on the line reminding you that the call on Line 1 is still on hold. This timer begins to increment after Line 2 is answered.	Yes

Call Transfer Disabled	Enables or disables the Xfer key on the IP phone. If this parameter is set to false, the key is active and can be pressed by the user. If this parameter is set to true, pressing the Xfer key is ignored.	No
Call Waiting	Allows you to enable or disable Call Waiting on the IP phone.	Yes
Call Waiting Tone	Enable or disables the playing of a call waiting tone when a caller is on an active call and a new call comes into the phone.	Yes
Call Waiting Tone Period	Specifies the time period, in seconds, that the call waiting tone is audible on an active call when another call comes in. When enabled, the call waiting tone plays at regular intervals for the amount of time set for this parameter.	Yes
Collapsed Context User Softkey Screen	When enabled, user configured softkeys on the applicable phones will collapse and fill in any unused softkeys starting on the first page of softkeys during the following states: • outgoing • ringing • connected • hold	Yes
Collapsed More Softkey Screen	Controls how softkeys are displayed on the 6920, 6930, and 6940 IP phones' screens when the number of softkeys configured matches the exact number of softkey buttons on the phone.	Yes
Collapsed Softkey Screen	Enables or disables the 6920/6930/6940 from collapsing the softkeys to remove blank keys	Yes
Conference Disabled	Enables or disables the Conf key on the IP phone. If this parameter is set to 0 - False, the key is active and can be pressed by the user. If this parameter is set to 1 - True, pressing the Conf key is ignored.	No
Conference/Transfer In Live Dial Mode	Enables/disables support for live dial mode when initiating a conference call or transfer.	Yes
Date Format	This parameter allows the user to change the date to various formats.	No
Directory Digits Match	Specifies how many digits of an incoming call's phone number the phone will take into consideration when performing a directory lookup.	Yes
Display DTMF Digits	Enables and disables the display of DTMF digits when dialling on the IP phone.	Yes
DST Config	Enables/disables the use of daylight savings time.	No
Goodbye Key Cancels Incoming Call	Enable or disables the behaviour of the Goodbye Key on the IP phone.	Yes
Idle Screen Font Color	Specifies the font colour of the date, time, and status message text on the home/idle screen of the 6920, 6930, and 6940 IP phones.	Yes
Idle Screen Mode	Used to switch between the two Home/Idle screen modes. The primary screen mode provides users with a larger date and time and displays the Screen Name ("sip screen name") parameter beside the line number in the top status bar. The secondary screen mode displays both the Screen Name and Screen Name 2 ("sip screen name 2") parameters above the smaller, repositioned date and time.	Yes

Inactivity Brightness Level	Specifies the brightness level when the phone is inactive.	No
Input Language	Allows you to specify the language to use for inputs on the IP Phone. Entering a language value for this parameter allows users to enter text and characters in the IP Phone UI and in XML applications via the keypad on the phone (or for the 6940 on-screen keyboard), in the language(s) specified.	Yes
Language	The language you want to display for the IP Phone UI.	No
Line Show Caller Id	Enable or disable the caller ID display on the line and mobile softkeys.	Yes
Live Dialpad	Turns the “Live Dialpad” feature ON or OFF. With live dial pad ON, the IP phone automatically dials out and turns ON Handsfree mode as soon as a dial pad key or softkey is pressed. With live dial pad OFF, if you dial a number while the phone is on-hook, lifting the receiver or pressing the Speaker/Headset key initiates a call to that number.	No
Link Layer Discovery Protocol	Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLD-MED) on the IP Phone.	Yes
Map Conf Key To	Sets the Conf key as a Speed Dial key if a value is entered for this parameter. If you leave this parameter blank, the Conf key returns to its original functionality.	No
Map Redial key To	Sets the Redial key as a Speeddial key if a value is entered for this parameter. If you leave this parameter blank, the Redial key returns to its original functionality.	No
Mask SIP Password	Enables the enhanced security feature whereby a user’s SIP account password is hidden/masked in the server.cfg and local.cfg files (downloaded from the IP phone’s Web UI troubleshooting page for debug purposes).	Yes
Minimum Ringer Volume	Specifies the minimum ringer volume level.	Yes
Mobile Contacts Enabled	Enable or disable the mobile contacts import.	Yes
Mobile Contacts Name	Override the default folder name “Mobile Contacts” to provide a customized name to the mobile contacts folder.	Yes
Options Password Enabled	Enables or disables password protection of the Options key on the IP phone. If enabled, upon pressing the Options key, a user has to enter a password at the IP phone UI.	No
PC Port PassThru Enabled	Enables or disables the PC port.	Yes
Picture Refresh Timeout	Indicates the timeout in hours for a downloaded picture.	0
Priority Non-IP	Specifies the priority value for non-IP packets.	Yes
Proximity Lock	Enable or disable phone automatic lock on proximity detection.	Yes
Proximity Lock Delay	When proximity lock is enabled, delay after proximity event detection before locking the phone.	Yes

Proximity Unlock	Enable or disable phone automatic unlock on proximity detection.	Yes
Proximity Unlock Delay	When proximity unlock is enabled, delay after proximity event detection before unlocking the phone.	Yes
Redial Disabled	Enables or disables the Redial key on the IP phone. If this parameter is set to 0 - False, the key is active and can be pressed by the user. If this parameter is set to 1 - True, pressing the Redial key is ignored, and the dialled number is not saved to the "Outgoing Redial List".	No
Ring Audibly Enable	Enables/disables the feature whereby the ring tone of an incoming call is played through the IP phone’s speaker if a user is on an active call.	Yes
Ringback Timeout	Specifies the timeout period (in seconds) before the phone terminates the call. For outgoing calls, the originating phone will send a SIP CANCEL to stop the ringing at the destination phone after the timeout expires. For incoming calls, the terminating phone will send a SIP 486 Busy Here to stop the ringback at the originating phone after the timeout expires.	No
Ringtone	Globally sets the type of ring tone on the IP phone. Ring tone can be set to one of 15 pre-defined rings (excluding silence) or one of 8 custom ringtones.	No
Screensaver Time (seconds)	Specifies the amount of time (in seconds) the phone must be idle before the 6920/6930/6940 IP phone’s screen saver initiates.	Yes
Screensaver Background Image	Specifies the location and file name of the background image for the screen saver on 6920, 6930, and 6940 phones.	Yes
Screensaver Refresh Timer (minutes)	Specifies the interval (in minutes) when the screen saver background image is refreshed.	Yes
Simplified Options Menu	Allows you to enable a simplified options menu or enable the full menu on the IP Phone UI.	Yes
SIP Allow Auto Answer	Enables or disables the IP phone to allow automatic answering for an Intercom call. If auto-answer is enabled on the IP phone, the phone plays a tone to alert the user before answering the intercom call. If auto-answer is disabled, the phone treats the incoming intercom call as a normal call.	No
SIP Auto-Dial Number	Globally or on a per-line basis, specifies the SIP phone number that the IP phone autodials when the handset is lifted from the phone cradle. An empty (blank) value disables autodial on the phone.	No
SIP Auto-Dial Timeout	Globally or on a per-line basis, specifies the time, in seconds, that the phone waits to dial a pre-configured number after the handset is lifted from the IP phone cradle.	No
SIP Dial Plan Terminator	Specifies whether or not pressing the hash/pound (i.e. "#") key, while performing an outgoing call on an open line, should be sent as %23 to the proxy in the dial string or if the key should be used as a dial plan terminator (i.e. dials out the call immediately).	No
SIP Digit Timeout	Represents the time, in seconds, between consecutive key presses on the IP	No

	phone. The default for this parameter is 4 seconds. If you press a key on the phone and wait 4 seconds before pressing the next key, the key times out and cancels the digit selection. You must press consecutive keys before the timeout occurs.	
SIP Early Media Mute Mic	Enables or disables the microphone while in early media.	No
SIP Intercom Allow Barge In	Enable or disables how the phone handles incoming intercom calls while the phone is on an active call as well as how the phone handles multicast paging calls while the phone is in a dialling state.	No
SIP Intercom Line	Specifies the line for which the IP phone uses the configuration from, when making the Intercom call. The IP phone uses the first available line for physically making the call but uses the configuration from the line you set for this parameter.	No
SIP Intercom Mute Mic	Enables or disables the microphone on the IP phone for Intercom calls made by the originating caller.	No
SIP Intercom Type	Determines whether the IP phone or the server is responsible for notifying the recipient that an Intercom call is being placed.	No
SIP Intercom Warning Tone	Enables or disables a warning tone to play when the phone receives an incoming intercom call on an active line.	No
SIP RTP Port	Indicates the port through which the RTP packets are sent. This value must specify the beginning of the RTP port range on the gateway or router. The RTP port is used for sending DTMF tones and for the audio stream. Your network administrator may close some ports for security reasons. You may want to use this parameter to send RTP data using a different port.	No
SIP Update Caller Id	Enables or disables the updating of the Caller ID information during a call.	No
Suppress DTMF Playback	Enables and disables suppression of DTMF playback when a number is dialled from the softkeys or programmable keys.	No
Suppress Incoming DTMF Playback	Suppress playback of both SIP INFO and RFC2833 DTMF tones.	Yes
Tagging Enabled	Enables or disables VLAN on the IP phones.	Yes
Time Format	This parameter changes the time to 12 hour or 24 hour format. Use “0” for the 12 hour format and “1” for the 24 hour format.	No
Time Server 1	This parameter allows you to set the IP address of Time Server 1 in dotted decimal format.	No
Time Server 2	This parameter allows you to set the IP address of Time Server 2 in dotted decimal format.	No
Time Server 3	This parameter allows you to set the IP address of Time Server 3 in dotted decimal format.	No
Time Server Disabled	Enables or disables the time server. This parameter affects the time server1, time server2, and time server3 parameters. Setting this parameter to 0 allows the use of the configured Time Server(s). Setting this parameter to 1 prevents the use of the configured Time Server(s).	No
Time Zone Minutes	The number of minutes the timezone is offset from UTC (Coordinated Universal Time). This can be positive (West of the Prime Meridian) or negative (East of the	No

	Prim Meridian). Eastern Standard Time (EST) has a value of 300 which is the default.	
Time Zone Name	This parameter allows you to set the time zone code or customize the time zone for their area as required.	No
Tone Set	Globally sets a tone set for a specific country.	No
User Password	Allows you to set a new user password for the IP phone.	No
VLAN Id	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 0 (LAN port).	Yes
VLAN Id Port 1	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 1 (PC port).	Yes
Web Interface Enabled	Specifies whether or not to disable the web user interface.	Yes

Custom Configuration Options

To support configuration options that might be added to the phones in the future (and ones that have not been added to the configuration profile template), it is possible to add custom entries to a configuration profile.

To do this, select the 'Custom...' option from the list when adding an option to a configuration profile.

When this is selected, a 'Key' as well as a 'Value' is requested. Enter in the required values and then save the option down.

9.1.7.7 6900 Handset Images

Mitel 6900 series handsets have the ability to display background images and screen savers. Both of these types of image can be customised as required.

Handset images can be created on the server and then assigned to phones as a background image or screen saver through a Configuration Profile.

Adding / Editing Handset Images

To create or edit a handset image on the server, an image file for each Model type must be provided. The image sizes for the models currently supported are shown in the table below:

Model No	Screen/Image Size in Pixels (Width x Height)
6920	320 x 240
6930	480 x 272
6940	800 x 480

Any images file uploaded must also have the following properties:

- JPEG format
- 24 or 32bit depth
- Less than 1MB in size

To add a handset image, press the 'New' button and enter a unique description into the window that appears. Upload images for all handset models and then press 'Save'.

Background Images

To use a handset image as a background image, the configuration option 'Background Image' must be used. Edit or create a new configuration profile, add a new configuration option for 'Background Image' and then select the handset image from the list provided. If applied to the *[Default]* configuration profile, the background image will display on all phones. Background images can then be overridden in specific configuration files if required for different departments etc.

If a dark image is provided, it may not be possible to read the extension number, time and other idle screen properties. If this is the case, the 'Idle Screen Font Color' configuration option can be used.

> Background images only appear on the handset while it is idle.

> Background images can be useful for showing hot desk status. By configuring a different images for fixed phones and hot desk phones, user will be able to see from a distance which phones are free to logon to.

For information on using handset images in screen savers, please refer to the 6900 Screen Saver section.

9.1.7.8 6900 Handset Screen Saver

Each 6900 handset by default runs a local screen saver with pre-loaded images. using Handset Images uploaded to the MCS, it is possible to customise the screen saver. Screen savers configured on the MCS can be applied to handsets using Configuration Profiles.

Creating / Editing Screen Savers

A screen saver is a group of one or more handset images. Before screen savers can be created, the images required must already have been uploaded through the Handset Images configuration section of the MCS website.

To create a new screen saver, press the 'New' button then give enter a unique description in the form that appears.

Press the plus icon to the right of the Images property and select an image from the context menu. Repeat this process adding as many images as needed. If required, the same image can be added more than once. when all the images required have been added, press the 'Save' button.

To apply the screen saver to a handset, create a new Configuration Profile or edit an existing one. Add a new configuration option and select 'Screen Saver Background Image'. Select a screen saver from the list provided then save the option and profile.

Screen savers applied in the *[Default]* configuration profile will apply to all handsets.

The following configuration options can be used to control how the screen saver appears on the handsets:

- ScreenSaver Time, time in seconds before the screen saver appears on the phone
- ScreenSaver Refresh Timer, time in minutes for the phone to switch between images in the screen saver

If required, different screen savers can be applied to different handsets / models by using multiple configuration profiles.

9.1.7.9 6900 Handset Hot Desking

The MCS server provides a SIP Hot Desking feature specifically for 6900 series handsets. This differs from the existing MiVoice Office 250 Hot Desking and Agent Hot Desking.

SIP Hot Desking allows users to logon to any 6900 handset that has hot desking enabled (even ones on other nodes*). Once logged in, the handset becomes their own, all keymaps, configuration options and SIP configuration gets transferred to the target handset.

For information on configuring a SIP Hot Desking implementation, please refer to the 6900 Engineering Guidelines.

> * SIP Hot Desking is supported across nodes if all 6900 handsets are controlled by the same MiVoice Office Application Suite.

Managing SIP Hot Desk Phones

The hot desking configuration section displays all SIP hot desk phones that have been configured on the system.

Each hot desk phone has the following properties:

- Device Number, the SIP device on the telephone system
- PIN, the number used by the user when logging on and off
- Keymap Profile, a keymap profile to apply when logged on (Optional)
- Configuration Profile, a configuration profile to apply when logged on (Optional)

To add a new hot desk phone, press the 'Add' button. In the form that appears, enter the number of the SIP device on the telephone system to configure as a hot desk phone (the device picker will filter out any SIP device which are already have a fixed mapping to a handset).

Once a hot desk phone has been created, it can be used to logon to any handset that has been enabled for accepting hot desk logons. Please see the 6900 Handset Phone section for more information.

The effective keymap option can be used to see the combination of hot desk keymap and user keymap. The actual keymap that gets sent to the phone will differ depending on the phone the hot desk device is logged into.

> To login to teleworker phones, SIP Hot Desk phones must also be configured on the MiVoice Border Gateway. Please refer to the Teleworker section of the 6900 Engineering Guidelines for more information.

> Each SIP extension which is to be used as a SIP Hot Desk phone must be configured on the PBX and MCS as any other Softphone/6900 would be. Please refer to the Softphone/6900 Support section for more information.

9.1.7.10 6900 Handset Phone Page Zones

6900 series handsets have a built in paging facility that uses IP multicast to broadcast RTP from one handset to multiple handsets at the same time.

The 6900 Paging section provides an interface for creating one or more 'Page Zones' that can be used to page between groups of handsets.

Due to the nature of IP multicast, 6900 handset paging can only be used where the handset are on the same network and will receive the multicast packets.

> As well as multicast paging, 6900 handset supports direct point to point paging via the 'Intercom' softkey. Please refer to the Softkey Features section for more information.

> 6900 Handset Page Zones are separate to the page zones configured on the telephone system. 6900 handsets can access telephone system page zones to page MiNET and Digital handsets, but this cannot be done in reverse.

Page Zones

Each page zone created requires three properties:

- A list of handsets that will listen to this address and port combination
- An IP multicast address (calculated from the Base Paging Multicast address)
- A port number (uses the Base Paging Port number)

In normal use the IP address and port are configured automatically by the system and will not need to be altered. If they do need to be altered they can be amended under the Advanced Options.

How the multicast address is calculated for each page zone

The 'Base Paging Multicast Address' is used as the IP address for the first page zone created. Every time a page zone is added, this is incremented by one to use for the next page zone IP address. If a page zone is deleted the IP address will not be re-used. This means if you have 10 paging zones they will use (by default) IP addresses 224.0.0.150-224.0.0.159. If you delete and add a new one it will use 224.0.0.160.

> The default base paging multicast address is configured to 224.0.0.150.
>
> The base address may need to be changed if there is other equipment on site using multicast addresses is the range from the base address up to the number of paging zones you created. The valid range of IP multicast addresses is: 224.0.0.0 to 239.255.255.255.

> The default base paging port is 33100. This is used for all paging zones. The port number has a valid range of 1 to 65535.

Configuring Page Zones

To add a new page zone, press the 'Add' button. On the form that displays enter a unique description. (To override the automatically generated multicast address at this time, tick the Advanced Options and enter an IP multicast address E.g. 244.0.0.3).

Once a page zone has been created, the 'Apply' icon can be used to select the phones that will be configured to listen on this address/port combination.

> Pages cannot be sent to hot desk phones, only fixed phones. Pages will still be sent to a base phone if a hot desk phone is logged in.

At this point, the page zone has been created and the phones have been configured to listen. A page button will need to be added to the keymap of any handset required to make pages. Please refer to the Keymap Profile section for more information.

> Page Zones can not be sent to the handsets in real-time. Handsets will not start to receive pages until they are rebooted. If a Handset is removed from a page zone it will continue to receive pages on that zone until it is rebooted.

> A Handset can be in a maximum of 5 Page Zones. If it is added to more than 5 Page Zones then additional zones will be ignored.

9.1.7.11 6900 Handset General Settings

The following settings relate to some of the interaction between the MCS and any Mitel 6900 Handsets.

Setup PIN

The setup PIN is used to when rolling out 6900 handsets. It provides access to the setup dialog which allows an engineer to configure a newly installed 6900 handset and link it to a SIP device on the telephone system. The PIN can be configured to be any combination of keypad digits.

*Default: ****

Send DND Notifications

When 6900 handsets make calls to other extensions (MiNET, Digital, SIP or Analogue) that are in DND, they show a 'Busy' message on the screen and do not give the caller any information about the DND state.

MCS provides the DND (and Presence information if relevant) to the caller so that they can see why they are receiving a busy response to the call.

Default: Enabled

> The timeout on the Toaster style notification is not currently configurable.

Send Hunt Group Camp-on Notifications

When calls are queuing at ACD hunt groups, MCS can notify logged in members that there are calls waiting.

This feature works on ACD hunt groups only. This is a system-wide feature currently and cannot be enabled/disabled on a per hunt group basis.

Default: Enabled

> The timeout on the Toaster style notification is not currently configurable.

Show Chat Notification Preview

When enabled, a preview of the chat message received will be displayed in the notification toaster that displays on the 6900 phone.

Default: Disabled

> Chat notifications will appear on the phone even when it is locked.

Override Dial Plan

The MCS server will provide each 6900 handset with a dial plan based on the Dial Plan configured on the server. This dial plan is designed to allow the user to dial internal numbers, external numbers and service codes (including emergency numbers). The dial plan that is automatically sent to the handset can accommodate 3 & 4 digit dialling and will automatically workout the length of internal extensions based on the devices configured.

> If 3 digit dialling is required, ensure all internal extensions that being with the same number are the same

length. For example, for 3 digit dialling of extensions beginning 1, ensure all extensions beginning 1 are 3 digits long. This includes the built in modem extension.

In addition, the dial plan is designed so that the user does not need to enter the outgoing access code, it will automatically be entered for them when the dial plan detects an external number has been entered.

To manually assign a dial plan, enable the override and enter the dial plan required.

Default: Disabled

The outgoing access code will only be automatically entered if the external number being dialled starts with the toll digit. To dial numbers without the toll digit, the outgoing access code must still be entered.

The default Dial Plan for dialling any number is 'x+#|xx+*'

The Live Dialpad and SIP Dial Plan Terminator can be used to force the phone to evaluate the dial plan after every digit is entered and dial automatically when a match is made. Please refer to the Configuration Options section for more information.

Please refer to the 6900 Series Administration Guide for information on 'sip dial plans' and how to configure them.

By changing the Dial Plan passed to the phones, it is possible to prevent the handset from being able to make emergency calls. Ensure that all dial plan changes are thoroughly tested before rolling out.

Enable SRTP on Remote Handsets

When enabled, the MCS server will instruct any remote 6900 handsets to use SRTP for audio connections back to a MiVoice Border Gateway.

For more information on enabling SRTP, please refer to the 6900 Handset Engineering Guidelines.

If SRTP is not enabled on both the MBG configuration and the MCS configuration then calls will fail. The handsets will be able to make calls but not receive them.

Default: Disabled

Auto Detect Non-Internal Addresses as Remote

When enabled, the system will class any handset that does not have an IP address in the range 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16 as being a remote handset.

Handsets that are connecting through a MiVoice Border Gateway (MBG) will show up with internal addresses. To correctly identify these as remote, the internal address(es) of the MBG will need to be configured in the Phone Systems section.

Default: Enabled

Send Phone System Alarms to Admin Phones

When enabled, any phone system alarms will automatically be send to Mitel 6900 Handsets that have been configured as Administrator on the telephone system.

Default: Enabled

For more granular control over which alarms get sent to handsets, use the Alarm Notification feature.

Call Mode for Softkey Screens

This setting controls the behaviour of the phone if a call starts alerting when the user is in a softkey screen (changing presence or DND for example). If set to 'Notify via Toaster', the user will be left in the softkey screen but will be notified of the call via a toaster message. If set to 'Call Overrides Softkey', the softkey screen will be closed down and the call details screen will be displayed.

Default: Notify via Toaster

Display Voicemail Notification on User BLF Softkeys

When enabled, the number of new voicemails notifying a user will be displayed on any User BLF keys that are configured for the user on other phones.

Default: Disabled

Use HTTPS for Local Phone Softkeys

By default, all phones are configured to use HTTPS for softkey requests made to the MiVoice Office Application Suite server. This adds an overhead in processing time to each softkey press. Disabling HTTPS on softkey press can improve the user experience and reduce the processing overhead. This option only applies to local phones, not remote.

Default: True

> HTTPS will still be used for configuration updates if disabled for softkey requests.

9.2 Site Settings

Overview

The site level configuration settings are configured from here. The Site settings are accessed from the '⚙' -> Site Settings section and provides access to the following site-wide settings.

Setting	Description
Site License	This provides details of the license that has been activated for this site.
Users & Business Units	The configuration of Users & Business Units.
Phone Systems	This enables the connection to the PBX to be configured.
Dial Plan	This configures the dial plan rules that are used when making calls and controls any formatting rules that need to be use on the outside numbers.
Custom Tags	This configures the custom tags for adding additional info to call records
Email & SMTP	This configures the email and SMTP settings used to send out emails.
Database Maintenance	This configures the maintenance and backup schedules used.
Network Shares	This configures the Network Shares for transferring data to and from various parts of the solution.

9.2.1 Site License

Overview

Licensing is controlled via a software based Activation key. The server that performs the licensing role requires it own licence key that is tied to a MAC address on the server and the site is assigned a unique "Site ID". The licence key needs to be activated via the licensing portal before it can be used (online and offline activation is supported).

Server Vs Site

The architecture of the Communication Service software supports scaling by introducing the concept of Roles for servers. It is theoretically possible therefore that multiple physical (or virtual) servers could combine to form the "Site" e.g. One server could be used as a dedicated Web server whilst a separate server could perform the remainder of the roles such as Database and Application Server.

Critically, one of the roles is licensing. Since it's possible that in a multi-server configuration only one server can perform the licensing role, the licence configuration is visible both in Site Settings -> Site License and in Servers Settings -> License sections for the server performing that role. In the vast majority of cases one server will perform ALL roles.

This section displays the site wide licences that are activated on the system.

Each licensed feature will either have a green tick to indicate that this is enabled or a red cross if it is disabled. Whilst navigating the user interface, any features that are not licensed have a locked icon next to their configuration section. The unlicensed feature can still be configured but it will not be able to be used until a license has been obtained.

This view of the licence will report which server is running the licence, the site ID, which features are licensed and for any licences that are user based, both the licensed limit and the quantity of users consuming that licence class.

> Activating, De-Activating and updating (upgrading) licensed features are performed in the Servers Settings -> License section.

9.2.1.1 License Overview

The MCS license contains information about all the different features that can be used on the system. The following section outlines all the licenses available and how they can be used.

License Details

The properties listed under this section uniquely identify the license. If the original license certificate provided with the software is lost, it is advisable to make a note of the Site ID and Serial number of the software in case of hardware failure.

Licensed To

The name provided during installation. This is usually the company name and cannot be updated post installation.

Site ID

The unique ID for this license.

> To obtain the serial number for the solution as well, press the *Manage License* button to navigate to the Site License page.

Application Record ID

This is the application record ID that was provided on installation. This should be the application record ID for the telephone system the MCS is connected to.

Licensed Version

This shows the version number the software is currently licensed for. If there is a valid SWAS contract in place and a newer version of software is available, a message will display in green indicating an updated version can be applied.

PBX

This should show MiVoice Office 250, the MCS will not currently work on other telephone systems.

Software Assurance & Support

Shows whether there is a valid contract in place and if there is, when it is due to expire.

MiVoice Office Call Recorder

Small Business - Channel License

The small business license covers both Record-A-Call and IP/SIP Extension recording sources. The licensing is calculated on concurrent calls in progress.

IP/SIP Extension - Channel License

The IP/SIP extension license allows the recording of IP and SIP devices using port mirroring (this is also support on the Small Business license, but only up to 8 channels maximum). The licensing is calculated on a concurrent calls in progress.

> Concurrent recording licensing -> If an MCS is licensed for 8 concurrent calls and 4 are currently in

> progress, it will display as '4 / 8'. The number of devices currently configured to use the license is display in brackets after the license. If the number of devices configured is greater than the number of licenses available then licenses will distributed on a first come first serve basis. Using the example of 8 licenses, the 9th call made would fail to be recorded.

Call Recorder Client Licenses

This license controls the use of the call recorder client for PCI compliance. Call Recorder Client licenses are included when purchasing the PCI Compliance license.

PCI Compliance

This license controls the use of the manual and automated methods of muting out sensitive information from call recordings. this is a site wide license.

PCI Compliance (DTMF)

This license controls the use of DTMF to mute out sensitive information from call recordings.

> DTMF Pause/Resume is not supported when using the Record-A-Call recording source.

Communication Service

Alarm Notification

This license controls whether the alarm notification features of the solution can be used.

Agent Hot Desking

This license controls whether the agent hot desking features of the solution can be used.

IP SMDR

This license controls whether the IP SMDR features of the solution can be used.

Node Licenses

This license controls whether features of MCS will work across multiple MiVoice Office 250 Nodes or not.

For more information on how node licensing affects MCS, please refer to the PBX section.

Night Mode

This license controls whether the night mode features of the solution can be used.

CPN Substitution

This license controls access to the CPN Substitution features of the solution. This is a system-wide license.

Call Routing

This license controls access to the Call Routing features of the solution. This is a system-wide license.

Mitel 6900 SIP Handsets (Basic)

This license controls how many 6900 Series Handsets can be managed by the system. For more information, please refer to the 6900 Handset Overview.

Mitel 6900 SIP Handsets (Advanced)

This license controls how many 6900 Series Handsets can have advanced softkeys added to their keymaps. For more information, please refer to the 6900 Softkey Features section.

Phone Manager

Outlook Integration Clients

This controls how many concurrent Phone Manager Desktops using an Outlook license can be connected to the MCS.

Professional Clients

This controls how many concurrent Phone Manager Desktops using a Professional license can be connected to the MCS.

Team Leader Clients

This controls how many concurrent Phone Manager Desktops using a Team Leader license can be connected to the MCS.

Mobile Clients

This controls how many licenses can be used of Phone Manager Mobile. Unlike Phone Manager Desktop, licenses are persistently consumed from the first time a user connects their Phone Manager Mobile client.

TAPI Licenses

This controls how many concurrent Phone Manager Desktops using a TAPI license can be connected to the MCS.

Softphone Licenses

This controls how many concurrent Phone Manager Desktops or Mobiles can use a Softphone license.

> Phone Manager Outlook, Professional, Team Leader and TAPI licenses are only consumed when the Phone Manager client is connected to the system.

> To assign Phone Manager licenses to users, use Client Profiles.

MiVoice Office Call Reporter

Call Logging

This is a site wide license which enables/disables the use of Call List and Configuration reports.

Call Reporting Devices

This is a device based license that controls access to grouped reports. To use grouped based reporting, there must be enough licenses to cover the number of extensions programmed on the telephone system.

> The number of extensions on the phone system is calculated by adding up all Digital, IP, Analogue and SIP extensions. To see which devices are being counted, browse to the PBX programmed within MCS

> and filter the view by *Call Reporting Devices* (If you have 16 programmed on a DDM but are only using 1, 16 will still be counted towards the total).

> ⚠ If the number of extensions on the telephone system exceeds the number of Call Reporting Devices, the system will allow 30 days to rectify the license before restricting access to grouped reports. Please refer to the License Violation section for more information.

Dashboard Licenses

Not currently available.

Wallboard Licenses

This license controls how many Real-Time Wallboards can be in use concurrently. For more information, please refer to the Real-Time Wallboard section.

Report Scheduling

This is a site wide license which enables/disables usage of the Report Scheduling features.

Phone Manager Outbound Clients

This controls how many concurrent Phone Manager Outbound users can be connected to the MCS. Licenses are only consumed when logged in and dialling.

Campaign Licenses

This limits how many campaigns can be created within the Phone Manager Outbound database.

DND Logging

This license controls DND event logging for historical and real-time reporting. This is a system wide license. DND events are not logged historically or accessible in real-time until this license is applied to the system.

ACD Reporting Users

This license controls how many ACD agents can be concurrently logged in and tracked for historical and real-time reporting purposes. If there are no ACD Reporting User licenses available, ACD agent event data will not be historically stored or accessible in real-time.

External Data Sources

Not currently available.

Trial License

If any trial licenses have been applied to the server, they will display here. If they have not expired then they will already be accounted for in the relevant license section. For example, if there are 5 Phone Manager Professional trial licenses that have not expired, the Phone Manager section will take these licenses into account when displaying how many Professional licenses are available.

9.2.1.2 License Violation

License violation applies to Node and Call Reporting Device licenses. If the MCS is connected to a telephone system and does not have the necessary licenses then features of the solution will cease to operate until the license violation has been resolved.

Node Licenses

If the MCS is licensed for either the Call Recording or Call Reporting features then it must have be licensed with enough Node licenses for the number of nodes it is connecting to.

Call Reporting Device License

If the MCS is licensed for Call Reporting, it must have enough Call Reporting Device licenses to cover all extensions on all nodes that the MCS is connected to.

Grace Period & Resolving a License Violation

If the MCS does not have enough Node or Call Reporting Device licenses then it will start a grace period to allow the license issues to be resolved before access to features are restricted.

This grace period is currently 30 days.

If the number of nodes licenses is currently in violation, the offending node must be removed from the MCS and CT Gateway or a Multi-Site license must be purchased.

If the number of Call Reporting Devices license is currently in violation, extensions must be deleted from the MCS and PBX or additional Call Reporting Device licenses must be purchased.

If the license violation is not fixed within the grace period then users will be restricted from accessing the features involved.

9.2.1.3 Voucher Licenses

Voucher based licenses can be used to add additional licenses to an MCS installation. When ordering additional licenses from Mitel, they will provided in two formats:

- A pdf certificate providing details of the part number ordered and the voucher code
- A text document listing all vouchers generated for an order so that multiple vouchers can be assigned to an MCS in one go

For more information about applying vouchers to the MCS, please refer to the Server License section.

> Vouchers can be assigned to MCS installations running versions prior to 5.x using the Mitel Communication Service portal.

9.2.1.4 Licence Usage

Many of the licences provided through MCS are used on a per user or per device basis. The following sections provide information on which users and devices are using licences:

- User Connections -> Provides information on Phone Manager Desktop, Mobile, Call Recorder Client and Real-Time Reporting connections
- Connected Devices -> Provides information on ACD Reporting and Mitel Handset Licence usage

9.2.1.4.1 Connected Devices

The connected devices section shows a list of Agent IDs and Extensions that are using licences on the system.

Usage of the following licences can be viewed on this page:

ACD Reporting Users

These licences are consumed when an ACD Agent ID logs into the telephone system. If there is no ACD Reporting User licence available when an Agent ID logs in, no historical or real-time reporting information about the agent will be recorded. If a licence becomes available, an unlicensed agent will need to log out and back in again to consume it.

Mitel Handset Licences

These licences are consumed by Mitel 6900 Handsets that are using the MCS server as a configuration server.

for more information, please refer to the 6900 Overview section.

9.2.1.4.2 User Connections

The user connections screen provides a snap shot of information about any User based connections to the MCS server. The screen is designed to provide information about which licences users are consuming and which client types are connected.

Client Types

- Phone Manager Desktop
- Phone Manager Mobile
- Call Recorder Client
- Real-time Reporting

Licence Types

- Outlook
- Professional
- Team Leader
- Mobile
- Softphone
- TAPI
- Wallboard
- Dashboard

> To see what ACD Reporting and Mitel Handset licences are being consumed, please refer to the Connected Devices section.

Client Information

The following information is displayed about each connection:

User's Name - The name of the user that the connection is associated with

Client Type - The type of connection (Phone Manager Desktop, Call Recorder Client, Phone Manager Mobile or Real-Time Reporting)

Licences - Any licences being consumed by the client connection.

Version - The version number of the software the client is running. When a 5.0 or higher version of the client is running then the build number will be displayed in brackets).

Duration - The time the client has been connected for.

Additional Information

The following additional information about a specific client connection can be viewed by clicking on the magnifying glass icon (where applicable):

Extension - The extension number the client is currently associated to.

IP Address - The IP address of the remote client.

OS - The operating system running on the remote client's machine.

Disconnecting Clients

The connected clients screen also provides the ability to disconnect desktop clients from the system. This can be done on a connection by connection basis using the delete icon on the list itself or en-mass by pressing the 'Disconnect All Desktop Clients' button below the list.

9.2.2 Phone Systems

Overview

The system integrates with a MiVoice Office 250 (PBX) phone system or network of phone systems to perform the features required. If the PBX is networked to other PBXs in a multi-node configuration then a Mitel CT Gateway is required.

> As well as settings on the system there may be specific configuration and/or licenses that are required on the PBX such as CAT F licenses for the Phone Manager Softphone and OAI. See your phone system representative for details.

Configuration

To configure a new phone system:

1. Check the system is listed within the PBX Supported Versions section.
2. For multi-node environments decide on the most appropriate configuration, see the Multi-Node Scenarios section.
3. Configure the PBX with the details in PBX OAI Configuration section.
4. Follow the procedure in Add and Edit Phone System.
5. Check the Node Configuration .
6. Configure the IP Address of any MiVoice Border Gateways

9.2.2.1 PBX Supported Versions

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
- Call Processing Version 6.3.x

> ⚠ If Mitel 6900 Handsets are being supported, the Call Processing Version must be 6.3 SP1 (6.3.7.58) or higher.

The following Multi-Node configuration is supported:

- Multiple MiVoice Office 250 nodes via the use of a Mitel CT Gateway(Version 5.0.64 or higher is required).
- 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 Mitel 6900 Series Handsets:

- Cat F licenses are required for each connected 6900 handset.

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).

> ⚠ MCS will not connect to CT Gateway Versions below 5.0.64. If it detects the version is lower than this it will fail to start.

> ⚠ MCS does not support ACD member hunt groups, only ACD Agent hunt groups.

> ⚠ 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 G711

> 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.

9.2.2.2 PBX OAI Configuration

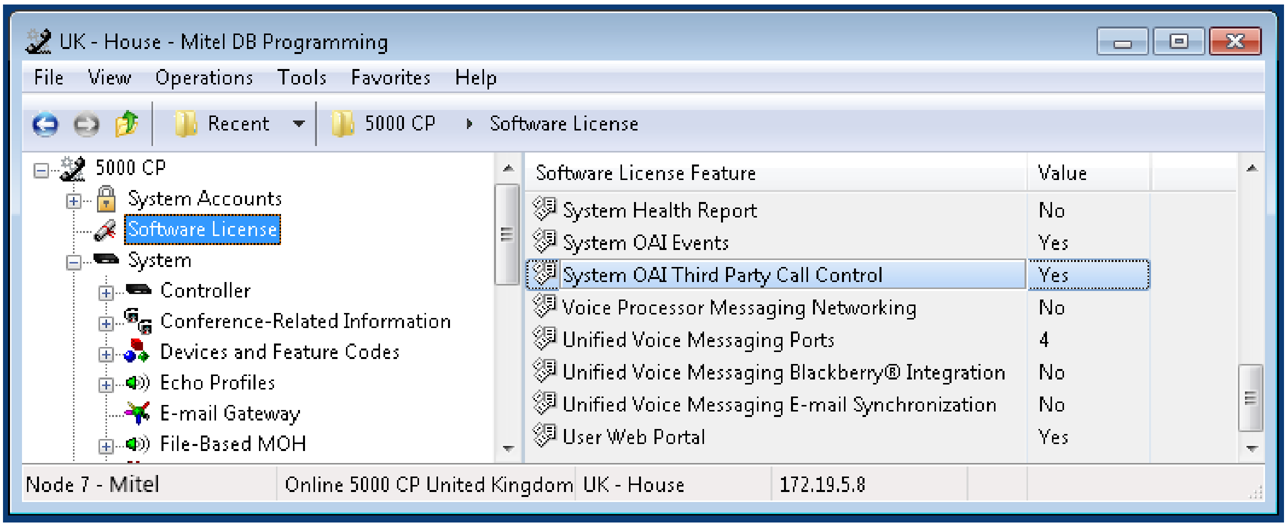
Overview

Configuration is required on the PBX to allow the Communication Service to connect.

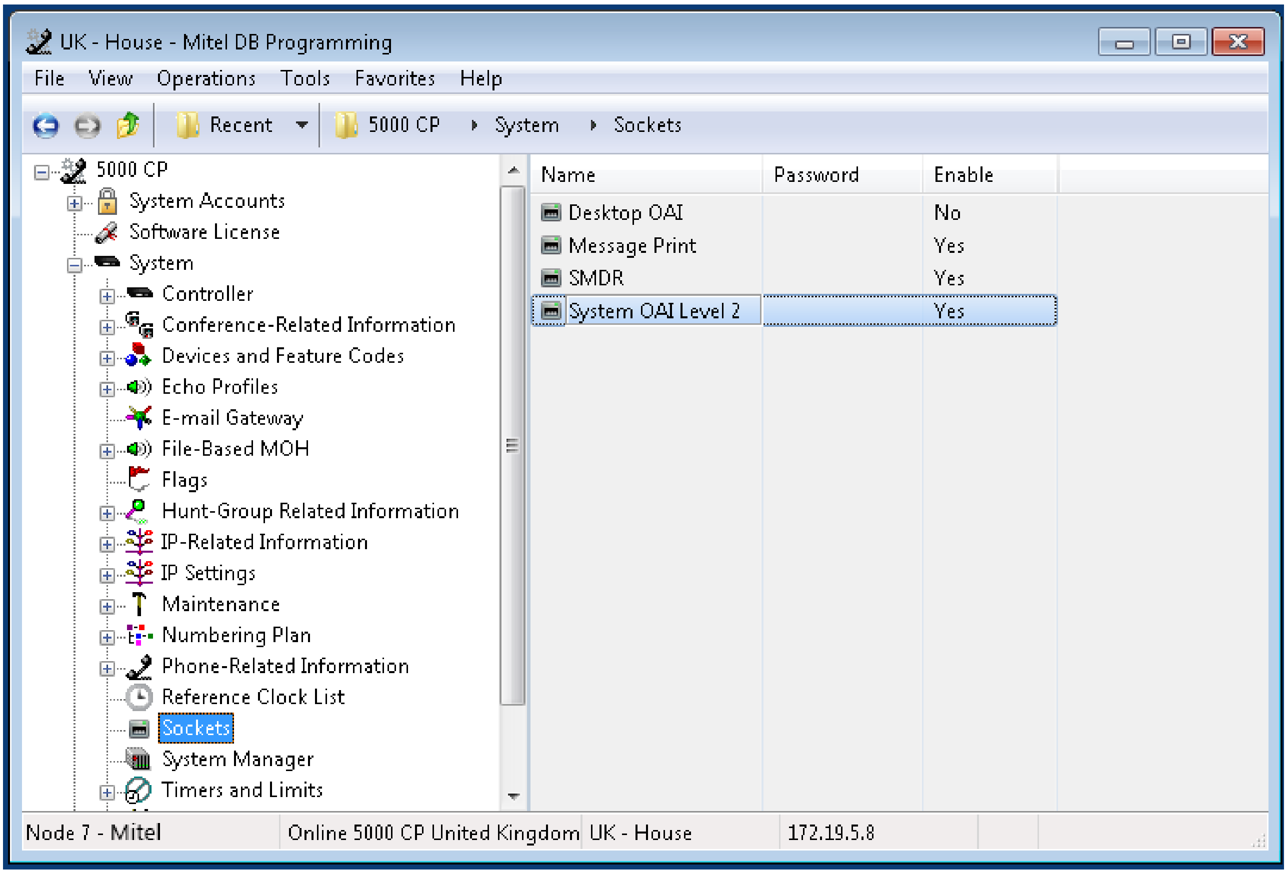
Configuration

To configure the PBX:

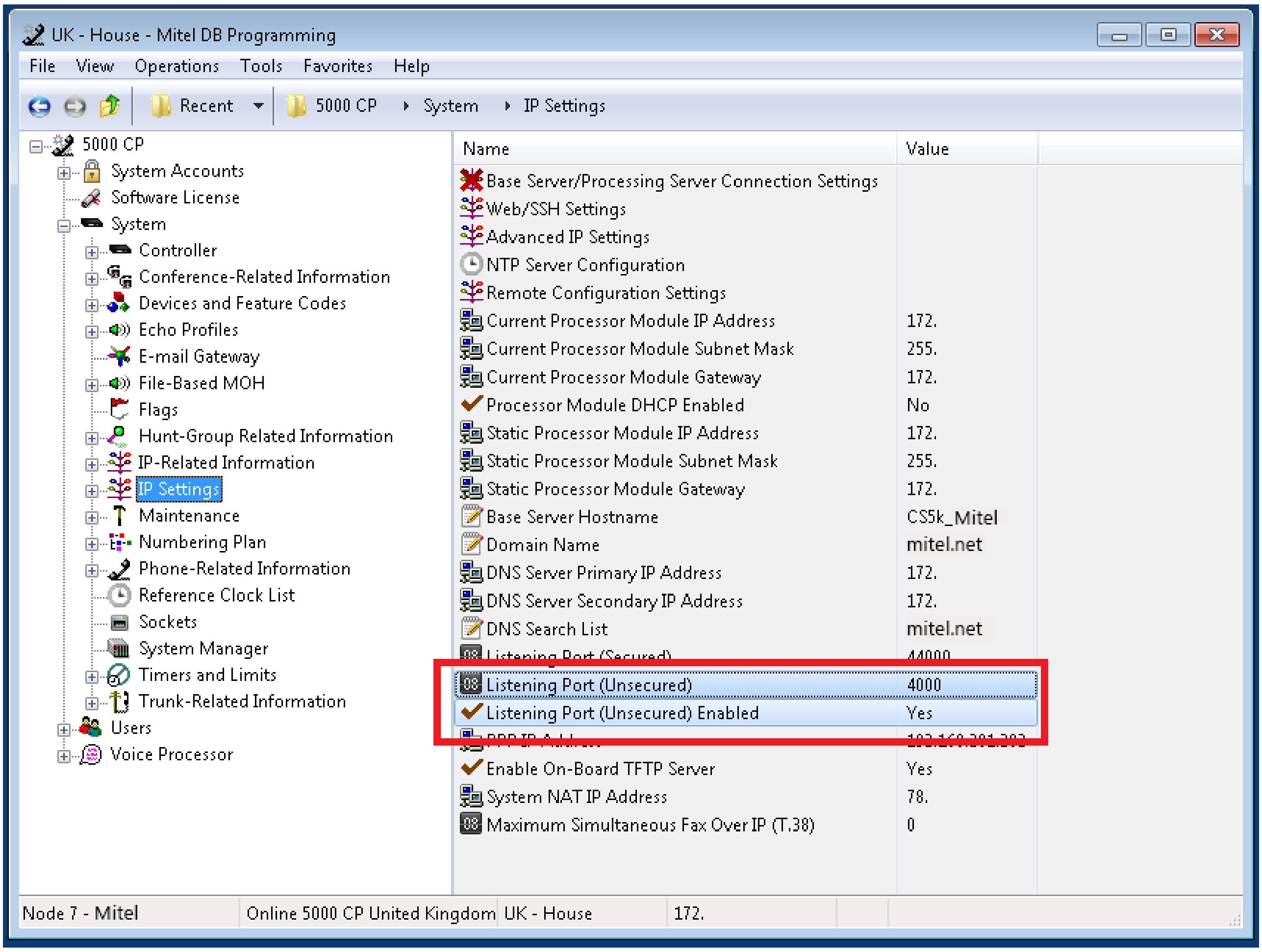
1. Open Mitel Database Programming
2. The connection to the PBX uses the *System OAI Level 2* socket on the PBX. This needs to be licensed on the PBX as *System OAI Third Party Call Control* as shown.



3. To enable the *System OAI Level 2* events open the *System -> Sockets* section.
4. Set the *Enable* property for *System OAI Level 2* to be *Yes*.



5. To enable the system to connect to the PBX the required connection port on the PBX also needs to be enabled, open the *System -> IP Settings* section.
6. Set the *Listening Port (Unsecured)* to 4000.
7. Set the *Listening Port (Unsecured) Enabled* to *Yes*.


UK - House - Mitel DB Programming
File View Operations Tools Favorites Help
Recent 5000 CP System IP Settings
5000 CP
System Accounts
Software License
System
Controller
Conference-Related Information
Devices and Feature Codes
Echo Profiles
E-mail Gateway
File-Based MOH
Flags
Hunt-Group Related Information
IP-Related Information
IP Settings
Maintenance
Numbering Plan
Phone-Related Information
Reference Clock List
Sockets
System Manager
Timers and Limits
Trunk-Related Information
Users
Voice Processor
Name
Value
Base Server/Processing Server Connection Settings
Web/SSH Settings
Advanced IP Settings
NTP Server Configuration
Remote Configuration Settings
Current Processor Module IP Address
172.
Current Processor Module Subnet Mask
255.
Current Processor Module Gateway
172.
Processor Module DHCP Enabled
No
Static Processor Module IP Address
172.
Static Processor Module Subnet Mask
255.
Static Processor Module Gateway
172.
Base Server Hostname
CS5k_Mitel
Domain Name
mitel.net
DNS Server Primary IP Address
172.
DNS Server Secondary IP Address
172.
DNS Search List
mitel.net
Listening Port (Unsecured)
4000
Listening Port (Unsecured) Enabled
Yes
Enable On-Board TFTP Server
Yes
System NAT IP Address
78.
Maximum Simultaneous Fax Over IP (T.38)
0
Node 7 - Mitel
Online 5000 CP United Kingdom
UK - House
172.

9.2.2.3 Add and Edit Phone System

Overview

Follow this procedure to create a new connection to the PBX.

Configuration

To add a new phone system

1. Access the Site Settings -> Phone Systems section.
2. Click *Add* / *Edit* and then enter the requested information.
    - **Type:** This will always be MiVoice Office 250
    - **Name:** Give the Phone System entry a logical name
    - **Host:** Enter the IP address or hostname of the MiVoice Office 250 PBX or CT Gateway into the **Host** field.
    - **Port**: Configure the OAI connection **Port**, the default is 4000.
    - **Password**: Enter the OAI **Password** if one has been set, the default is with no password.
3. Click *Save*.
4. Click on *Yes* to import the devices from the PBX.

9.2.2.4 Device Configuration

Once the PBX configuration has been configured the devices will be automatically imported. It is not required to manually maintain the list of devices, this will be done automatically via the OAI connection to the PBX.

The list of devices imported into the system can be seen from the Site Settings -> Phone Systems -> PBX section. Clicking on the *Import* button under the *Devices* section will force an import, or additional devices can be manually added if required.

> If any extensions on the telephone system are numbers generally used for emergency services (e.g. 999, 112 or 911), they cannot be dialled using Phone Manager because these are hard-coded emergency numbers. If there are extensions on the telephone system that match these numbers then they should be renumbered.

CT Gateway

If the MCS is connected to a CT Gateway it will import devices from all nodes the CT gateway is connected to. The MCS will also download details about the nodes themselves, the node details can be configured from the Nodes section, see the Node Configuration section for more details.

Connecting the MCS to a CT Gateway will have an impact on the licenses required to run the system. Please refer to the License Overview section for more information.

Device Settings

Device Types

When the MCS imports information about all the devices on the telephone system, it imports the device number, description and type. This information is kept up to date by default so there is no need to edit it manually except for the following two types:

DDI Numbers

DDI numbers cannot be automatically imported from the telephone system. If required, they can be manually added here and kept up to date. Any DDI numbers added here can then be used in other parts of the application.

Hot Desking

If a Hot Desk user is logged in when MCS starts up, the MCS will not know the device in question is a Hot Desk device until it first logs out. To manually update the database, find the device under the PBXs section and select 'Edit' Select 'Phantom' from the 'Device Type' drop down and then check the 'Hot desk device' checkbox.

Once the system knows a device is a Hot Desk device it will present the user with a Hot Desk login/logout toggle within Phone Manager.

MAC Address / IP Address

This property is used in conjunction with the MiVoice Office Call Recorder features when using the IP/SIP Extension recording source. To match the audio on the network to a device on the telephone system, the MCS needs to know either the MAC address or IP Address of the extension.

> The MCS server should auto detect all MAC and IP addresses so this property will not need to be manually configured unless it fails to do so.

Disable (Not Used)

Each device the MCS has imported provides an option for disabling the monitoring of events. This option should not be used unless instructed by a Mitel engineer. This option cannot be used to avoid Call Logging licenses and will cause problems with the call modelling if used.

SIP Authorisation

The details entered on this tab are essential for the operation of Phone Manager Softphones (both Desktop and Mobile) and the 6900 handsets. The MCS passes these credentials to the softphones and 6900 handsets so that they can successfully register as SIP devices with the telephone system.

Authorisation Name / Password

These credentials are used by handsets/softphones connecting from the local network to the telephone system. They will also be used by remote handsets/softphones if the 'User remote authorisation credentials' option is not checked. When using a MiVoice Border Gateway, the internal authorisation name must match the extension number of the phone otherwise authentication with the telephone system will fail.

> Phone Manager Mobile softphones always use these credentials because the SIP connection is between the MCS and the telephone system.

Remote Authorisation Name / Password

If the 'User remote authorisation credentials' option is checked, these credentials will be used for remote sofpthones/handsets when registering with the MiVoice Border Gateway. By default, when the 'Use remote authorisation credentials' option is enabled, the name and password fields will be pre-configured with random complex entries.

If the Rest API for the MiVoice Border Gateway has been configured, enabling 'Use remote authorisation credentials' against a SIP extension
cause the MCS to provision the SIP extension as a teleworker on the MBG. For more information, please refer to the Remote Connections engineering guidelines.

> ⚠ It is important to configure complex usernames and passwords for SIP Authentication to reduce the risk of unauthorised access. It is advisable not to use the extension number as the authorisation name.

> ⚠ When using a MiVoice Border Gateway, the internal authorisation name must match the extension number of the phone otherwise authentication with the telephone system will fail.

Call Statistics

The MCS system can model calls differently depending on the device type. The following two options are available to alter how the calls are modelled:

Treat this device as not answering calls

Enabling this setting will cause any calls that are answered by this device to be treated as NOT answered. This should always be set for devices such as CRAs which play queuing announcements to calls waiting at a hunt group. This prevents calls showing as answered to a CRA when still ringing at the group.

Treat this device as not having rung

Enabling this setting will cause any calls ringing at this device to be treated as NOT ringing. This ignores that a call is ringing at the device (e.g. a CRA) and correctly measures the ring time for the hunt group.

> The MCS will automatically enable both of these settings for all CRA, STAR and AutoAttendant applications when they are first imported.

Reset call timers when a call rings this group

Enabling this setting will reset any call timers associated with a call that rings the hunt group. This provides a way to the reset real-time statistics so that any time spent in call routing announcements can be ignored. Depending on the system-wide setting 'Reset Call timers Only Once per Call', a call's timers will either be reset every time it starts ringing at a hunt group or only the first time it rings at a hunt group.

> The MCS will automatically enable both of these settings for all Hunt Groups when they are first imported.

9.2.2.5 Node Configuration

Multiple MiVoice Office 250 PBXs can be networked together to allow calls to be routed from one node to another. This allows calls to be handled by devices (agent, extensions, voicemail etc) on other nodes to where the call originated from and allows calls to be made through trunks on remote nodes using ARS.

There are two reasons why node configuration needs to be entered into the MCS website:

- Provide connection details for Phone Manager Softphones
- Define the 'Default Node' when using MCS without additional node licenses.

Phone Manager Softphones & 6900 Phones

Each SIP device connected to the PBX has a specific node that they are programmed against and they connect to. Due to this, the MCS needs to now about these nodes and what their connection details are.

For example, when using a Mitel Phone Manager Softphone, a SIP connection would need to be made to the specific node that it has been programmed on. If connecting from the internal LAN network, the internal IP address of the node would be required. If connecting from a remote location, the external NAT IP address would be required.

The system will automatically import the node configuration during a device import but not all of the information can be retrieved this way and needs to be manually configured.

For more information on Softphone & 6900 SIP configuration, please refer to the Softphone/6900 Support section.

Default Node

If Mitel Communication Service has been connected to multiple MiVoice Office 250 systems using a CT Gateway but has no Multi-Node license then one of the nodes needs to be selected as the 'Default' node. This node will be the one that MCS will accept Phone Manager connections from and provide IP SMDR and Agent Hot Desking services to.

Configuration

To access the node configuration section, browse to the '⚙' -> Site Settings -> Phone Systems -> PBX section. Scroll down to the *Nodes* section under *Devices.* If MCS is already connected to the PBX network then the Nodes section should already be pre-populated.

The following settings can be configured against each node:

General

Node ID: The unique node number for this PBX node as programmed on the telephone system in Database Programming

Description: In the Description field enter a user friendly name to identify this node.

Local IP Address: Set the ***Local IP address*** to be the internal LAN IP address of this node.

> ⚠ If the system has a PS-1 attached then the Local IP Address should be the PS-1 address not the Base Server.

Local SIP port: Set the Local SIP port that will be used by the Softphone to use, by default this is 5060. This should match the configuration within Mitel Database Programming.

NAT IP Address: Set the NAT IP address to be the external IP address of this node. This will be used when the Softphone connects from a remote location.

NAT SIP port: Set the Nat SIP port that will be used by the Softphone to use on when connecting from a remote location.

Extension Programming Password: If there is an extension programming password configured on the node, it needs to be configured here so that the MCS can perform operations such as changing the Caller ID on an extension.

Encryption Password: This password is used when querying SIP Authorisation Credentials from the telephone system for use with 6900 phones and Phone Manager Softphones. The password configured here must match the App Suite Encryption password configured on the node. For more information, please refer to the Encryption Password section.

Is default: The Is Default setting sets what the primary node connection is.This is to configure what extensions that Phone Manager clients can connect to when the system does not have a multi-node license. If a Phone Manager client tries to connect to an extension on a node other than the one that has the Default setting then the connection will be refused. With a multi-node license Phone Manager clients can be associated with any extension on any node. See the Multi-Node Scenarios section for more details.

Dialling

Voicemail DDI: An external DDI number to access the Voicemail Retrieval application on the telephone system. This is used by Phone Manager Mobile.

Auto Attendant: An external DDI number to access the auto attendant on the telephone system. This is used by Phone Manager Mobile

Wait time: The amount of time after a call is connected before any DTMF digits are dialled.

9.2.2.6 Multi-Node Scenarios

The Communication Service supports single and multi-node MiVoice Office 250 configurations. Depending on the requirements of the customer there are two different ways to implement the solution in a multi-node scenario:

- Multiple Communication Services with single-node licenses
- Single Communication Service with a multi-node license

The benefits and restrictions of each method are outlined below.

> ⚠ The scenarios outlined below only affect Phone Manager usage, From release 5.0, if using any of the Call Reporting or Call Recording features, a license for each node is required.

Multiple Communication Services with Single-Node Licenses

Out of the box Communication Service can be configured to connect to a Mitel CT Gateway and provide users with device status information across more than one node. It will however only provide Phone Manager capability for a single node. If the Communication Service is configured to connect to a CT Gateway without a multi-node license then one of the nodes needs to be configured to be the node Mitel Communication Server is going to support Phone Manager clients on.

In this scenario each Node can have it's own Communications Service to support it's own Phone Manager clients.

Example

A company has two MiVoice Office 250 systems. Each system has it's own Communication Service providing Phone Manager connections for a single node. Both Communication Services are connected to a CT Gateway.

Benefits & Restrictions

Configuring the Communication Service in this way has the following benefits and restrictions:

Benefits

- No Multi-site license needs to be purchased
- Each site can configure of their own Communication Service
- Minimal inter site traffic in a WAN environment

Restrictions

- Users cannot Chat between Communication Servers
- All configuration needs to be duplicated on each Communication Service, User & Business Units for example
- Non of the Call Reporting or Call Recording features could be used
- IP SMDR and Agent Hot Desking would only work for the default node

This configuration is usually recommended for scenarios where multiple nodes are installed at different physical locations.

Single Centralised Communication Service with a Multi-Node License

To work in the this configuration the Communication Server must have a Multi-Node license applied, this will allow the Communication Service to support Phone Manager connections from all the nodes available.

Example

A company has two MiVoice Office 250 systems. A single Communication Service connects to both systems via a CT Gateway and provides connectivity for Phone Managers users on both systems.

Benefits & Restrictions

Configuring the Communication Service in this way has the following benefits and restrictions:

Benefits

- Central point of administration
- Chat between all users of the system
- Call Reporting and Call Recording features can be used
- IP SMDR and Agent Hot Desking would work on all nodes

Restrictions

- Increased traffic in WAN environments
- Less resilience to WAN connection loss

This configuration is usually recommended for scenarios where multiple nodes are installed at the same physical location.

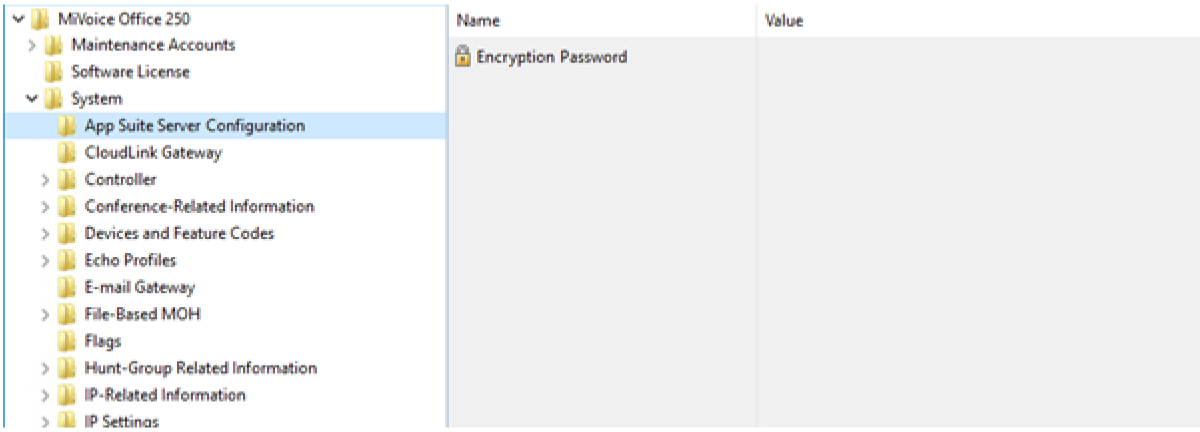
9.2.2.7 Softphone/6900 Support

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

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

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

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



Encryption Password

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

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

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

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

Node Configuration for SIP

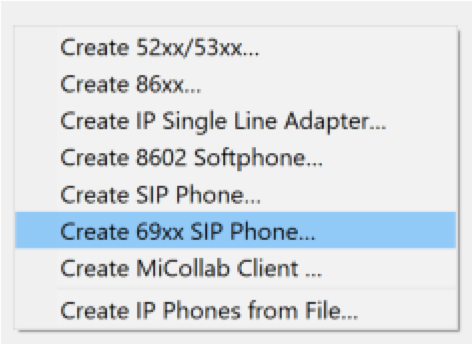
The MCS server needs to provide each 6900 phone and Phone Manager Softphone with the IP address of a SIP server to register with (the MiVoice Office 250). The IP address required will depend on which MiVoice Office 250 node the SIP extension is configured on and whether the phone is local or a teleworker.

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

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

69xx SIP Phone

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

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

SIP Phone Group

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

- Maximum Number of Calls = 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.

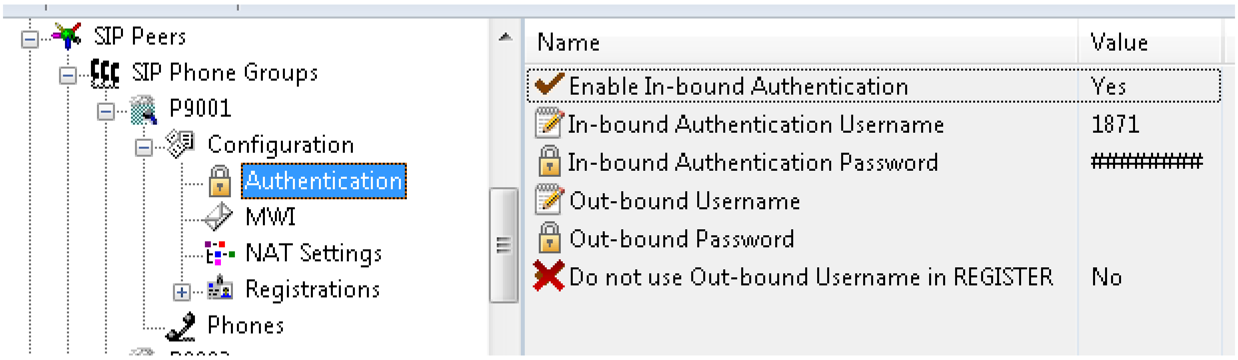
Manual Authentication Configuration

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

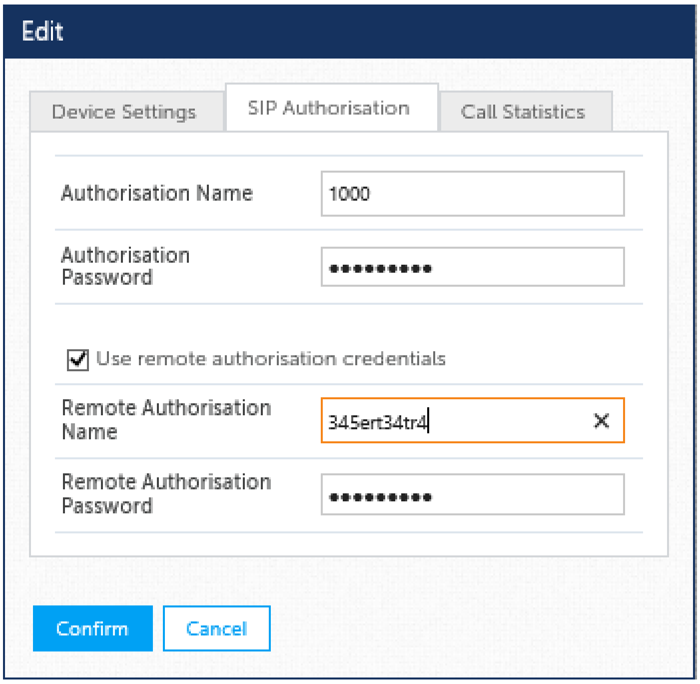
> If release 6.3 SP1 or higher is being used, check the App Suite Server Configuration section below.

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

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



This same username and password combination would then need to be set on the device configuration on the Communication Service for this extension.



For information on configuring Teleworker phones, please refer to the Remote Connections engineering guidelines.

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

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

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

Call Configuration

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

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

Phone Manager Mobile Softphone)

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

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

> It is important to connect only one softphone to each extension number on the telephone systems. Registering more 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.

9.2.2.8 Call Segmentation

Overview

Call segmentation is the name given to how the system models calls in real-time and historically when storing the calls the database. This call modelling affects the call recording and call reporting areas of the solution. The following section explains how the MCS models calls and what users need to be aware of when using different features of the solution.

The MCS connects to the MiVoice Office 250 using OAI and logs all call information (internal and external) from all nodes (to be connected to multiple nodes a CT Gateway must be used). When calls are transferred between different devices on the telephone system the MCS will create call segments. Call segments will get created when calls ring at or get answered at different device. These devices can be extensions or phone system applications such as call routing announcements (CRA).

Segmentation & Reporting

When viewing reports, it is important to understand how call segments will affect the data being displayed. Some reports will count individual call segments while others will only count calls (refer to the Report Templates section to see which show call segments and which show calls).

For example, a 'Calls By DDI' report will only count complete calls and will ignore call segments. This is because the report is designed to show how many actual calls came in on a DDI. A 'Calls By Hunt Group' report will count individual call segments. This is because a call may get presented to more than one hunt group and so needs to be counted against each.

Segmentation & Call Recording

Segmentation effects the recording in three ways:

- Security
- Exclusion / Inclusion
- Playback

Security

When the system evaluates Access Scopes and Access Filters, it will do so on a segment by segment basis. This may mean a user has permission to see/playback only certain segments of a call, not all of them. This provides a granular level of access control for recording playback.

Exclusion/Inclusion Lists

The call recorder evaluates exclusion and inclusion lists on a segment by segment basis. This allows certain segments of calls to be discarded while keeping others.

Playback

The example below shows 5 separate calls with the last device that handled the call before it was cleared shown in the Endpoint and Agent columns. Without segmentation then only the last device that handled the call would be tagged against the call record.

Outside Number	Endpoint	Agent	Answered	Duration	Call Type	User	Play	Save	Email
No CLI available	1833	1021	08/05/2012 14:51:22	00:00:08	Inbound	Tony Leroy			
07977000000	1862	1024	08/05/2012 14:49:51	00:00:27	Inbound	David Smith			
07977000000	1833	1021	08/05/2012 14:49:22	00:00:16	Inbound	Tony Leroy			
07977000000	1833	1021	08/05/2012 12:14:13	00:00:05	Inbound	Nacho Valencia			
07977000000	1833	1021	08/05/2012 11:57:40	00:00:04	Inbound	Isa Sastre			

Page 1 of 1 (5 results)

With call segmentation, each row on the grid shows either a single segment of the call or an aggregate call if there is more than one segment. The aggregate calls are shown with a ▸ at the start of the row, clicking on this expands the grid to show all the separate segments.

	Outside Number	Endpoint	Agent	Answered	Duration	Call Type	User	Play	Save	Email
	No CLI available	1833	1021	08/05/2012 14:51:22	00:00:08	Inbound	Tony Leroy			
A	07977000000	1862	1024	08/05/2012 14:49:51	00:00:27	Inbound	David Smith			
1	07977000000	2523		08/05/2012 14:49:51	00:00:09	Inbound	Tony Leroy			
2	07977000000	1833	1021	08/05/2012 14:50:02	00:00:08	Inbound	Nacho Valencia			
3	07977000000	1862	1024	08/05/2012 14:50:12	00:00:09	Inbound	Isa Sastre			
	07977000000	1833	1021	08/05/2012 14:49:22	00:00:16	Inbound	Tony Leroy			
	07977000000	1833	1021	08/05/2012 12:14:13	00:00:05	Inbound	David Smith			
	07977000000	1833	1021	08/05/2012 11:57:40	00:00:04	Inbound	David Smith			

Page 1 of 1 (5 results)

The * on the right shows a single logical call that has been segmented. The row marked *A* is the aggregate entry that is displayed when the row is collapsed and summarises all segments, showing the details of the last device that handled the call. Rows 1, 2 and 3 show the individual segment details of the call.

1. Inbound call to a call routing announcement 2523.
2. Answered on device 1833, agent 1021.
3. Transferred to endpoint1862, agent 1024.

9.2.2.9 MiVoice Border Gateways

If there are any MiVoice Border Gateways configured to support teleworker extensions on the telephone system, the MiVoice Office Application Suite needs to know about their internal IP Addresses.

The MiVoice Border Gateways have an effect on two aspects of MiVoice Office Application Suite operation:

- IP Extension call recording -> The internal address of the MiVoice Border Gateway is required so that system can correctly self-learn the IP addresses of IP Extensions and can filter out the duplicated traffic from the internal address of the gateway.
- 6900 Handsets -> The internal address of the gateway is used to identify when a 6900 handset is local to the system or remote.

Enter all internal addresses that are necessary. There may be more than one if there is more than one MiVoice Border Gateway or it has more than one internal address.

Rest API

MiVoice Office Application Suite supports the MiVoice Border Gateway's API for provisioning. This allows the MCS server to automatically provision SIP Users on the MBG to simplify the deployment of Teleworkers using:

- 6900 Phones
- Phone Manager Desktop Softphone
- Phone Manager Mobile Softphone

The settings for enabling and using the MBG's Rest API are listed below. For information on how the teleworker deployment works and how to enable the API on the MBG, please refer to the Remote Connections engineering guidelines.

> The MiVoice Office Application Suite supports the Rest API for one MBG only. If more than one IP address is configured for MBGs, the first address will be used for Rest API access.

> Teleworker licenses on the MiVoice Border Gateway are required for each SIP User provisioned.

Enable Rest API

This setting controls the MCS server's integration with the MiVoice Border Gateway (MBG). When enabled, the MCS will actively add/delete/update SIP Users on the MBG.

> Once the Rest API has been enabled and configured, MiVoice Office Application Suite will be able to provision all SIP Users on the MBG. Any SIP Users that are configured on the MBG for uses other than 6900 or Phone Manager Softphones will still need to be configured on the MiVoice Office Application Suite.

Name / Consumer ID / Shared Secret

These settings are required by the MCS to communicate with the MBG. They must match those configured on the MBG in order for the MCS to be able to request API access.

For information on configuring the API link to the MBG, please refer to the Remote/Teleworker Connections engineering guidelines.

Request Access Token

This process can be used to setup the connection between the MCS and the MBG so that the MCS can automatically provision teleworker phones.

For information on configuring the API link to the MBG, please refer to the Remote/Teleworker Connections engineering guidelines.

Provisioning Teleworker Phones

This process can be used to provision (or un-provision) any SIP phones as Teleworkers on the MBG. Pressing the button will display the SIP phone device picker which will show which phones have already been provisioned on the MBG and which phones have not.

9.2.3 Dial Plan

Overview

When calls come into the PBX the outside number may contain extra digits or not be complete, for example contain 141 to suppress caller ID, contain ARS (least cost routing) digits or a user could have dialled a number without the local area code. The system can be configured to "clean" the number before it is stored or used in Phone Manager to provide a consistent format for all numbers.

The dial plan is also used to format outbound dialling digits for Phone Manager users. It is necessary to configure the dial plan to match the configuration of the PBX.

> As a minimum the **Outside line** prefix should be configured.

Configuration

To configure the dial patterns:

1. Access the Site Settings -> Dial Plan section.
2. Enter the settings used to "clean" the number in the *Call history* section.
    - **DDI Prefix to add:** When an incoming call is received on a direct dial number the telephone network provider often only sends the last few digits of the DDI/DID number dialled. For example if the number 01617123456 is dialled the telephone system only receives 123456. In this case 123456 will be logged against the call. To add the DDI prefix you can enter in the preceding digits for the rest of the number dialled, 01617 value for this example.
    - **Outbound prefixes to remove**:When outbound calls are made, unwanted prefix digits can be removed by adding the prefixes into this section. Multiple entries can be entered by separating them with a comma. For example if the PBX was configured with 8 as the **Outgoing line** digit and users regularly dial 141 to suppress CLI, enter 8, 8141.
3. Enter the settings used for the dialling out rules into the *Outbound dial patterns* section.
    - **Country**: Select the country from the drop down menu that thePBX resides in and this will put the default settings in for the country that has been selected.
    - **Outside line**: Select the digit that is used to access an outside line on the PBX.
    - **Local area codes**: Enter the local area code for the area that the PBX provider's trunks are installed.
    - **Local override codes**: Enter the local area codes for local calls that are treated as long distance calls. This is required when there are certain numbers with a local area code that must be dialled as a long distance number.
    - **Max extension length**: Select the maximum length of an extension on the PBX; by default this is set to 4. If this is not set correctly then dialling an extension may result in an external call being made. This allows Phone Manager users to dial outside numbers without having to enter the outside number prefix.
    - **Service codes**: Enter the service codes that are dialled from the PBX. Any numbers here will be dialled as though they are an outside number, i.e. if 911 is dialled then 8911 will actually be dialled with the outside line digit prefixed.
    - **Toll digit**: Select the toll digit, in the UK the toll digit should be set to 0 and for the US this should be 1.
    - **National number length**: Enter the number of digits for a national telephone number in the country where the PBX is installed. This should include the local area code and the toll digit.
    - **International code**: Set the country code of where the PBX resides, for example: 1 for North America or 33 for France.
    - **International outbound code**: Set the international outbound code that is required to dial international numbers excluding the code to obtain an outside line, for example: 011 for North America and 00 for European countries.
    - **Dial toll on long distance calls**: Enable this if the toll digit should be added to long distance calls.
    - **Dial toll on local calls**: Enable this if a toll prefix should be added to all locally dialled calls.
    - **Dial hash**: A pound / hash (#) can be automatically added to the dial string to send the call to the PBX

immediately without waiting for the inter digit timeout.

- **Dial primary local area code**: Enable this option if local area codes should be dialled. If this is not enabled then when a number is dialled that has an area code it will be removed automatically unless the area code has been configured in the **Local override codes** section.

> MCS only supports a single dial plan for a single region. For installations where multiple dial plans are required, multiple MCS solutions will need to be installed.

9.2.4 Client Locations

Overview

The addresses configured here are used by the various client applications to connect back to the Communication Service (i.e. the IP address or FQDN of the Communication Service).

Clients that use these addresses (locations) are:

- Phone Manager Desktop
- Call Recorder Client
- Phone Manager Mobile
- 6900 Handsets

There are two categories of address available, Local and Remote.

> ⚠ Changing either of the Client Location addresses will cause the local certificate on the server to be recreated. This will mean all mobile clients will need to accept or install the new certificate before they can connect.

Local Location

The local location is for clients/phones that are running on the internal network or from the same network that the server is connected to and when there is no requirement for any NAT traversal.

The MCS will automatically populate the Local Location with the FQDN of the server if it is a member of a domain or the IP Address of the server if it is not. If the hostname or IP Address of the server changes, MCS will update the Local Location.

> ⚠ When using 6900 handsets, the location must be an IP Address or FQDN, it cannot be a hostname.

6900 Syslog IP Address

6900 handsets will use the Local Location address for server connections but require an IP address for Syslog connections. This is because the handsets do not support FQDN for logging.

SIP Addresses

When a softphone/6900 is connected using this location, it will use this address for the server connection but will require the telephone system address for SIP connectivity. The addresses/ports for SIP connectivity need to be configured against each individual node (see the Node Configuration section for details).

Remote Location

The remote location is for client/phone connections external to the network where the server is connected. This is used for when the connection is via a public address and uses NAT traversal through a router or firewall and where the connection IP address or host name is different to the internal IP address or FQDN of the system.

6900 Syslog IP Address

6900 handsets will use the Remote Location address for server connections but require an IP address for Syslog connections. This is because the handsets do not support FQDN for logging.

SIP Addresses

When a softphone/6900 is connected using this location, it will use this address for the server connection but will require the telephone system address for NAT SIP connectivity. The addresses/ports for NAT SIP connectivity need to be configured

Configuration

To edit the client locations:

1. Access the '⚙' -> Features -> Phone Manager Desktop -> Client Locations section.
2. Enter the **Name** for this connection, this is what will be displayed to the users when they are selecting the connection to use in their client software settings.
3. Enter a **Description** to describe what this connection is for.
4. In the *Local* section set the **Local IP Address/Hostname** to be the IP address or hostname of the server.
5. In the *Remote* section set the **NAT IP Address/Hostname** to be the NAT'd IP address or hostname of the server.
6. Click on *Save*.

> If using AD integrated login for Phone Manager clients it is essential that the Local Location is configured to be the DNS name of the server so that Kerberos is used for authentication not NTLM.

9.2.5 Email & SMTP

Overview

Email integration is essential for the correct operation of the system. There are several areas that require the email integration to be configured and working:

- When new user accounts are manually created for login to the website UI, the account details are sent out via email, without this users are unable to retrieve the password details to logon with.
- The Watchdog uses email to send out alerts when services are stopped or for critical notifications such as if the PBX link is lost.

For specific SMTP configurations see the How To's for:

- SMTP Configuration for Gmail
- SMTP Configuration for Office365

Configuration

To configure the Email SMTP settings:

1. Access the Site Settings -> Email & SMTP section.
2. Enter the details.
    - **System email address**: This is the email address that any alerts will be sent to. Typically the IT support or PBX support team might be configured here.
    - **Source email address**: This is used as the senders return address for any emails sent out.
    - **SMTP Server**: This is the IP address or hostname of a valid SMTP email server.
    - **Server requires authentication**: If the SMTP server requires authentication details to send emails then this should be checked and the Username and Password fields completed.
    - **Username**: If using SMTP authentication then this is the username to use.
    - **Password**: If using SMTP authentication then this is the password to use.
    - **Use SSL**: If the email connection requires an SSL connection then enable this. Note this is not always required when using authentication.
    - **Alternate Port**: Set this value to the SMTP port that the email server uses, by default this is 25.
    - **Email alarm interval**: This determines the frequency that repeat emails are sent out, for example if the PBX connection is lost then it will only send emails out every 60 minutes.

9.2.6 Database Maintenance

The system uses a Microsoft SQL Server database to store the details of the call history and the configuration of the system. Due to the amount of call data that is stored within the database it is necessary that regular maintenance occurs and reliable backups are performed. The system has built in support for performing these actions.

When maintenance runs the databases are backed up and then the call history database entries are moved into an archive database. This enables the current database to remain relatively small and maintains performance.

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.

> When using the MiVoice Office Call Recorder features of the solution, audio files are not archived until the associated call data record has been archived using the database maintenance process. For more information please refer to the Call Archiving section.

Configuration

To configure the maintenance settings:

1. Access the Site Settings -> Database Maintenance section.
2. Enter the details in the relevant areas.
    - **Backup database daily**: This enables or disables the daily automatic backup of the database.
    - **Backup path**: This defines the path where the backup file (.bak file) will be stored relative to the server.

      > Ideally this should be changed to a different server to ensure that a backup is available in case of server hardware failure.

    - **Backup time**: This sets the time to perform the backup in 24 hour format.
    - **Database archiving enabled**: This enables the movement of the call logging data from the main database to the Archive databases.
    - **Archiving period**: This defines the period of time that each archive database should store. This value should only be changed under high call volumes when the Microsoft® SQL Server limits are being exceeded or where performance is affected by high volume. By default, the system will automatically create a new archive database once the limit of 1 million call records per archive database has been reached or 12 months has passed.

Manually Archiving

It is possible to request an archive of the call information in the database manually. This can be done by using the 'Archive Now' feature. Once the archive has been request, check the Event tab on the dashboard and filter for the 'Mitel MCS DB Service' to check the status.

Requesting a manual archive also performs a database backup.

9.2.7 Users and Business Units

Overview

The Communication Service controls who can access the system and features by requiring each person that needs access to have a user account configured. These users are different from the PBX users or Microsoft® Active Directory users - although they can be linked. Each Communication Service user account has authentication details configured against it; either with a username and password, or a Windows logon name if Active Directory authentication is being used.

> In order to use Windows authentication for the User it is necessary to enable this in the Website settings.

The privileges that are needed are then controlled for each user via User Roles, and this controls what they can do with the system. For example a supervisor user could be granted access to the configuration section of the website and allowed to manage other users, whilst a basic user could have no access to the website and only connect using a Phone Manager client.

As each user will generally be a PBX user and making and receiving calls, multiple extensions and/or agent IDs can be associated with them. This enables all the calls a user makes (even if they have multiple devices) to be associated with them and provides Phone Manager with the extension and agent IDs that it needs to connect with. This also reduces the configuration information that an end user needs to provide and ensures that they connect using the correct details.

When a user has the Phone Manager role enabled they will have a Client Profile assigned to their user account and this will control what features are available to them. This determines what license that they will use and other options that control what features they can access from Phone Manager.

Users are organised into Business Units within the site to group them into logical departments or teams. These departments can be linked to existing Operational Units (OUs) in a Microsoft® Active Directory if required.

Users can be manually created if necessary but in order to keep maintenance of users to a minimum, most customers would opt to automatically create users. (See User Auto-creation section).

> If you are planning to automatically create users make sure to plan in advance of the installation to establish the process and ongoing maintenance of the Users. For example, if you plan to create users based on Active Directory then the customer's IT manager needs to be consulted.

The Business Units are grouped and maintained in a tree style structure with the users assigned to a specific unit. Individual users can be drag and dropped into different units. The different types of Users and Business units are shown by the type of icon shown against each entry.

Type	Description
Users:	This is an individual user on the system.
Business Unit	This is a specific business unit.
Unassigned User Business Unit	This contains any users that are not assigned to a specific business unit.
Deleted User Business Unit	This contains any users that have been deleted.

> Selecting a specific Business Unit will turn the text orange and then display all of the Users within the Unit on the right hand side.

9.2.7.1 Creating Business Units

Overview

Follow the procedure below to configure a new Business Unit.

Configuration

To add a new business unit

1. Access the Features -> Users & Business Units section.
2. Select the parent business unit that this new one will be under.
3. Click *New* underneath the list of business units on the left hand pane, or right click on the parent unit and select *New Business Unit.*
4. Enter the business unit name in the orange box.
5. Press *Enter*.
6. See the Business Units and Active Directory section to associate this with an Microsoft® Active Directory Organisational Unit.

9.2.7.2 Business Units and Active Directory

Overview

Business Units can be associated with an Active Directory Organisational Unit (OU) to enable Users to be automatically created within this Business Unit anytime new Users are created within the Active Directory (AD) Operational Unit (OU). This requires the Active Directory User Creation option in the User Auto-Creation section to be enabled. Once this is enabled the **OU Link** field is visible when creating or editing a Business Unit.

For example in the **OU Link** field either manually enter in the Distinguished Name of the OU or click on the *Browse* button to list all of the AD OUs in the domain. Using the *Browse* button will provide a list of OUs in the domain and selection will populate the **OU Link** with the correct naming convention.

For example: OU=Sales,OU=UK,OU=Contoso.Net Users,DC=Contoso,DC=Net.

9.2.7.3 Editing Business Units

Overview

Follow the procedure below to edit an existing Business Unit.

Configuration

To edit a business unit

1. Access the Features -> Users & Business Units section.
2. Select the business unit to edit.
3. Click *Edit* underneath the list of business units on the left hand pane, or right click on the parent unit and select *Edit*.
4. Enter the new business unit name in the **Description** field.
5. If applicable, enter the Active Directory **OU Link**, see the Business Units and Active Directory section for details.
6. Press *Save*.

9.2.7.4 Moving Business Units

Overview

Follow this procedure to move a business unit into a different location.

Configuration

To move a business unit

1. Access the Features -> Users & Business Units section.
2. Select the business unit to move.
3. Drag the business unit to the new location within the hierarchy.

9.2.7.5 Deleting Business Units

Overview

Follow this procedure to delete a business unit.

Configuration

To delete a business unit

1. Access the Features -> Users & Business Units section.
2. Select the business unit to delete.

   > If the business unit contains any users or business units then they will need to be moved or deleted before the parent business unit can be deleted.

3. Click *Delete* underneath the list of business units on the left hand pane, or right click on the parent unit and select *Delete*.
4. Click *Delete* to confirm the deletion.

9.2.7.6 Unassigned Users Business Unit

Overview

The **Unassigned Users** business unit contains any users that have been created on the system that have not been assigned to a specific business unit.

> This will include any auto created users.

Configuration

To view the unassigned business unit

1. Access the Features -> Users & Business Units section.
2. Select the **Unassigned Users** business unit.

9.2.7.7 Deleted Users Business Unit

Overview

The **Deleted Users** business unit contains any users that have been deleted on the system. When users are deleted they are only flagged as been deleted to enable any historical information to be maintained.

See the Deleting Users section for more details.

> Once a user has been deleted they cannot be restored.

Configuration

To view the deleted user business unit

1. Access the Features -> Users & Business Units section.
2. Select the **Deleted Users** business unit.

9.2.7.8 Users Overview

Overview

Users accounts are an integral part of the system, they control access to the system (both the website and Phone Manager clients) and call history entries so that user's can see all the calls made on any of their devices / agent IDs on the telephone system.

Call History & Associated Devices

Each user can have an associated agent ID and/or associated extensions assigned so that for each call that is handled by this agent ID and/or extension the call is tagged to this user. An agent ID/Extension can only be associated to one user at a time so there are no conflicts.

Each user can have one primary agent ID/extension and multiple secondary ones. The primary device is will be the device that other Phone Managers use to call by default and the extension where any Presence Profile selected by the user is applied.

If users change agent ID or use different extensions they can then be updated whilst maintaining the association with any calls that they made using the previous device(s). If users leave, and the agent ID and/or extensions are reused, then they can be assigned to different users and any calls from that point would then be associated with the new user.

DEE Devices

If a user's primary extension is configured on the telephone system as a Dynamic Extension Main extension then MCS will query the user's associated DEE extensions and keep track of them (The DEE extensions are only queried after the user object is first saved). If an extension is gets associated to a user as DEE extension and has not been assigned to any other user as a primary or secondary extension then any calls made will also appear in the users call history.

> Agent IDs will take precedence over extensions if a call is handled on an extension that has one user associated with the extension and another with the agent ID that is logged into that extension.

Security

User accounts are also used for controlling access to the system. To be able to login to the website or to connect with a Phone Manager client a valid user account is required. Each user can have a User Role assigned that can control what they do on the system and what they can access.

Users are accessed from the Features -> Users & Business Units section.

9.2.7.8.1 User Auto-Creation

Overview

Depending on the configuration new users can be automatically created. The auto creation can be linked to new devices added or updated on the PBX or when new users are added to a Microsoft® Active Directory Organisational Unit. This way any calls made from that extension will be tagged against this new user.

For example if a new extension is added to the PBX then a new user can be created that is automatically associated with this extension.

> This can be used so that there is no extra configuration required on the Communication Service to enable a new user to connect.

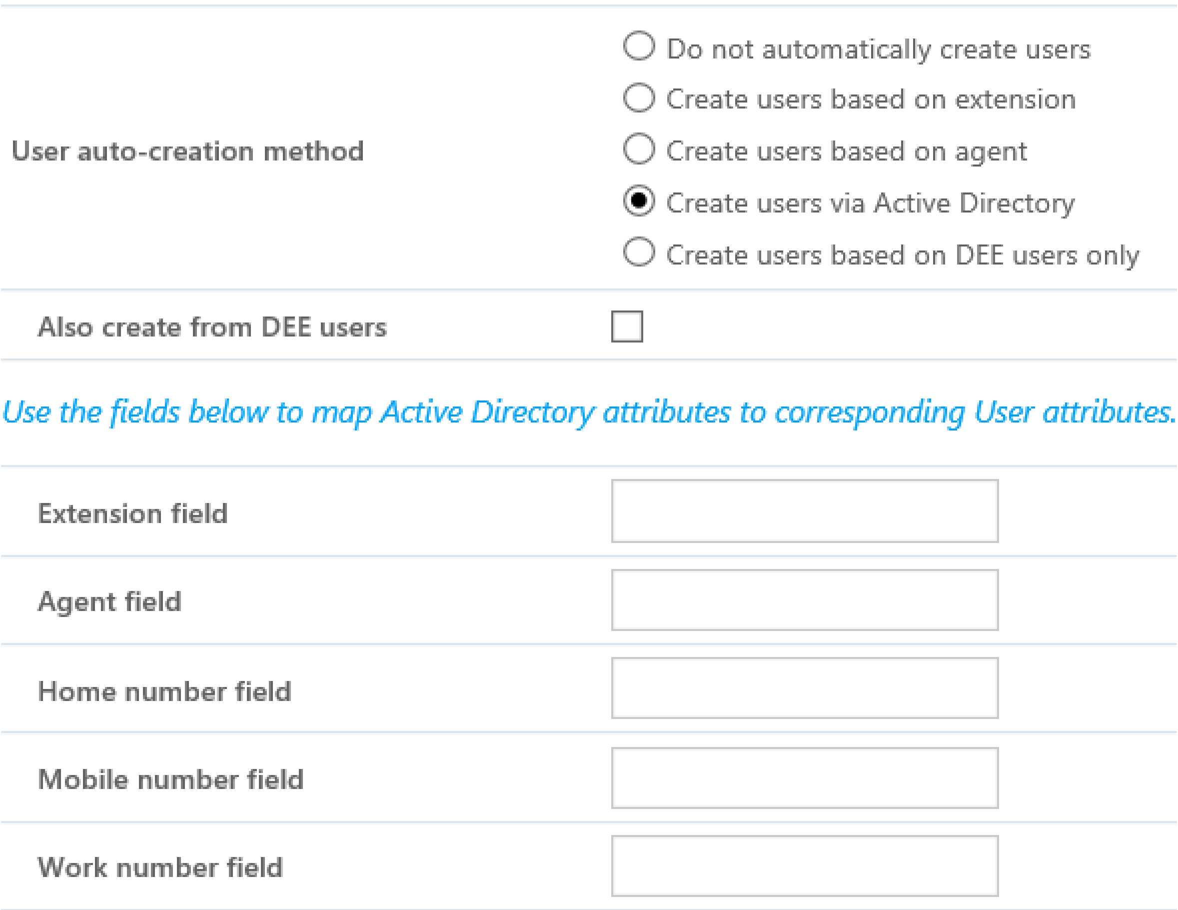
Configuration

To enable auto creation of users:

1. Access the '⚙' -> Features -> Users and Business Units -> User Auto-Creation section.
2. Select the creation method from the options displayed.
3. Click *Save.*

There are four different auto creation methods, select the option that best meets how the PBX is maintained.

1. **Do not automatically create users**: Users will need to be manually created and associated with the correct agent ID and/or extension.
2. **Create users based on Extension**: Users will be automatically created when a new extension is created in the PBX.
3. **Create users based on Agent**: Users will be automatically created when a new agent ID is created in the PBX.
4. **Create users via Active Directory (AD)**: Users will be automatically created when new Active Directory users are created. When this option is enabled the **Extension field** and **Agent field** options can be configured to map to corresponding AD fields for the user (defaults are *ipPhone* for extension and *pager* for agent). By populating these fields in AD as part of creating a new AD user, this will allow the administrator to also automatically associate the new user with the correct extension or agent ID. The relevant Active Directory Organisational Unit (OU) can also be associated with a specific Business Unit and AD users will be imported into the associated Business Unit automatically. See the Business Units and Active Directory section for details.
5. **Create users based on DEE users only:** Users will only be created for the DEE users programmed on the telephone system. If one of the other **'Create users...**' method is selected then an extra option **'Also create from DEE users**' will appear. This will create user's based on DEE users in addition to the other method chosen.



> If a user in AD is disabled then the associated Communication Service user account will also be disabled, But if a user in AD is deleted then the Communication Service user account will NOT be deleted. It is recommended to disable users in AD then wait until the next scheduled import before they are deleted from AD. This way the user account in Communication Service will be disabled.

> If any of the AD users do not have a surname or a UserPrincipalName then they will not be created as Users on the system.

> When using Agent Hot Desking users will be potentially connecting to multiple extensions. In this scenario add the users Agent ID to the Active Directory agent field, leave the Active Directory extension field blank and set the Phone Manager clients to prompt for extension when the user logs in.
>
> The user would then be temporarily associated with that extension when Phone Manager starts and when they log off this extension mapping would be removed. Please note when the user closes Phone Manager there will be no call history as their user is not associated with an extension.

There are several options that can control when new Users are created,

For Auto-creation by Extension or Agent ID:

Rename users when device changes: This is useful in situations when a new member of staff starts and an existing extension/agent ID is recycled and allocated to them. Any calls from the point when the name was changed will then automatically be associated with this new user.

> **Do not enable this when using any form of Hot Desking. If enabled, new users will be created each time a user logs in with their hot desk id.**

When auto user creation by extension or agent ID is enabled the following scenarios apply:

- Changing the description column against an extension or agent in the phone system without blanking out the description column will rename an existing User

- Blanking the description column against an extension or agent in the phone system then setting a new description will create a new User and assign the extension/agent to that user
- Blanking the description column and entering no description will leave the extension assigned to the last user
- Blanking the description column and setting a new description that matches an existing user will NOT associate the new User to the existing User. Instead a new User will be created

Ignore non-alphabetic prefix: This prevents new Users being created if the name configured on the PBX starts with a non-alphabetic letter.

Ignore all uppercase: This prevents new Users being created if the name configured on the PBX is all in upper case.

The settings above do not apply unless Users are created by extension or agent ID and will not be visible in the UI if Create Users via AD or Do not automatically create users are selected.

> Users will not be created if the name configured on the PBX is blank.

> Once the auto-creation has been enabled then any new agents and/or extensions created will have associated users created and these will be shown in the Unassigned Users Business Unit.

Create users for new PM connections: This configuration option is valid for Windows Domain environments only. If a Phone Manager client attempts to connect to the server with a domain account not known by the server, a new User will automatically be created. This will associate a Phone Manager client profile and role without any further configuration.

> This option only works for Active Directory Domain environments when the server and the client are both connected to the AD domain.

Default Client Profile: This is the default client profile that will be applied to new users.

Default Role: This is the default role that will be applied to new users.

If no users have been created for any agents/extensions that already exist then click *Import Now* to create them.

9.2.7.8.2 Manually Creating Users

Overview

Follow this procedure to manually create a new user.

Configuration

To create a new user:

1. Access the Features -> Users & Business Units section.
2. Select the parent business unit that this new User will belong to.
3. Click *New* underneath the list of users on the right hand pane, or right click in the right hand pane and select *New User*.
4. On the *Account* tab enter the following details.
    - **First name**: The first name of the user, this is used to tag against any calls that they are associated with.
    - **Last name**: The last name of the user, this is used to tag against any calls that they are associated with.
    - **Email**: This is the email address used by MCS to contact the user.

    > The default password for a user when it has been created automatically when based on extension or agent is Ext3ns10n.

    - **Username**: This is the username required for the user to access the website. Use this if not using Windows username to authenticate
    - **New password**: This is for changing the current users password, enter the new password here or leave blank to keep the existing password.
    - **Windows Username**: If Windows Authentication is being used then configure the Active Directory Domain username. See Website for details.
    - **Role**: The User Role to associate this user with. Their specifies what rights they have if they login to the server website UI.

    > If a user is not granted any role then they cannot login to the website, but they will have their user linked to calls with the associated agent or at the extension.

    - **Client Profile**: This is the client profile for this User if they require Phone Manager access. This is what assigns the license features to the user's Phone Manager software. See the Client Profiles section for details.
    - **Hide call information for this user from other users:** When enabled, any caller ID for external calls the user is receiving or making will not be visible to other users via the contacts screen within Phone Manager.
    - **Disable user:** This can be used to stop the user being able to connect as a Phone Manager client.
5. On the *Information* tab enter the following details. This information can also be configured from the Phone Manager client under Settings -> User Preferences.
    - **Save Hot Desk passcode**: When this option is enabled the user's passcode will be saved and automatically entered when they login with their Hot Desk Profiles using Phone Manager.
    - **Hot Desk passcode**: This is the users hot desking passcode for their hot desk profile. This can be blank.
    - **Log Hot Desk off on shutdown**: When this is checked and the user closes Phone Manager then their hot desk extension will also be logged out.
    - **Voicemail box:** This is the user's mailbox number. This will default to be the same as the user's Primary Extension

- **Prompt for Voicemail passcode:** When this is enabled Phone Manager will prompt the user for passcodes when accessing voicemails. If not, the user will have to enter the passcode using DTMF on the extension or the Phone Manager Dial Pad.
- **Save Voicemail passcode:** Enabling this option allows Phone Manager to persistently store the user's mailbox passcode for future attempts.
- **Voicemail passcode:** This is the users voicemail passcode. This is used to automatically access their voicemail mailbox when retrieving messages. This can be blank.
- **Meet-Me access code:** If applicable enter the user's Meet-Me conference access code. This will be used by the @ACCESSCODE variable when creating Microsoft® Outlook calendar appointments in the Phone Manager Outlook Add on (see Application Support document for Microsoft Outlook)
- **External Direct Dial**: This number is the external direct dial for the user's Primary Extension. This is used by Phone Manager Mobile to avoid having to dial through the Auto Attendant.

6. On the *Devices* tab enter the following details
   - **Primary Extension**: This should be set to be the user's main extension. If the user is a Hot Desk user then this should be their Hot Desk extension. If the user is user DEE on the telephone system then this should be their main DEE extension. Any calls made on this extension will be logged against the user historically.
   - **Secondary Extensions**: any secondary extensions in use by the user should be added here if the call history needs to be logged against the user.
   - **Primary Agent**: This is the primary agent ID in use by the user. This ID will be displayed to the user in the Phone Manager UI when they attempt to log in. If the user is using Phone Manager Outbound then this agent ID will be used it the sync ACD agent status feature is being used.
   - **Secondary Agents**: Any other agent IDs the user may need to use.

> Any calls made on extensions that have been mapped to a user will be logged against that user. An extension can only be mapped to one use at a time.

> If the user's Primary Extension is a DEE extension then the DEE internal extensions will display as read-only on this page. To see the DEE devices you will need to close and re-open the form is a Primary Extension has just been assigned.

7. On the *Numbers* tab enter the following details
   - **Outside Numbers**: Any external numbers the user may be contacted on. When these are configured other users will see these numbers in the list of available numbers when they dial them from the Phone Manager contacts window.
   - **Active Directory (Home, Mobile, Work)**: If the user is linked with an Active Directory account then their external numbers will appear read-only here,

> If the user's Primary Extension is a DEE extension then the DEE external numbers will display as read-only on this page. To see the DEE devices you will need to close and re-open the form is a Primary Extension has just been assigned.

> If using the Chrome browser it is advisable to disable the Auto-Fill feature for this website. If using Auto-Fill Chrome can auto populate the username/password fields of a created/edited user with those of the currently logged in user. If this happens an error will occur when saving the user because the username already exists.

9.2.7.8.3 Searching Users

Overview

To find existing users on the system there is a search field that will find users containing the search criteria entered.

Configuration

To search for an existing user:

1. Access the Features -> Users & Business Units section.
2. Enter the search term in the **Find user** text box.

   > Searching can be performed using either the first name or last name and also the associated agent id or extensions if configured. Matching is performed using a fuzzy match query, so entering only partial search terms will match any users that have the term contained within. Matching is not case sensitive.

3. Click on *Search*.
4. Any matching users are shown on the right hand panel.

9.2.7.8.4 Editing Users

Overview

Follow this procedure to edit an existing user.

Configuration

To edit a user:

1. Access the Features -> Users & Business Units section.
2. Find the user to edit and then select them.
3. Click *Edit* underneath the list of users on the right hand pane, or right click on the user and select *Edit*.
4. Enter the user details in the dialog box.
5. Press *Save*.

> ⚠ If using the Chrome browser it is advisable to disable the Auto-Fill feature for this website. If using Auto-Fill Chrome can auto populate the username/password fields of a created/edited user with those of the currently logged in user. If this happens an error will occur when saving the user because the username already exists.

9.2.7.8.5 Deleting Users

Overview

Deleting a user will not permanently delete the user but instead move them to the Deleted Users Business Unit so as to enable call history logs that have been assigned to this user to be retrieved. The associated agent IDs and extensions will be unlinked from the user to prevent any further calls been tagged, as will their User Role to remove their access to the Communication Service website.

Permanently Deleting Users.

Users can also be permanently deleted and this will remove all users settings and any historical information related to this user. This will not remove any call information only remove the link from this user to the calls.

> This is a one way process and the user cannot be retrieved once this has been done.

Active Directory Users

When using Active Directory User Auto-Creation if a user is deleted then it will not be recreated automatically by the Active Directory import as it will still exist in the Deleted Users Business Unit. If the user is permanently deleted then it will be imported again with the next scheduled Active Directory import. By default this runs once an hour.

Configuration

To delete a user:

1. Access the Features -> Users & Business Units section.
2. Search, find and select the user to delete.
3. Click *Delete* underneath the list of users on the right hand pane, or right click on the user and select *Delete*.
4. Press *Delete*.

To permanently delete a user:

1. Follow the procedure to delete a user above.
2. Access the Features -> Users & Business Units section.
3. Open the Deleted Users Business Unit.
4. Find and select the user to delete.

   > The *Find user* search cannot be used as this does not include deleted users.

5. Click *Delete* underneath the list of users on the right hand pane, or right click on the user and select *Delete*.
6. Press the *Delete* button to permanently remove this user.

9.2.7.9 Security

Overview

The security features of the system can be controlled through this section. This includes the password policies that are to be enforced so that they can match the local requirements that are in place. Access control to the system can be managed with User Roles that determine what a user can see and configure on the system.

Configuration

To configure the Security Policies:

- See the Security Policy section.

To configure the User Role:

- See the User Roles section.

9.2.7.9.1 Security Policy

Overview

The security policy controls the password policies that are to be enforced on the system. This is a global option for all users and if changed will enforce a user to meet these requirements when they next change their password.

Configuration

To configure the security policy settings:

1. Access the Site Settings -> Security -> Security Policy section.
2. Select the **Password strength.** There are 3 levels of policy that can be used:

Level	Description
Low Security	Password must be at least 6 characters long
Secure	Password must be at least 8 characters long and contain at least one lower case letter, one upper case letter and one digit
High Security	Password must be at least 10 characters long, contain at least one lower case letter, one upper case letter, one digit and one special character (#@?!£$%^&*-=+)

3. **Enable password expiration**: This forces the user to change their password after a certain amount of time. Once enabled, the **Password expire after** setting is displayed.
4. **Passwords expire after**: This is the amount of time in days that a user will have to change their password.
5. **Prevent password reuse**: This enforces password history so that the same password cannot be used repeatedly.Once enabled, the **Passwords to compare** setting is displayed.
6. **Passwords to compare**: The number of previous passwords to store to prevent reuse.
7. **Enable account lockout**: This is the maximum number of failed logon attempts (i.e. wrong password entered) for a user until the account becomes locked out for a period of time. Once enabled, the **Max login attempts** and **Account lockout duration** settings are displayed.
8. **Max login attempts**: The maximum number of failed login attempts before a lockout is enforced.

   > The number of failed login attempts is only reset back to 0 on a successful login.

9. **Account lockout duration**: The number of minutes that the account is locked.
10. **Reset All Password**: This causes all users to change their passwords when they next login.

    > This does not apply to Active Directory users.

9.2.7.9.2 User Roles

Overview

User Roles are used to enforce security and access permissions for all Users that interact with the MCS. Roles are used whenever a user logs into the website in order to determine what rights they have within the user interface or to restrict the users to Phone Manager use only.

Configuration

To configure the security policy settings:

1. Access the Site Settings -> Security -> User Roles section.
2. Click on *New.*
3. Enter a short descriptive **Name** that is used to reference the role in other forms.
4. Enter a **Description** that provides more information on what this role is used for.
5. Select the **Security Profile** to use.
6. Click on *Save* to save the new role.

9.2.7.9.2.1 Security Profiles

Overview

A security profile contains a list of the areas on the system that a user can have access to and configure. There are four default profiles available but custom profiles can also be created if needed.

1. **Admin**: This is the profile associated with the engineer account. This profile cannot be edited. This profile should only be used to give permissions to trained engineers who need to configure the essential components of the system.
2. **Supervisor**: This profile is for supervisor level access and gives access to features required for every day management tasks.
3. **User**: This profile can be used to give general users access to the website to edit their password.
4. **Phone Manager Only**: This profile grants no access and prevents the user from being able to login to the website.
5. **Phone Manager with Playback:** This profile grants access to use Phone Manager and playback calls from the call history tab.
6. **Recording Only:** This profile grants the user access to the website and the recordings playback area.
7. **Reporting Only:** This profile grants the user access to the website and the reporting area.
8. **Wallboard Only:** This profile grants the user access to the website and the real-time wallboard.
9. **Dashboard Only:** This profile grants the user access to the website and the real-time dashboard.

Any user account can connect as a Phone Manager user as long as they have been assigned a Client Profile.

Configuration

The default configurations for the built in security profiles are shown below.

Option	Description	Admin	Supervisor	User	PM Only	PM with Playback	Recording Only	Reporting Only	Wallboard Only	Dashboard Only
General										
Allow web access	Allows the user to log on to the MCS website.	✓	✓	✓	✗	✗	✓	✓	✓	✓
Create & modify tasks	For future use.	✓	✓	✗	✗	✗	✗	✗	✗	✗
View System Status	The user can view the system status area including alerts	✓	✓	✗	✗	✗	✗	✗	✗	✗
View Audit Trail	For future use.	✓	✓	✗	✗	✗	✗	✗	✗	✗
View System Business Units	The user can view the system Business Units for deleted and unassigned users.	✓	✓	✗	✗	✗	✗	✗	✗	✗
View shared filters	The user can view shared filters that have been created on the system.	✓	✓	✗	✗	✗	✓	✓	✓	✓
Modify shared filters	The user can create and manage shared filters.	✓	✓	✗	✗	✗	✓	✓	✓	✓
Recordings										
Play recorded calls	Allows the user to playback their own calls through Phone Manager if the system is linked to a call recording system.	✗	✓	✓	✗	✓	✓	✗	✗	✗
Save	The user is able to save call recordings locally.	✗	✓	✓	✗	✗	✓	✗	✗	✗
Email	The user is able to email out call recordings.	✗	✓	✓	✗	✗	✓	✗	✗	✗
Silent Monitor	The user can listen in to live calls from the website.	✗	✓	✓	✗	✗	✓	✗	✗	✗
Delete Recordings	The user is able to delete recordings from the system. Until this option is enabled the Recording Deletion option will not be	✗	✗	✗	✗	✗	✗	✗	✗	✗

	visible in the user interface.									
Modify Call Details	The user is able to edit call details such as custom tags, notes and change the assigned user of a call.	✘	✔	✔	✘	✘	✘	✘	✘	✘
Live View	The user is able to configure their recordings page to automatically refresh.	✘	✔	✔	✘	✘	✔	✘	✘	✘
Reporting										
Run reports	The user has access to the reporting section to run and view reports.	✔	✔	✘	✘	✘	✘	✔	✘	✘
Schedule reports	The user has access to schedule automated reports.	✔	✔	✘	✘	✘	✘	✔	✘	✘
Real-Time Access	Controls real-time reporting access on the website.	✔	✔	✘	✘	✘	✘	✘	Wallboard	Dashboard
Phone Manager Outbound Settings										
Allow web access	Gives the user access to the Phone Manager Outbound website.	✔	✔	✘	✘	✘	✘	✘	✘	✘
Campaigns	Gives the user varying levels of access to view or edit Campaigns.	✔	✔ (full)	✘	✘	✘	✘	✘	✘	✘
Dispositions	Gives the user varying levels of access to view or edit Disposition codes.	✔	✔ (full)	✘	✘	✘	✘	✘	✘	✘
Imports	Gives the user access to view and edit import details.	✔	✔	✘	✘	✘	✘	✘	✘	✘
Exports	Gives the user access to view and edit export details.	✔	✔	✘	✘	✘	✘	✘	✘	✘
Reports	Gives the user access to view and edit reports.	✔	✔	✘	✘	✘	✘	✘	✘	✘
Schedules	Gives the user access to view and edit schedules.	✔	✔	✘	✘	✘	✘	✘	✘	✘
Barred Numbers	Gives the user access to view and edit barred number tables.	✔	✔	✘	✘	✘	✘	✘	✘	✘
Edit system settings	Gives the user access to view and edit system settings.	✔	✔	✘	✘	✘	✘	✘	✘	✘
Configuration Area Settings										
Contact Directories	Gives access to the Contact Directories configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Server Applications	Gives access to all areas under the Applications section of the MCS website.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Phone Manager configuration	Gives access to the Phone Manager configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Macros	Allows a user to manager published macros on the website.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Call Banner	Allows a user to edit	✔	✘	✘	✘	✘	✘	✘	✘	✘

Profiles	call banner profiles.									
Client Toolbars	Allows a user to edit client toolbars.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Call Categorization	For future use.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Phone Systems	Gives access to the Phone Systems configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Exclusion List	Gives access to the Exclusion list configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Inclusion List	Gives access to the Inclusion list configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Call Reporting	Gives access to the Call Reporting configuration section.	✔	✘	✘	✘	✘	✘	✔	✔	✔
Dial Plan	Gives access to the Dial Plan configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Custom Tags	Gives access to the Custom Tags configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Email	Gives access to the Email configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Database Maintenance	Gives access to the Database Maintenance configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Security	Gives access to the Security Policy and User Roles configuration sections.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Users & Business Units	Gives access to the Users & Business Units configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Compliance Muting	Gives access to the Compliance Muting configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Servers	Gives access to the Servers configuration section.	✔	✘	✘	✘	✘	✘	✘	✘	✘
Manage License	The user can activate, deactivate and update the system license.	✔	✘	✘	✘	✘	✘	✘	✘	✘

To give users access to the Recordings section of the website, assign them an Access Filter or Access Scope.

9.2.7.9.2.2 Access Scope

Overview

Every user belongs to a Business Unit, the Access Scope defines the calls the user has access to relative to their assigned Business Unit. Then if a user is moved between Business Units then their Access Scope will be changed automatically based upon their position.

The following options are available:

- **None**: The user does not have access to any calls.
- **Own calls**: The user only has access to their part or segment of each call they are associated with.
- **Business unit**: The user has access to any calls assigned to their Business Unit, but not any child Business Units.
- **Business unit master**: The user has access to any calls assigned to their Business Unit and any child Business Units.
- **Site**: The user has access to any calls within a specific site.
- **Organisation**: The user has access to any call from any site within a specific organisation.

The Access Scope is applied to an Access Filters.

> A user must have an Access Scope or Access Filter before they will be given access to the Recordings section of the website.

9.2.7.9.2.3 Access Filters

Overview

A user can be given access to or denied access to calls in addition to their Access Scope by assigning them to a configured Access Filter. Additional information associated with a call can then be used to create the Access Filter including adding additional Business Units.

> Before using Access Filters consider if you can configure the Business Units to achieve the desired result more easily via the Access Scope. The Access Filter should only be used for exception cases.

Configuration

To configure the Access Filter:

1. Access the Site Settings -> Users & Business Units -> User Roles -> Access Filters configuration section.
2. Click on *New* to open the Access Filters details.
3. Configure the filter, see the Add and Edit Access Filter section for details.
4. Click on *Save*.

The new access filter will then be displayed on the grid and can be used within the User Roles section.

> A user must have an Access Scope or Access Filter before they will be given access to the Recordings section of the website.

9.2.7.9.2.4 Add and Edit Access Filter

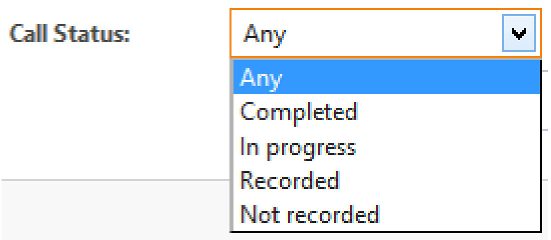
Overview

Use the following procedure to configure the Access Filters.

Configuration

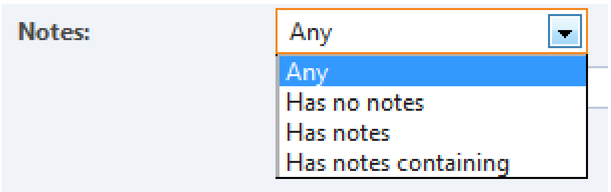
To add or edit an access filter:

1. Access the Site Settings -> Security -> User Roles -> Access Filters -> Add and Edit Access Filter configuration section.
2. On the *General* tab configure the details.
   - **Name**: The descriptive name used to help identify this filter in other forms.
   - **Access mode**: Is this filter a grant (i.e. allow access to everything configured) or deny (restrict access to anything configured).
3. On the *Basic* tab configure the details.
   - **Outside number:** The outside number presented for this call. For inbound calls this is the caller ID and for outbound calls this is the dialled number. Wildcards can be used to generalise the search, for example *09%,* any calls that have an outside number starting with 09 would be matched.
   - **Extensions**: A specific extension or range of extensions. For multiple extensions separate each one with a comma and for a range use a dash. For example 1001,1002-1008,1010.
   - **Extension name**: The name configured against this extension.
   - **DDI**: The direct dial number.
   - **Trunk**: The trunk number that the call was connected on.
   - **Duration**: The duration of time that the call was connected for. Use the sliders provided to add a duration to the filter.
   - **Call type**: Was the call either inbound, outbound or internal.
   - **Call status**: Is this call completed, in progress, recorded, not recorded or any of these.

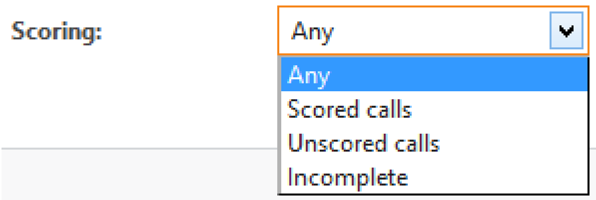


4. On the *Advanced* tab configure the details.

- **Agent IDs**: A specific agent id or range of agent ids. For multiple agents separate each one with a comma and for a range use a dash. For example 1001,1002-1008,1010.
- **Agent name**: The name configured against this agent id.
- **Hunt group name**: The name configured against this hunt group.
- **Hunt group number**: A specific hunt group or range of hunt groups. For multiple hunt groups separate each one with a comma and for a range use a dash. For example 2001,2003-1005,2013.
- **Speed dial name**: The speed dial name associated with the outside number.
- **Account code**: The account code entered against this call.
- **DNIS**: The name associated wit the direct dial number.
- **Notes**: Selects records that have had notes attached or if the notes contain specific words.



- **Serial**: The unique serial number of a specific recording.
- **Scoring**: Selects records that have either been scored or un-scored.



5. On the *Customer Details* tab configure the details.

- **Field 1**: The value stored within custom tag field 1.
- **Field 2**: The value stored within custom tag field 2.
- **Field 3**: The value stored within custom tag field 3.
- **Field 4**: The value stored within custom tag field 4.
- **Field 5**: The value stored within custom tag field 5.

6. The *Business Units* tab allows the user to be selected who need to be applied to this access filter.

9.2.8 Network Shares

Network shares can be used by the following features of the system:

- Scheduling Reports
- Importing/Exporting Campaign Data in Phone Manager Outbound
- Archiving Call Recordings

A share must already have been created on a target server before it can be added here. The grid displayed on the 'Network Shares' section of the website shows all the shares that the system has been told about.

Adding/Editing a Share

To add the details of a network share, press the 'New' button then add the following information:

Description

A unique reference for the share

Server

The IP address or the FQDN/hostname of the server hosting the share.

Share Name

The name of the share on the server hosting it

Sub Folder

Enter a sub folder (or folders) of the share that will be accessed. Alternatively, a sub folder can be set when configuring the usage of the share from a specific feature such as Phone Manager Outbound or Call Archiving.

Requires Authentication

If the system is required to authenticate with the target server when accessing the share, check this box and then enter the username, password and domain which has the necessary read/write permissions.

The 'Test' button can be used to check whether the details provided are correct.

Once a share has been successfully added, review the content of the relevant features on how they can then be used (e.g. Call Archiving, Report Scheduling).

9.2.9 Custom Tags

In addition to all the standard data stored against each telephone call (DDI, CLI, Agent ID, Account Code etc), the MCS provides five custom fields that can be used to store extra customer specific information about a call. This information can be used in search filters to quickly find calls or added to reports. Examples of the type of information stored in these custom fields includes; customer reference numbers, order numbers, fault reference or ticket numbers.

Each of the custom tags can be given a custom name so that on the search and filter screens this description is displayed to the user. For example, Tag Field 1 could be renamed 'Customer Account No'.

Configuration

The custom tag descriptions can be changed at any time and the names on the filters will be immediately updated. To configure the custom tags:

1. Access the Site Settings -> Custom Tags configuration section
2. Enter the required description against each tag in the relevant area

> The Account Code tag is specifically for the account code received from the PBX, if this is supported.

The custom tags can be used to filter from within a Filter Details under the Customer Details tab, within Additional Filters and they can also be configured to be displayed onto the Recording grid or within Reports.

Tagging Calls

The custom tag fields can be populated using one of three different methods:

- Using a Phone Manager Desktop Toolbar button or API
- Using the Call Recorder Client 'Tag' button
- Using the Call Recorder Client Web Service API

For more information about using any of the tagging methods, please refer to the relevant technical guide.

9.2.10 SSL Certificate

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

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

Certificate Properties

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

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

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

Requesting/Using a Trusted Certificate

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

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

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

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

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

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

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

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

For more information on enabling HTTPS on the website, please refer to the Enabling HTTPS section.

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

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

9.3 Servers Settings

Overview

A site can have multiple servers that work together and perform specific roles within the site, for example running the database or hosting the website:

- **WCF Server**: This is a required role for each server and provides core service processes
- **Database**: This role is for the server that hosts the Microsoft SQL Server database. There can only be a single server with this role
- **Licensing**: This role performs the license management and activation process for site. There can only be a single server with this role
- **Website**: This role is for servers that will host the website. There can be multiple servers with this role
- **Communications Gateway**: This role provides integration services for client applications
- **CTI Host Service**: This handles the CTI connection to the PBX for Phone Manager clients
- **Call Logging / Reporting**: These roles handle call logging information and historical reporting
- **Real-Time Reporting:** This role enables the services and features to support MiVoice Office Real-time Wallboard & Dashboard
- **Phone Manager Outbound:** If the Phone Manager Outbound dialler is to be run on this server, this role needs to be enabled.
- **Server Applications:** If Phone Manager or any of the Server applications such as Agent Hot Desking or IP SMDR are used, this role needs to be enabled.
- **Mobile Gateway:** If Phone Manager Mobile Softphones are being used, this role needs to be enabled.
- **Call Archiving / Recording:** These roles handle the MiVoice Office Call Recorder features. (Call Logging must also be enabled)
- **Mitel Handset Support:** This role enables the services that support the Mitel 6900 Series Handsets

It may be necessary to *Add* a server if you wish to split roles across more than one server.

> Some roles will require specific requirements, additional hardware and/or licensing.

Configuration

To create a new server:

1. Access the '⚙' -> Servers Settings section.
2. Click on the *Add* button.
3. Enter a **Server ID** numeric value. This needs to be a value between 1-99 and each server within a site needs to have a unique value.
4. Enter a **Name** to identify this server. This can be a short descriptive name and does not have to be the host name.
5. Enter the **Host name / IP address** for this server.

   > The server must have a static IP address and **NOT** DHCP.

6. Select the roles the new server will have.
7. Click *Save*.

9.3.1 General

9.3.1.1 License

Overview

The Communication Service is licensed with a software key. To activate the license you will need one of the following combinations:

- Voucher number
- Site ID / Serial Number

The default format is the Site ID / Serial number combination. In certain circumstances you may be sent a Voucher Number combination to license the MCS server.

> ⚠ MCS servers are no longer licensed using the Application Record ID and Reseller ID method. If you are not provided with a certificate for either a Site ID/Serial or a Voucher code for your MCS system then please contact Mitel Order Processing.

Configuration

Licensing is activated and updated from the Server License page for the server performing the Licensing role. Follow the relevant procedure below to administer the licensing:

- To activate a new server license see Activating a new license
- To upgrade an existing server license see Upgrade an existing license
- Adding new licenses using voucher codes.

> In future releases there will be support for multiple servers per site to spread load

> ⚠ If the server is installed in a Virtualised environment then it must have a static MAC address assigned. If the MAC address changes after activation then the license will become invalid and the system will stop functioning.

Activating a new license

To activate a new server license using a provided Site ID and Serial Number (or voucher code), either online or offline process for the first time:

1. Make sure you have the license certificate containing the Site ID and Serial number (or voucher code) on hand.

   > The certificate for the MCS will either have a Site ID and Serial number or a voucher code. If you have multiple voucher codes for the MCS server and additional parts then license the MCS first. The other vouchers can be added later to update the license.

2. Navigate to the Server Licensing section
3. Click on the *Activate* button to display the activation form.
4. Enter the **Site ID/Serial Number** (or voucher code) from the license certificate.
5. Enter the **Application Record ID (ARID)** for the telephone system the MCS will be connecting to. (If in a multi-node network, just pick one of the nodes)
6. Enter a **Site name**, this is passed back through during the activation process and should be used to easily identify this specific server for the support group.
7. Select the **MAC Address** to associate this license with.

   > ⚠ It is recommended to use the MAC address that is the main IP address for the server for LAN use. If the MAC address changes or is removed after activation for any reason then the license will become invalid and the system will stop working.

8. Click on *Activate* to start the process.
9. If the process was successful then a confirmation will be displayed. If it fails then a relevant message will be displayed in red.
10. If the server cannot contact the licensing portal then offline activation can be performed.

    > The connection to the Licensing Portal requires HTTPS/SSL access on TCP port 443 from the server that has the license role in order to activate the license.

11. For *Offline* registration you will need to *Download* and save the *LicenseFile.xc2v* to your desktop.
12. Copy the license file to a computer that has internet access.
13. Browse to the licensing portal (www.mitelcommunicationservice.com) from the computer you have copied the license file to.
14. Follow the instructions on the portal.
15. Download the license key file, *LicenseFile.xv2c*, and copy back to the server MCS is installed on.
16. Navigate to the Server Licensing section.
17. Click on the *Process file* button.
18. Browse to the *LicenseFile.xv2c* click on *Process license file*.
19. If the process was successful then a confirmation will be displayed. If it fails then a relevant message will be displayed in red

Once licensed you will need to set up the connection to the PBX see the Phone Systems section for details.

Adding licenses using voucher codes

To upgrade an existing server license using online activation:

1. Access the Servers Settings -> SERVERNAME -> General -> License section.
2. Click on the *Add Licenses* button to start the process. A new form will be loaded on the screen.
3. Add one or more vouchers into the grid by entering them in the UI or uploading a file.
4. Once all the vouchers to be applied have been entered (do not forget to press *Add Voucher),* press the *Apply* button.
5. If the server cannot contact the Licensing portal then offline activation can be performed as above. Follow from Step 10 in the Activate a new license section.

> If the online update fails an offline license update can be performed in the same manner as the license activation in the previous section.

Upgrading an existing license

If new licenses (including SWAS contracts) or version updates have been applied on the license server then they can be downloaded to the MCS server using the Update process.

To upgrade an existing server license using online activation:

1. Access the Servers Settings -> SERVERNAME -> General -> License section.
2. Click on the *Update* button to start the process. The system will then connect back to the Licensing portal to retrieve any new or updated license feature information.
3. If any changes are found then they will be shown in green in the *New Value* section. To apply the license changes click on the *Update* button. Any new features will then be available but may require a restart to take affect.
4. If the server cannot contact the Licensing portal then offline activation can be performed as above. Follow from Step 10 in the Activate a new license section.

> If the online update fails an offline license update can be performed in the same manner as the license activation in the previous section.

Deactivating/moving a license

Sometimes it may be necessary to move the MCS to a new server. This may be to move to better hardware, virtualize the software or because the server running MCS has failed.

If the MCS software is still running and is accessible then it's license must first be deactivated before it can be used again on another server. To deactivate MCS, navigate to the Servers Settings -> SERVERNAME -> General -> License section and press the 'Deactivate' button.

When pressed, you will be asked to confirm your name and the reason for deactivation. You may also be asked to provide a deactivation code. If asked for a deactivation code, please contact Mitel Support who will be able to provide the information required.

If the MCS software is not still running or the server running the software is out of service then you will need to contact Mitel Support to have the license reset before it can be installed on a new server.

> To re-register MCS on a new machine you will need your original certificate which displays your Site ID and Serial number. If you do not have this information then please contact Mitel Support for help.

9.3.1.2 Logging

The system supports the creation of diagnostic logging to aid technical support for fault resolution. The retention limits on the amount of files generated and the size of the log files can be controlled. Automated maintenance can be scheduled to zip the logs to reduce the disk space used. The system will generate log files for all the different services that the are running and store them in separate folders within the log files folder for each of the services.

Configuration

To configure the logging settings:

1. Access the Servers Settings -> SERVERNAME -> General -> Logging section.
2. Configure each of the settings.
   - **Log files folder**: The folder location to store the system logs files.
   - **Max log file size**: Once log files reach this size, they will be archived and a new file created
   - **Event logging:** Enables basic logging information to be generated.
   - **Advanced logging**: This enables extended logging information and can generate a significant amount of information and consume high levels of disk space.

     > ⚠ Only enable this under instruction from a trained engineer.
3. Configure the log archiving settings. The log archiving process is controlled by the Watchdog service on each server. The contents of the log files folder will be compressed into a single zip file and then moved to the archive folder location on a daily basis. The contents of the log files folder are then deleted. Each of the zip files has the date and time within the file name, for example the file **cslogs_20130428010035.zip** was will contain the logs as of the 28th April 2013 at 01:00.
   - **Number of zip files to keep:** The number of archive zip files to keep.
   - **Archive folder**: The location to keep the archive zip files.
   - **Archive time**: The time in hh:mm to perform the daily archive of the logs files.

Download Server Logs

This option can be used to download a ZIP file containing the current day's log files without having to access the server running the MiVoice Office Application Suite directly. The zipped file can be saved locally and then sent to Mitel support as required.

9.3.1.3 Watchdog

The Watchdog is responsible for the start-up of the system. It controls which services should be running (based on role selection), when they should start and proactively monitors them to ensure that are running. If any of the monitored services are stopped, the Watchdog will try and restart them and raise alerts when this occurs.

The Watchdog also provides disk management services to check for low disk space and if using call recording, will check the database to ensure that call records have been added to the database in normal business hours to monitor for potential issues.

To configure which services the Watchdog monitors, edit the roles that have been assigned to the system under Server Settings.

Watchdog Configuration

The following settings provide control over how the Watchdog operates (To access these settings, navigate to 'Configuration -> Servers Settings -> SERVERNAME -> General -> Watchdog' in the configuration area of the MCS website).

Drive space warning threshold

This controls the percentage of free drive space that remains before alerts are raised. The local drives on each server are checked for free space and the Watchdog will raise alerts when the amount of free space drops below this threshold. The current status of each drive is shown on each server's status page in the Dashboard menu.

Reboot server daily

This will perform a schedule reboot of the server each day at 3am.

Check SMTP Settings

When this is enabled and there is an SMTP server configured in the Email configuration, each of the **system admin email addresses** will be used for email alarms. If this fails then an **Alert** in the site dashboard will be raised with the relevant details. No email will actually be sent out. Only a connection attempt tried and only if this fails will an alert be raised.

> If the SMTP connection requires SSL then this option has no effect.

Check database activity

When enabled, the Watchdog will check the call records in the database to ensure that calls are being logged during normal business hours. If no calls are detected when there should be, it could be there is a problem with the system which the Watchdog will raise an alert for.

- **Inactivity warning threshold** -> The time in seconds that needs to elapse between calls before an alert is raised
- **Working hours** -> The alerts will only be raised if no calls have been logged between these times
- **Work days** -> The alerts will only be raised if no calls have been logged on the selected days

9.3.2 Recording

Overview

The Recording section enables the recording configuration for this server to be set.

Configuration	Description
General	This configures the recording file paths, the volume adjustment levels and encryption details.
Recording Sources	This configures what devices are to be recorded and any PBX specific options that need to set for these devices.
Call Archiving	This configures when and how any recordings get moved to archive storage. This can be on server or on a Network Share

9.3.2.1 General

Overview

The General section is used to configure how calls are recorded, i.e. are they encrypted, the volume levels and where they are stored. The devices that are to be recorded need to be configured and enabled here for them to be recorded.

Configuration

To configure the recording settings:

1. Access the Servers Settings -> SERVERNAME -> Recording -> General configuration section.
   - **Recording path**: This sets the location to store the call recordings before they are archived. This is in UNC format and maps to a local share called *Recordings* on the call recording server. This is automatically configured and cannot be manually changed. If the server hostname and/or IP address changes then this will automatically changed to reflect this.
   - **Data volume**: This sets the local drive on the call recorder where the recordings and index files are saved.
   - **Enable volume control**: If this is set then the volume levels for inbound and outbound can be altered. The **Inbound volume** and **Outbound volume** sliders control each side of the call. The range is from -6 to +6 where each increment/decrement results in a 3dB increase or decrease in the volume for the specific side of the call.

     > Volume control is not supported for all recording methods

   - **Encrypt recordings**: This enables encryption of the call recording files, see the Encryption & Authentication section for more details.
   - **Create DAT files**: If this is enabled then a DAT file will be created along with each recording.

     > The data within the DAT file may change based on PBX, recording device and version.

     ```
     [CallId:X22*07]
     [CLI:08453736880]
     [DDI:7864350]
     [Extension:1001]
     [ExtensionName:Reception 1]
     [Direction:Inbound]
     [HuntGroup:2001]
     [Encrypted:True]
     [HuntGroupName:Reception]
     [AurixIndexed:False]
     [NetworkRecordingPath:\\server\Recordings\97201\]
     [LocalRecordingPath:D:\Recordings\97201\]
     [AgentId:1101]
     [AgentName:Jane Doe]
     [Trunk:97201]
     [Serial:97201201304261235046280]
     [StartTime:26/04/2013 12:35:04]
     [AnswerTime:26/04/2013 12:35:04]
     [EndEvent:CallCleared]
     [EventCause:Answered]
     [Segment:2]
     [LogicCallId:X22*07-20130426-XAR]
     [CurrentGlobalCallId:X22*07D20130426-XAR]
     [PrimaryGlobalCallId:X22*07-20130426-XAR]
     [CallerNumber:08453736880]
     [CallerDeviceType:Trunk]
     [CallerDeviceNumber:97201]
     ```

```
[CalledNumber:7864350]
[CalledDeviceType:Extension]
[CalledDeviceNumber:1001]
```

9.3.2.1.1 Recording File Formats

Voice Files

The Call Recorder currently only supports a single **Audio Codec** for saving the recordings.

GSM Format: This is the default format. Often called GSM-FR or GSM 06.10 this uses a bit rate of 13.2 kb/s, in mono format with a sampling rate of 8 kHz.

Format	Bit Rate (kb/s)	Sample Rate (kHz)	Mono/Stereo	Size of Audio file (approx)		Quality
				1 Minute (kB)	1 Hour (MB)	
GSM	13.2	8	Mono	100	5.9	Good

9.3.2.1.2 Encryption & Authentication

Overview

The system has the ability to be able to encrypt and digitally sign the call recordings to prevent unauthorised access and to provide an authentication check that the file has not been tampered or altered since it was generated.

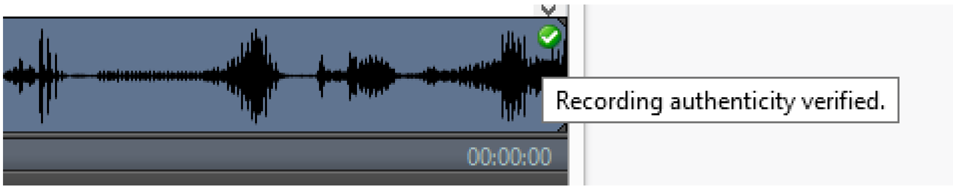
Encryption

The call recording files are encrypted once a call has completed using AES 256 bit industry standard techniques. The files are written to disk with a standard WAV file header but the audio contents of the recording are encrypted. Any attempts to play a recording back directly without it being unencrypted will fail. Access to the recording WAV files is then only permitted through the supported interfaces (i.e. using the website or API components) and they all adhere to the security model enforced on the system.

Encryption is enabled on all systems by default but can be disabled if required from the Servers Settings -> SERVERNAME -> Recording -> General configuration section.

Authentication

The call recording files each have their own authentication header written to the database that is generated once a call has been written to disc. This is a digital signature of the original recording that can be used to verify that a file has not been changed since it was recorded. When a user plays back a recording a digital signature is generated again on the current file and compared against the original signature stored within the database. If they match then the file has not changed since it was recorded. This can be seen on the playback page as a green tick on the top right hand corner of the timeline.



9.3.2.2 Recording Sources

Overview

Recording sources controls what devices are recorded and how the audio from the calls is captured by the system. Depending on the type of recording to be used the recording source will be different.

To enable a device to be selected to be recorded then it must have been configured in the Device Configuration section. The following types of recording sources are supported:

Type	Description
Record-A-Call Configuration	This if for recording of extensions via the Record-A-Call feature on the telephone system
RTP/SIP Interfaces	This if for IP/SIP RTP extensions using Port Mirroring

⚠ Peer-to-Peer Audio must be disabled on the telephone system when using Record-A-Call or RTP/SIP call recording.

9.3.2.2.1 Recorded Devices

Overview

The recorded devices section is where the list of devices to be recorded are configured, if the device is not listed here then it will not be recorded. Each device needs to have an entry in here and to be configured with the required information to be able to identify this device correctly.

Each different type of recorded device requires different information, for example:

- **Record-A-Call**: These devices will be recorded through a SIP Voicemail Record-A-Call stream directly from the telephone system.
- **RTP devices**: These are recorded via a network passive tap or mirror port connection, and to be able to identify the correct device the IP address or MAC address is required.

Configuration

To configure a device to be recorded:

1. Access the Servers Settings -> SERVERNAME -> Recording -> Recording Sources -> Recorded Devices configuration section.
2. This grid shows what devices are to be recorded and what recording method is to be used.
3. To add a new device or devices to be recorded, click on the *Add* button.
    - Select the recording method for this device(s), click *Next*.
    - Select the device(s) from the list shown and click *Save*.
4. To edit an existing device, select the device and click on *Edit*.
5. Depending on the type of device there will be different configuration options that need to be entered.

Record-A-Call

No additional information is required.

IP/SIP RTP Extension

When adding IP/SIP extensions to be recorded, the system needs to know either the MAC or IP address of the extension so that it can match the extension's audio with the data coming from the telephone system. Where possible, the MCS will auto-learn the MAC/IP address of the extensions so that no configuration is necessary here.

Device number: Enter the relevant device number.

MAC Address: Enter the devices MAC address.

IP Address: Enter the devices IP address that will be receive by the recorder.

> If the IP device is on the same subnet as the PBX that it is connected to then the MAC address can be used, otherwise the IP device will need to have a static IP address. If the device is behind any kind of NAT device, for example a remote worker, then their NAT'd/public IP address needs to be used. Only a single device can be configured against an IP address, so each device needs to have its own NAT'd/public IP address.

9.3.2.2.2 Record-A-Call Configuration

The following settings apply to any devices that have been configured to record using the Record-A-Call recording source.

For information on configuring the telephone system for this method of call recording, refer to the Features Section.

Play Pre-Record-A-Call Message

At the beginning of a recording, the MCS can play a message to the parties in the call to inform them that the call is going to be recorded. If this feature is enabled on the MCS, it must also be enabled on the telephone system.

Once enabled, a drop down list will appear from which you can choose which Audio file to use for the message.

The default message that is provided with the system is:

"This call is being recorded for training or monitoring purposes"

A default message for A-Law and Mu-Law is provided, ensure the correct one is used to match the Call Configuration setting for the SIP voicemail on the telephone system.

To change the message, copy a new file to the following location on the MCS server:

'C:\ProgramData\Mitel\Mitel Communication Service\Net Store\Audio files\RecordACall\"

The recordings are required in the following format: *16 bit, 8K, Mono (A-Law or Mu-Law).*

Restrict by IP Address

As part of the Record-A-Call recording source, the MCS server is accepting inbound SIP traffic from the telephone system. In order to stop the recording ports being used by unauthorised devices it is recommended to enter the address(es) of the telephone system here to allow the MCS to ignore IP traffic from other sources.

To add multiple address into the list box, press the 'Enter' key after each address entered to move to a new line.

> If the telephone system is configured with an expansion card or PS-1, enter the Base IP address, Expansion card IP Address and the PS-1 address here.

> A restart of the Call Logging service is required after changing these settings.

> Peer-to-Peer Audio must be disabled on the telephone system when using Record-A-Call or RTP/SIP call recording.

9.3.2.2.3 RTP/SIP Interfaces

Overview

The system supports the recording of IP devices that use standard RTP protocol for the audio by using port mirroring to send a copy of the RTP network traffic to the server. This is a software only solution that requires no physical voice card hardware.

> The RTP/SIP interface recording source must be used when recording Phone Manager Desktop and Mobile softphones.

> Peer-to-Peer Audio must be disabled on the telephone system when using RTP/SIP call recording.

> Only RTP traffic using the G.711 codec is supported.

To be able to capture the RTP traffic the system needs to know the port mirroring network adapters that it needs to listen on and what IP port ranges that the RTP traffic is using.

To configure the port mirroring network adapters:

1. See the Mirror Ports section for details.

To configure the IP port ranges:

1. See the Packet Filters section for details.

9.3.2.2.3.1 Mirror Ports

Overview

The port mirroring network adapter(s) that the system needs to use to receive the RTP/SIP traffic on for recording IP devices is configured from this section. The list of available network adapters is shown and allows the administrator to select the required ones.

The system needs to be able to receive all the RTP traffic that is sent and received from each device that is to be recorded. The easiest way to do this is to have the network connection that the PBX is connected to mirrored and any peer-to-peer media disabled as this will then ensure that all the RTP traffic flows through this connection.

As the network topology of each site can be different this may not be possible. Multiple adapters can be used together so that there can be multiple ports mirrored in different locations so that complete coverage of all the RTP traffic can be provided.

> Not all network hardware, i.e. switches, supports configuring a mirror port. Check your hardware manufacturers specifications to ensure the are compatible.

Configuration

To configure a mirror port:

1. Access the Servers Settings -> SERVERNAME -> Recording -> Recording Sources -> RTP/SIP Interfaces -> Mirror Ports configuration section.
2. From the list of adapters displayed check each one that needs to be used. The **Name**, **IP Address**, **MAC Address** and **Interface** name are provided for each adapter to help identify the correct one to use.
3. Click *Save*.
4. Restart the Call Logging service.

> For more information on setting up a mirror port on a Hyper-V VM, please refer to https://blogs.technet.microsoft.com/networking/2015/10/16/setting-up-port-mirroring-to-capture-mirrored-traffic-on-a-hyper-v-virtual-machine/

> A restart of the Call Logging service is required after changing these settings.

9.3.2.2.3.2 Packet Filters

Overview

When using port mirroring for RTP recording the system needs to know the range of UDP ports that the RTP traffic will be using. Depending on the PBX the range of ports will be different. There are some pre-configured ranges provided that the administrator can select depending on the PBX that the devices are connected to.

If the ranges are not contained with the preset then manual ranges can be configured.

Configuration

To configure the port ranges:

1. Access the Servers Settings -> SERVERNAME -> Recording -> Recording Sources -> RTP/SIP Interfaces -> Packet Filters configuration section.
2. From the preset list select the required entry from the list.
3. Click on *Load preset* to populate the range list.
4. Modify the list of ranges as required.
5. Click on *Save*.

> A restart of the Call Logging service is required after changing these settings.

9.3.2.2.3.3 Addresses

The IP address of the telephone system should be configured here. The MCS uses this information to identity the direction of call traffic when monitoring IP based extensions.

Addresses to add:

- All PBX IP Addresses (including base servers, PS-1 servers and PEC cards)
- Addresses for each node the system is monitoring IP extensions on

These addresses should be populated any time IP/SIP Extension recording is being used.

To add multiple address into the list box, press the 'Enter' key after each address entered to move to a new line.

> A restart of the Call Logging service is required after changing these settings.

9.3.2.3 Call Archiving

The system records all calls to the default recording path (configured under a server's General recording settings) which should be on the local server. As the server may only have a limited amount of storage available, archiving is essential to ensure that it does not run out of disk space. Call recordings can be archived to network based storage devices (for example a SAN or NAS) to stop the system running out of storage space.

> ⚠ If the server does run out of disk space then it will STOP recording any further calls until free space is made available. It is important to ensure that calls are archived or retention policies are used to stop this happening.

Call archiving moves the original recording files and DAT files to the configured destination(s) and then removes the original files. This minimises the risk of the system running out of disk space and allows for an unlimited amount of storage to be made available as additional storage can be added as and when required. Files can be copied to multiple destinations so that multiple copies can be kept. Limits can also be configured so as to allow only calls older than a specific date to be archived.

The call archiving works in combination with the Database Maintenance, calls will not be archived until they been through this process and the data associated with the call has been added to an archive database. If call archiving has not been used for some time then when this is started it will begin to archive the calls as long as they have been through the database maintenance. For large volumes of calls this can take a significant amount of time and resources whilst in progress, typically this is why archiving should always be running.

Configuration

To enable call archiving:

1. Access the Servers Settings -> Call Archiving configuration section.
2. Check the **Enable call archiving** option.
3. The archiving will not start without at least one archive location being set. See the Archive Locations section.
4. To prevent calls from being archived for a specific period of time set the **Archive delay** option. This will only archive calls that are older than what has been configured. If this is set to 0 then all completed calls will be archived.
5. Network Shares to archive to must first be configured before Archive Locations can be added.
6. Any changes made to the call archiving require a restart of the call archiving service.

9.3.2.3.1 Archive Locations

Call recording archive locations are a group of destinations that are used to copy files to. Multiple locations can be configured for archiving, files are duplicated across each of the destinations configured. A maximum of 5 separate destinations can be configured.

The archive locations are monitored to ensure that there is enough drive space available and that the correct permissions have been set. If the archive locations are not accessible or low on space then an alert will be raised.

The amount of space available is also shown on the Drive Information section on the Dashboard.

Configuration

To add an archive location:

1. Access the Servers Settings -> SERVERNAME -> Call Archiving configuration section.
2. Click on the *Add* button.
3. Select the Network Share from the list or click 'New Network Share' to add the details for a new one.
4. Click *Add*.

To remove an archive location:

1. Access the Servers Settings -> SERVERNAME -> Call Archiving configuration section.
2. Click on the location to remove and select *Delete*.

9.3.3 Website

Overview

The website configuration may need to be modified from the standard configuration depending on the environment that this is used in.

Configuration

To configure the website settings:

1. Access the Servers Settings -> SERVERNAME -> Website section.
2. Configure the settings.
    - **Use Windows Authentication:** This enables the website User Interface (UI) to be accessed using the current user's Active Directory Windows domain login profile. This requires each user to have their Windows Username configured against their User settings. When a user connects to the website and if they have a valid Windows login then they can access the website UI directly without needing to enter their login credentials.
    - **Website URL**: This is the URL that is to be used to access the server. If this field is left blank, the server hostname will be used instead.

> If the server is to be accessible over the Internet and ports have been forwarded through to the server, this needs to be set to the fully qualified domain name for the external IP address, for example https://server.domainname.com. This field is used if the system ever sends an email to a users containing a link to the server website.

  - **Domain redirect**: If this is enabled then the website will redirect/forward any visitors to the configured *Website URL*.
  - **Default language**: This sets the default language that is shown on the logon page before a user logs in. A user can then override this once they are logged in via My Settings.
  - **Session timeout**: This is the number of minutes before a session times out due to inactivity after which the user have to log back in to continue. When the session timer is about to expire then the user will be prompted with a warning.

    > The session timeout has no affect when using Windows Authentication.

  - Click on .

10 My Settings

Overview

Each user that is logged in has access to change their details, including first name, last name, password and email address. This is accessed by clicking on the Users name from the top right hand corner of the webpage page once they are logged in.

Once any changes have been made click on *Save* to save the changes. This will also prompt to enter your password as an additional security check. If you need to remove any changes that you have made click on the *Reset* button.

Preferred Language

By default this is not set, the website will use the browsers default language. If set, the website will be presented in the language selected.

Recordings - LiveView Refresh Rate

If the user has enabled the live view refresh on the recordings grid then this setting controls how quickly the grid automatically refreshes.

11 How To's

11.1 Backup the SQL Server Databases

Overview

The Microsoft SQL Server databases are critical as they contain all of the configuration details of the system and all of the call information for every call that has being recorded. If these are lost or corrupted then without a reliable backup you will not be able to search and playback calls using any of the meta data associated with those calls.

Having a reliable and up to date backup of these database enables the system to be recovered in a short period of time without any loss of historical information (up to the point of the last backup).

The system does have built in processes to maintain and backup the databases - see the Database Maintenance section for details.

How To

To backup all of the databases follow this procedure:

1. Log on to the server with the database role.
2. From the Start Menu open *Microsoft SQL Server 2008 R2 -> SQL Server Management Studio*
3. Set the *Server type* to *Database Engine*.
4. Set the *Server name* to "(local)\MCS".
5. Enter valid *Authentication* details.
6. Click on *Connect*.
6. Select *File -> New -> Query with Current Connection.* This will open a new query window within SSMS.
7. Copy this script into the new query window. This script is configured to backup all the database to the default destination of "c:\Backup\".

> ⚠ Before running this script ensure that there is enough free disk space on the relevant backup drive location.

```
DECLARE @name VARCHAR(50) -- database name
DECLARE @path VARCHAR(256) -- path for backup files
DECLARE @fileName VARCHAR(256) -- filename for backup
DECLARE @fileDate VARCHAR(20) -- used for file name

-- specify database backup directory
SET @path = 'C:\Backup\'

-- specify filename format
SELECT @fileDate = CONVERT(VARCHAR(20),GETDATE(),112)

DECLARE db_cursor CURSOR FOR
SELECT name
FROM master.dbo.sysdatabases
WHERE name NOT IN ('master','model','msdb','tempdb')  -- exclude these
databases

OPEN db_cursor
FETCH NEXT FROM db_cursor INTO @name

WHILE @@FETCH_STATUS = 0
BEGIN
       SET @fileName = @path + @name + '_' + @fileDate + '.BAK'
       BACKUP DATABASE @name TO DISK = @fileName
```

```
        FETCH NEXT FROM db_cursor INTO @name
END

CLOSE db_cursor
DEALLOCATE db_cursor
```

8. Click on the *Execute* button to start the backup. The time to run the backup will vary considerably depending on the size of the databases, the speed of the destination backup location and the performance of the server that this is running on.

9. Once complete the results window underneath the query window will show if the backup was a success.

10. Ensure that the backups are copied onto a reliable external storage device.

11.2 SMTP Configuration for Gmail

Overview

The Communication Service can integrate into Google's Gmail system for email.

How To

MCS Configuration

Use the following settings in the Email & SMTP section replacing any place holders with the user specific information:

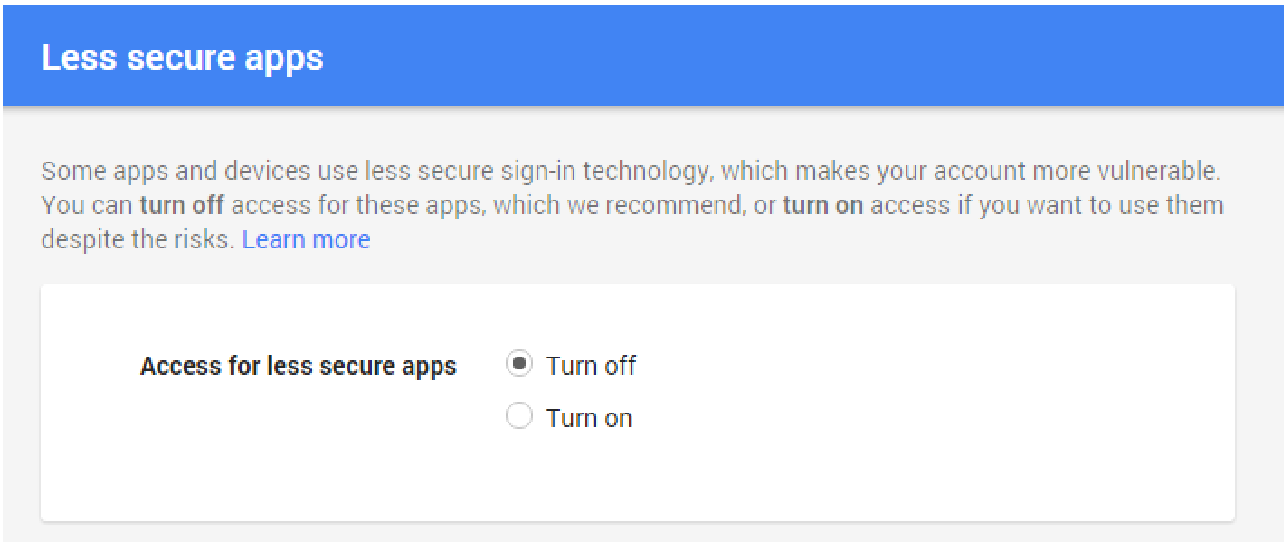
- **System admin email address**: <username>@gmail.com
- **Source email address**: <username>@gmail.com
- **SMTP server**: smtp.gmail.com
- **Server require authentication**: Yes
- **Username**: <username>@gmail.com
- **Password**: <password>
- **Use SSL/TLS**: Yes
- **Alternate Port**: 587

Gmail Configuration

Gmail now requires that a 'less secure' option be enabled for allowing access using SMTP authentication over SSL. You will need to browse to the following URL and 'Turn On' access:

https://www.google.com/settings/security/lesssecureapps

Example Image:



11.3 SMTP Configuration for Office365

Overview

The Communication Service can integrate into Microsoft's Office365 system for email.

How To

Use the following settings in the Email & SMTP section replacing any place holders with the user specific information:

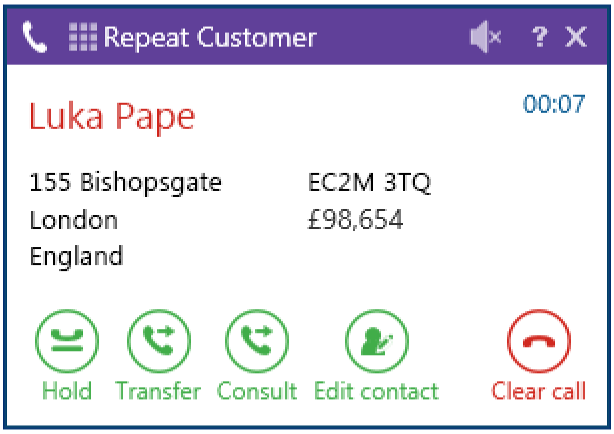
- **System admin email address**: <username>@office365.com
- **Source email address**: <username>@office365.com
- **SMTP server**: smtp.office365.com
- **Server require authentication**: Yes
- **Username**: <username>@office365.com
- **Password**: <password>
- **Use SSL/TLS**: Yes
- **Alternate Port**: 587

11.4 Banner Profiles VIP

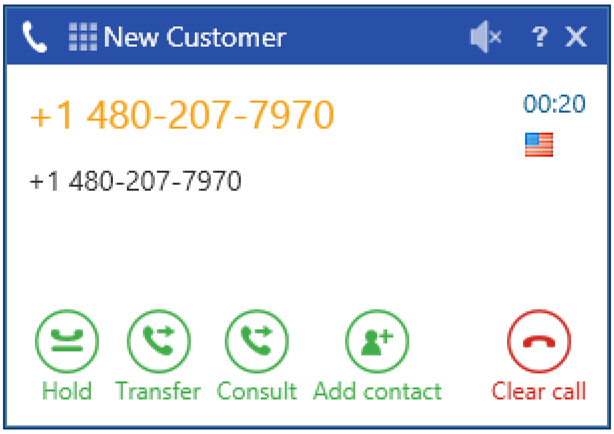
Overview

This example shows how to create call banner profiles that will highlight differently when either a repeat customer or a new customer calls in on a specific DDI/DID number. This will use check VIP text field of a contact that has been imported into a global directory that is set to "Repeat Customer".

When a repeat customer is matched this banner will be shown. As the customer is already known then their details can be shown on the banner, i.e. their name, address and account balance.



When a new customer is matched, i.e. they don't have the VIP text set then this will be shown. As the customer is new then they only information that is available is their telephone number and location.



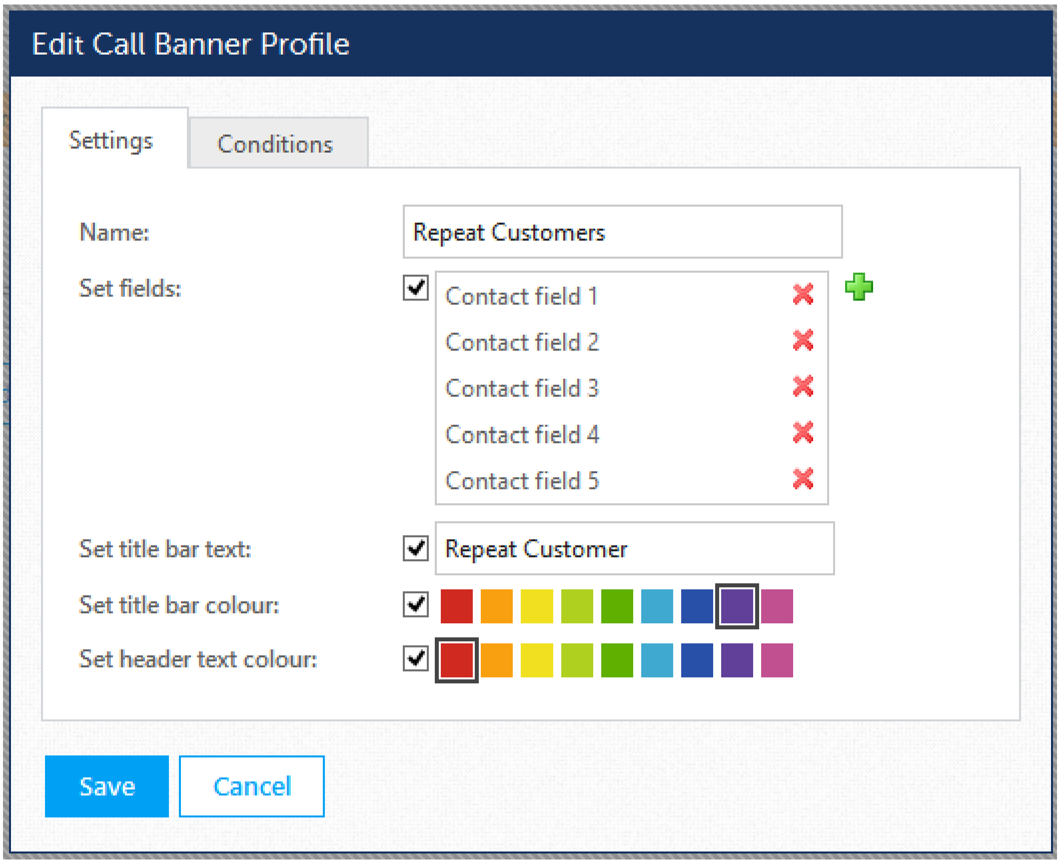
How To

To create the configuration start from the Call Banner Profiles section:

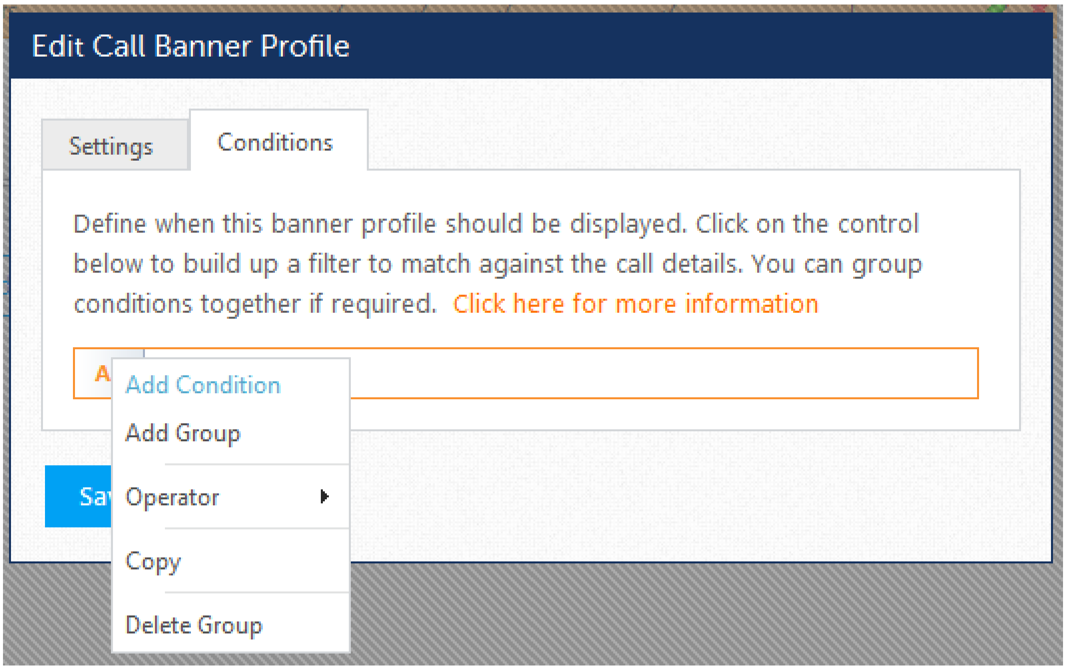
'⚙' -> Features -> Phone Manager Desktop -> Call Banner Profiles section.

There will need to be two new call banner profiles created, one for the repeat customers and the other for new customers. To create the repeat customer profile:

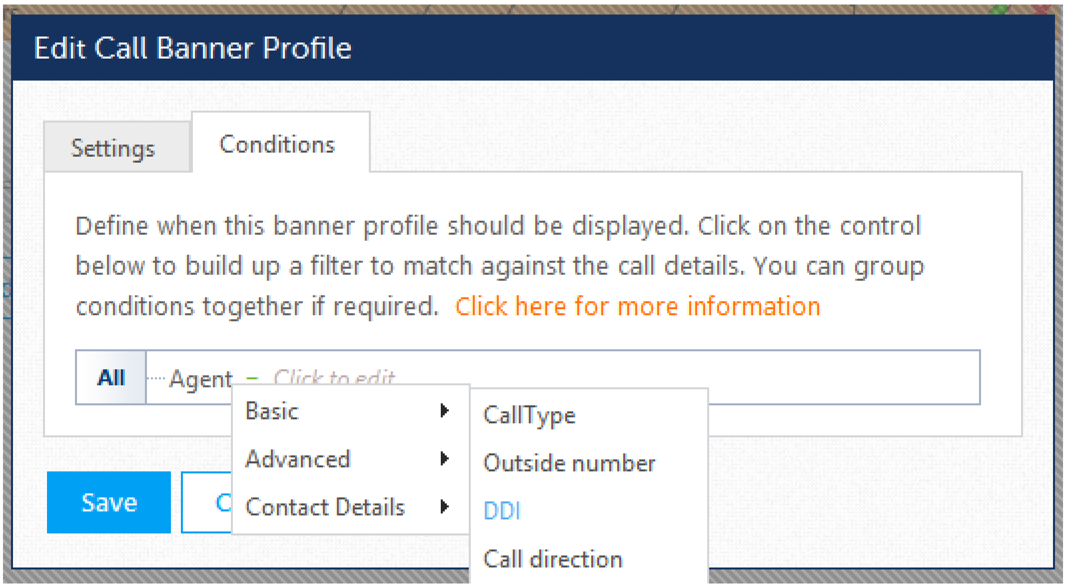
1. Click on *New* then configure the profile settings as shown so that the import contact information will be displayed:



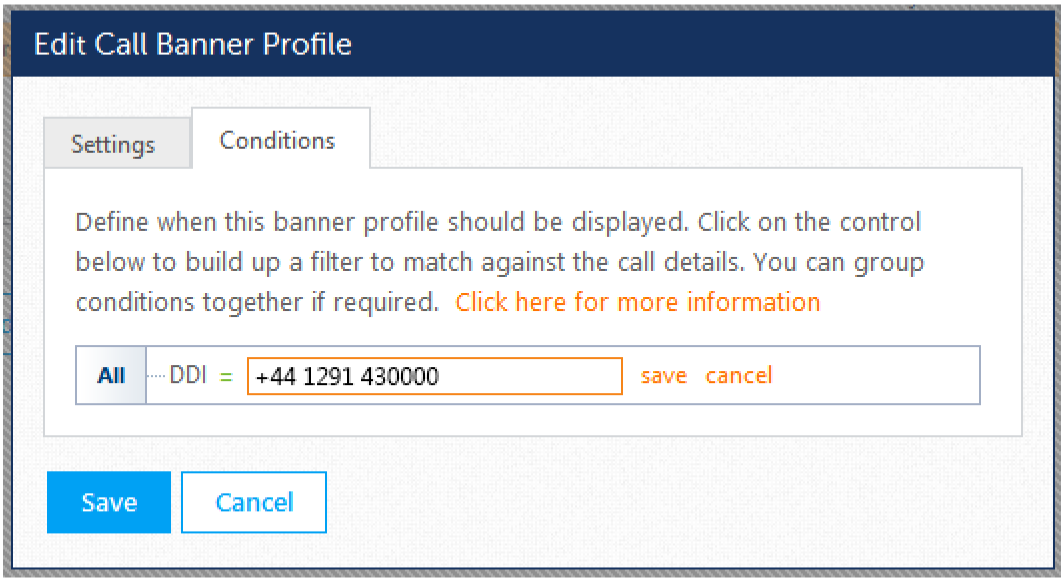
2. Click on the *Conditions* tab and then we are going to add a condition to only show this banner when the call has come in on a specific DDI/DID number. Right click on the *All* option and select *Add Condition*.



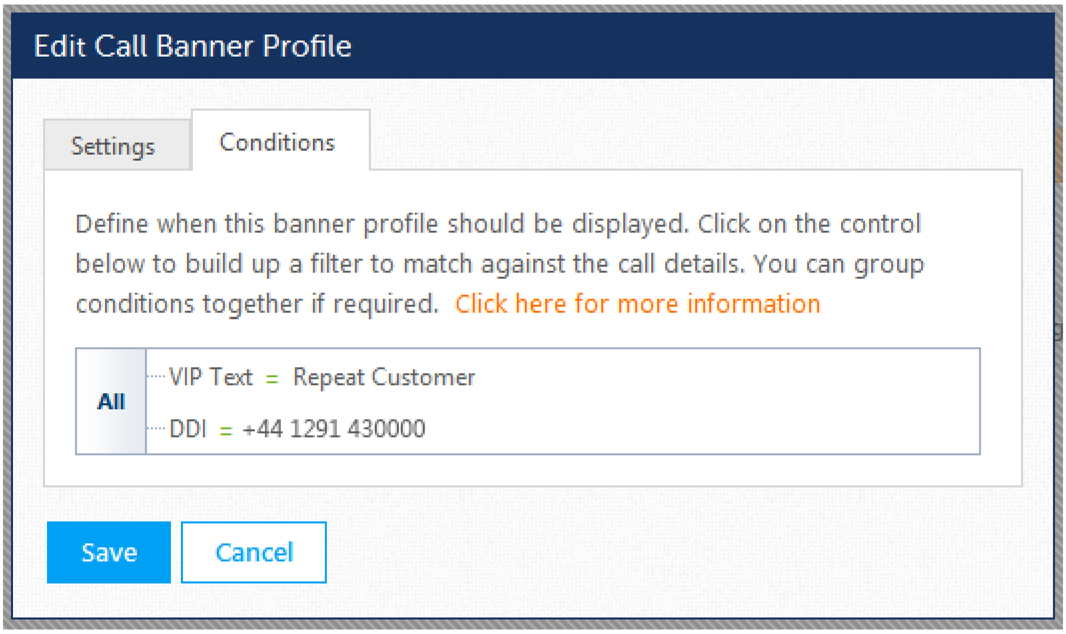
3. This will add a new condition for *Agent*, and we need to change this to *DDI* so left click on *Agent* and select *Basic -> DDI* from the drop down menu.



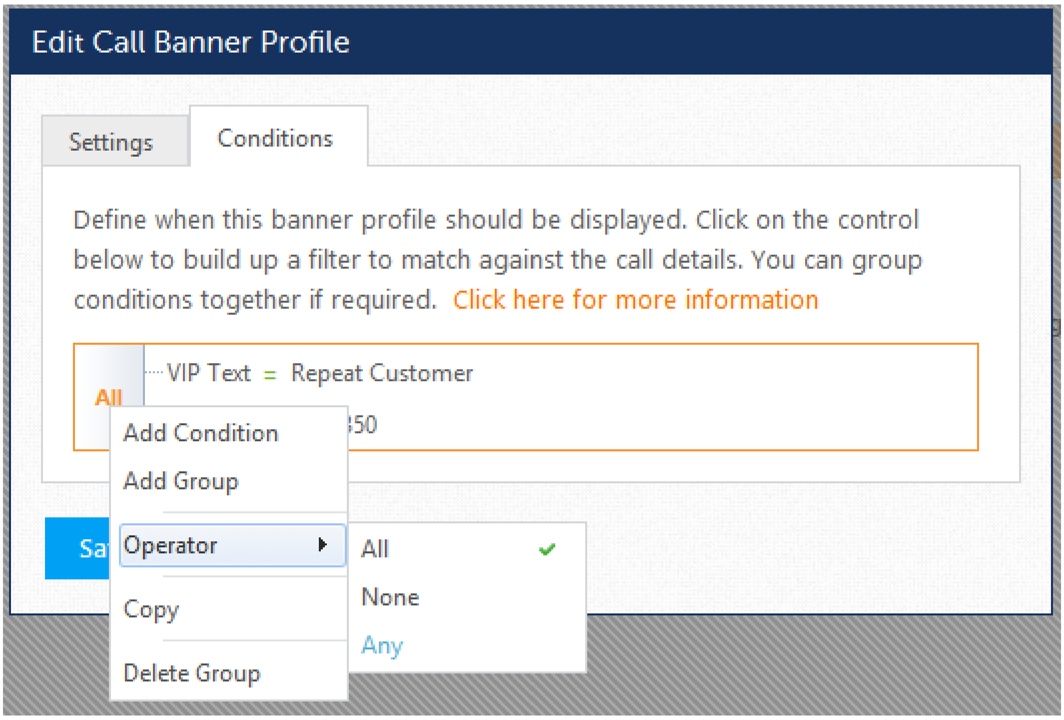
4. To enter the DDI/DID number to filter this on click on the *Click to edit* field and enter the number then click on save.



5. Repeat the process from step 2 to add the condition for VIP Text. After you have done this it should look like this.

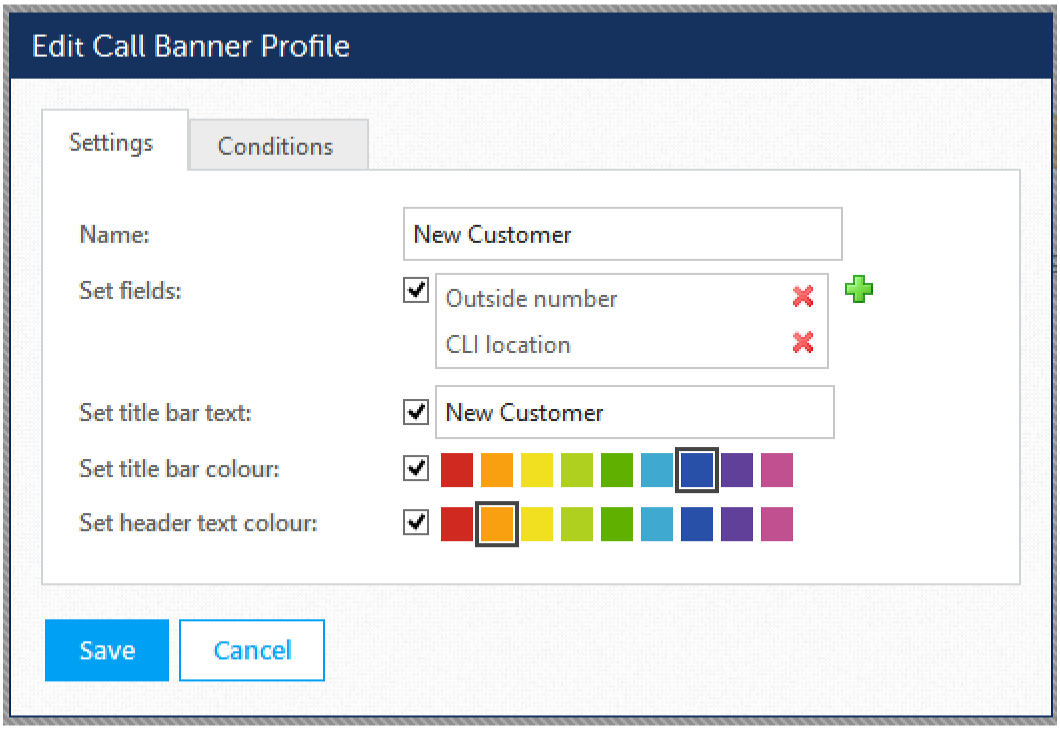


6. For this condition to be true both the *VIP Text* and *DDI* conditions need to be met. If only one of these conditions needs to be met then the grouping could be changed from **All** to **Any**.

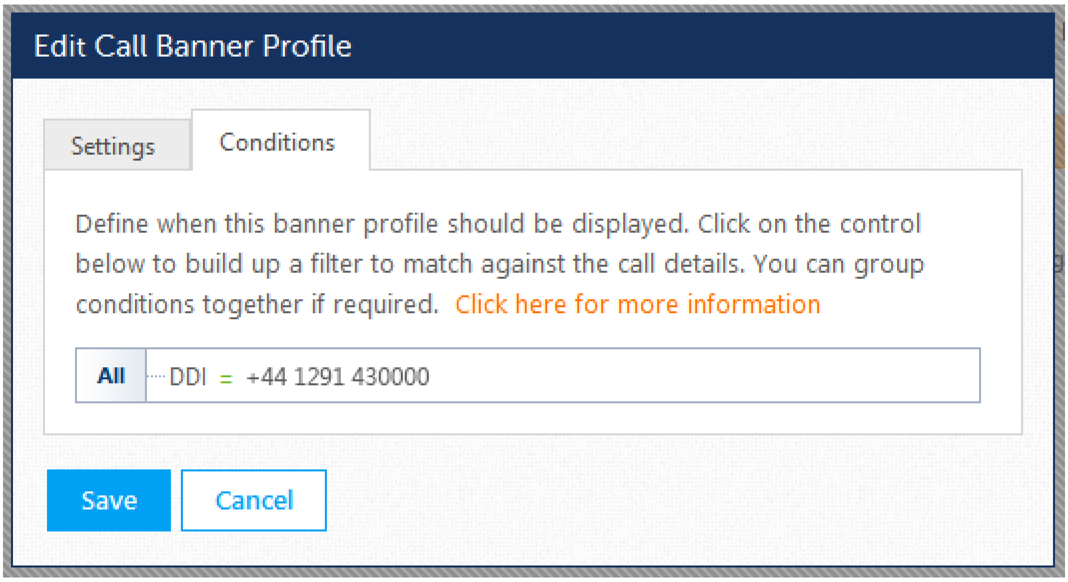


To create the "New Customer" profile follow the same steps as for the "Repeat Customer", except do not add the *VIP Text* condition.

1. This is how the *Settings* tab should look.



2. This is how the *Conditions* tab should look.



Now we have the banner profiles configured we need to set the *Priority* of these so that the correct ones are applied. From the Call Banner Profiles section using the mouse drag each line around until they are in this order.

Name	Fields	Title	Title Colour	Header Colour	Priority ▲		
Repeat Customers	✓	✓	✓	✓	1		
New Customer	✓	✓	✓	✓	2		
Default	✓	-	-	-	3		

Page **1** of **1** (3 items)

The client banner configuration is now complete. Import some contact records into a Global Directory with the VIP Text set to "Repeat Customer" and make an inbound call to the configured DDI/DID number to test.

11.5 Importing Phone Manager v3 Personal Contacts

Overview

If the user has upgraded from Phone Manager v3 then their existing personal contacts can be imported. This is only supported if the users personal contacts have been stored locally (either in the %PROGRAMFILES% folder on the computer they are on, or in their "My Documents" folder and NOT centrally. If they are stored centrally then they will need to be migrated before upgrading. If these files are present then Phone Manager will prompt the user automatically when started to import.

Considerations before upgrade

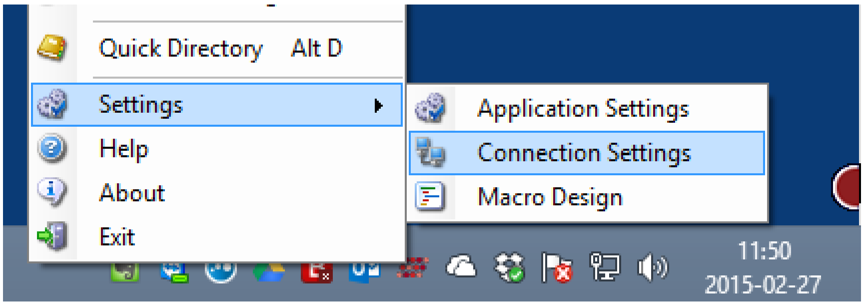
If the user already has version Phone Manager v3 installed on the PC then they had 3 places to save their personal contacts

1. C:\Users\[Username]\Documents\Application Data\Xarios\Phone Manager.
2. C:\Program Files\Xarios\Xarios Phone Manager\Phone Manager\ConfigFiles
3. On the Xarios Application Server.

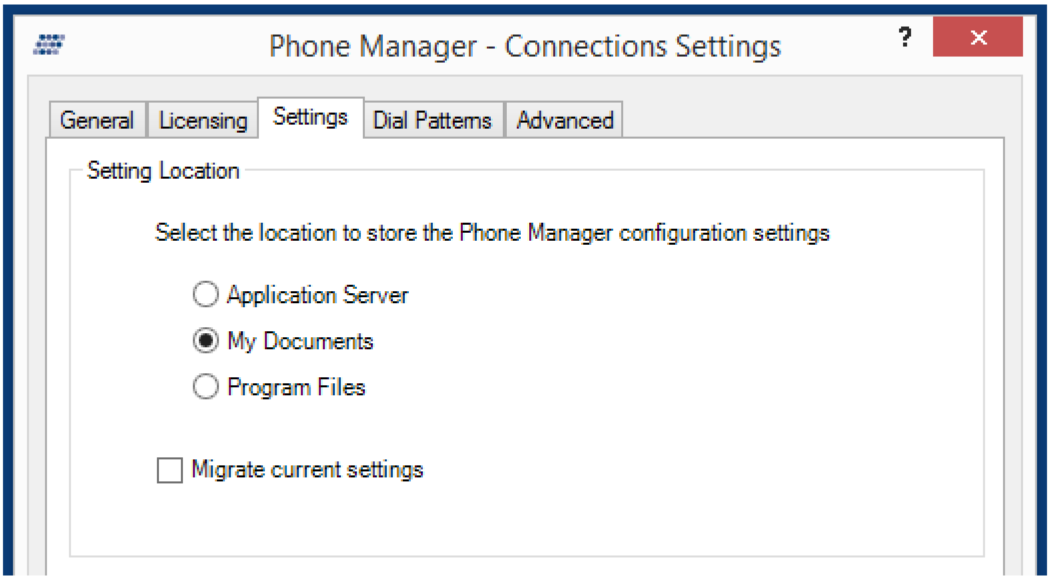
To be able to use the migration tool to import to your v4 and above client you need to make sure that the v3 client has personal contacts stored in either of the local locations i.e. options 1 and 2 above.

You can check where the client's directory is currently located in the v3 client by:

1. Right clicking on the Phone Manager Icon in the systray and select *Settings* -> *Connection Settings*.

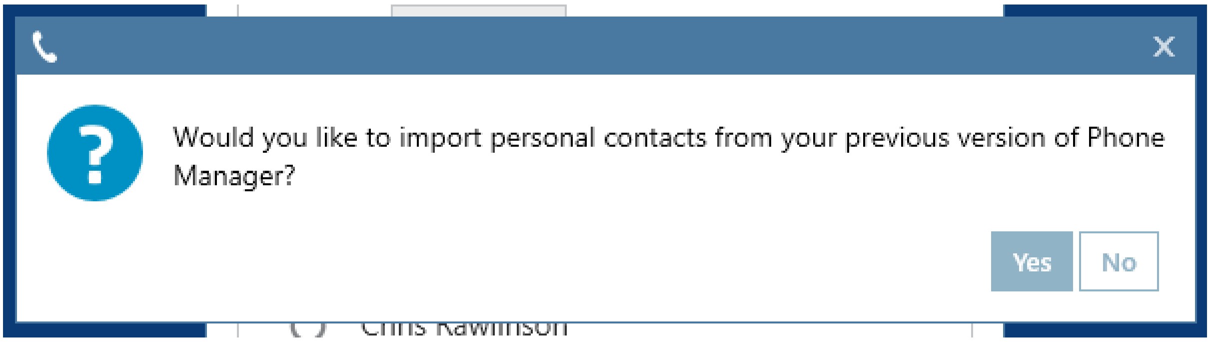


2. Select the *Settings* tab from the *Connection Settings* window.



From here will be able to tell where the contacts are located and if needed you can then migrate them to a local location. Once you have confirmed that the v3 personal contacts are stored locally you then need to install your v4 client.

Once installed open the v4 client and note the pop up box.



Click *Yes* and this will import all previously stored personal contacts. Click *No* and it will not import or prompt when next opened. Once complete you will get another pop up box to advise the number of contacts imported.

> Whilst the import is taking place you do not get a progress bar but this allows you to carry on using your client.

11.6 Enabling HTTPS

To improve security it is recommended to switch access to the MiVoice Office Application Suite website from HTTP (default) to HTTPS.

The website is hosted by IIS server which is part of the host operating system. This following steps explain the process involved in enabling HTTPS for the website.

Enabling HTTPS Steps

1. Create a CSR (Certificate Signing Request) for the server
2. Obtain a certificate from your provider
3. Install the certificate on the server

> If a certificate has already been installed for Phone Manager Mobile, the same certificate can be used for enabling HTTPS on the website.

Creating a CSR & Obtaining a Certificate

A CSR (certificate signing request) must be generated on the host server before a certificate can be purchased and installed. The 'SSL Certificate' configuration section can be used for generating a CSR.

> Ensure the Client Location addresses have been correctly configured with the servername/FQDN for local and remote connections before creating a CSR.

The method for doing this manually on the server will differ depending on the version of IIS installed. A good reference on how to generate the CSR can be found on the Digicert website: https://www.digicert.com/csr-creation.htm

Once you have a CSR, a certificate must be obtained from your Certificate Authority.

Installing a Certificate

Once a certificate has been purchased/generated, it must be installed on the host server. This can be done from the 'SSL Certificates' configuration section, ensure that the relevant checkbox is checked to apply the certificate to the website.

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

12 Statistics Overview

The reporting engine provides a range of information fields that show details of calls, status events and configuration. The fields available to add to a report will depend on the template the report is using.

- Call List Data Fields
- Status List Data Fields
- Grouped Call/Status Data Fields
- Configuration Data Fields
- Real-Time Data Fields

12.1 Call List Report Data

A call list report is a report that lists each call individually (and segments), rather than grouping calls together to get aggregated figures.

There are three templates that provide call list data:

- Call Data - Call List
- Call Data - Call List (Segmented)
- Call Data - Unreturned Lost Calls

For information about the data that these templates provide, refer to the Templates sections.

Each row in a call list report is an individual call or call segment and each column available contains a specific piece of information about that call or segment.

All of the data columns available on call list reports have been split up into the following categories:

Advanced - Information about a call not normally used.

Call Info - Standard information about a call; CLI, DDI, Account Code etc.

Call Times - Time and duration information about a call; Start Time, End Time, Ring Duration etc.

Devices / Agents - Device or Agent information about a call, who answered or where did it ring?

Tag Fields - Specific customer related information that has been tagged to the call by the user.

12.1.1 Call Statistics - Advanced

The following call list fields are designed for engineering use and are not required for normal reporting purposes.

(All columns below are available on the following templates: Call List, Call List (Segmented) and Unreturned Lost Calls).

Call ID

The telephone system call id of the call. This can be used to trace calls back to the telephone system data or to match calls in other applications.

End Event

This columns contains the event code provided by the telephone system when the call ended. This is for engineering use only.

Logical Call ID

This column refers to the call id assigned to the call by the software. The logical call id is used to link call segments and announced transfer segments together as being part of the same call.

Rec ID

This column contains a unique id assigned to each call segment by the software.

12.1.2 Call Statistics - Call Info

Account Code

The last account code that was entered on this call. If no account was entered on the call then this will be empty. On segmented call list this will be the last account code entered on the segment, on a non-segmented report this will be the last account code entered on the call.

Call Answered

Was this call answered or not? On a segmented call list this will show the answered state or each segment. On a non-segmented call it will show whether the entire call is being treated as answered.

Call Direction

The direction of this call segment, either (In)bound or (Out)bound for external calls and n/a for internal calls.

Call Matched

Was the CLI associated with this call matched to a Contact Directory record?

Call State

What is the current state of the call (ringing, connected, on hold etc).

Call Type

The type of call, either (Int)ernal or (Ext)ernal.

CLI

The caller ID associated with this call for external calls. The will be the received number for inbound calls and the dialled number for outbound calls. On internal calls this property is empty.

CLI Received

Was the inbound call received with a Caller ID? This applies only to inbound external calls.

Contact Name

The contact information associated with this call segment. This may be populated from a Contact Directory.

> Personal contacts do not show on reports by design as the matching happens centrally.
>
> System Speed Dials only match on Inbound Calls - the same way as the PBX handles it.
>
> Speed Dial matches will be shown in the Contacts fields in reports. If you have a System Speed Dial and Global Contact with the same number the Global Contact name will take precedence.

DDI Digits

The significant DDI digits received from the network provider to identify a call originated via a particular DDI number. This applies to inbound external calls only and will be empty for all other call types.

DDI Received

Was the inbound call received with DDI digits? This is a Yes/No property that relates to inbound external calls only. For all other calls this will be displayed as n/a.

DNIS

A description against the DDI that the inbound call originated on. This is the description programmed against the DDI on the telephone system. This applies to inbound external calls only and will be empty for other call types.

Segment No *

The segment number of the call segment. Use the Logical CallID to link multiple segments together. This property is only available on segmented call list reports.

Segment Count **

The total number of segments for the call. This property is only available for non-segmented call list reports.

Short Call

A call is designated Short if the talk time (plus hold time) is less than the configured Short Call value. This property will be displayed as Yes/No.

Speed Dial Name

Any speed dial match from the telephone system for external calls. This property will be empty for other call types.

Telephone Number

The telephone number associated with this call segment. For external calls this will contain the CLI information, for internal calls this will contain extension number of the device making the call.

> * This column is only available on segmented call lists.

> ** This column is only available on un-segmented call lists.

12.1.3 Call Statistics - Call Times

Answer Time

The time of day that this call or call segment was answered. If the call was not answered this will be empty.

Call Duration

The total duration for this call or call segment including ring, hold and talk durations.

End Time

The time of day that this call segment ended.

Hold Duration

The duration this call segment spent on hold.

Ring Duration

The duration this call segment spent ringing.

Start Time

The time the call or call segment started ringing.

Talk Duration

The duration this call segment was in the answered state.

> Each of the time and duration columns can be configured to display using different formats. For more information refer to the Report Creation section.

> If '#ERROR' appears in any column, this is an indication of missing data. this can happen if the reporting service is stopped or loses connection to the telephone system.

12.1.4 Call Statistics - Devices / Agents

Agent / Agent Name **

The details of any agents associated with this call segment. On internal and conference calls there may be more than one agent associated with the call. For an agent to be associated with a call, the call doesn't need to have been passed from a hunt group, the agent just needs to be logged into the telephone associated with the call.

Answering Agent / Answering Agent Name *

The agent the call was first answered at.

Answering Extension /Answering Extension Name *

The extension the call was first answered at.

Extension / Extension Name **

The details of any extensions that were involved in this call segment. On internal and conference calls there may be more than one extension. This can be any device on the telephone system so can include voicemail applications etc.

First Rang Agent / First Rang Agent Name *

The first agent the call rang at.

First Rang Extension / First Rang Extension Name *

The first extension the call rang at.

Hunt Group / Hunt Group Name

The details of the hunt group the current call/call segment was presented from. On non-segmented calls this will be the first hunt group the call was presented to if there was more than one. If the call was not delivered through a hunt group this will be empty.

Last Rang Agent / Last Rang Agent Name *

The last agent the call rang at.

Last Rang Extension / Last Rang Extension Name *

The last extension the call rang at.

Transferred From / Transferred Agent From

The source device/agent if the call was transferred from another location. On non-segmented calls this will the first device/agent that transferred the call if the call was transferred more than once.

Transferred To / Transferred Agent To

The destination device/agent if the call was transferred to another location. On non-segmented calls this will the first device/agent that the call was transferred to if the call was transferred more than once.

Trunk Number / Trunk Description

If the call is external, this will contain the information about the trunk line used for the call. On internal calls this will be empty.

Username **

The name of any users associated with the call. On internal calls there may be more than one.

> * This column is only available on the un-segmented call lists.

> ** This column is only available on the segmented call lists.

12.1.5 Call Statistics - Tag Fields

Tag Field 1 to 5

There are 5 custom fields for each call that can be populated with information by the user. This is most commonly used to attach customer specific information to calls such as account numbers or reference numbers. These number can then be added to reports or used to search and find recordings. Selecting one of the 5 fields here will add them to a call list reports.

> For more information on tagging calls with custom information, please refer to the Phone Manager user guide.

> For more information on naming each custom field, please refer to the Default Report Settings section.

12.2 Grouped Report Data

timesGrouped reports provide aggregated call information (totals, averages, percentages etc.) for devices on the telephone system. For more information on grouped reports, see the Reporting section.

The data columns listed below are available when selecting any of the grouped call templates:

- Call Data - Calls by Account Code
- Call Data - Calls by Agent
- Call Data - Calls by DDI
- Call Data - Calls by Extension
- Call Data - Calls by Hunt Group
- Call Data - Calls by Start Time
- Call Data - Calls by Telephone Number
- Call Data - Calls by Trunk
- Call Data - Calls by User

For information about the data that these templates provide, refer to the Templates sections.

All of the data columns available have been split up into the following categories:

Account Codes - There are 10 account code fields that can be added to grouped reports.

ACD Times - Average, Percentage, Total time on duty etc

Call Times (%) - Time spent in ringing/talk, number of calls answered/lost with ring durations.

Call Times (Average) - Average talk time, ring time, hold time per call etc.

Call Times (Min/Max) - Longest ringing, shortest ringing, first call at etc.

Call Times (Total) - Total time spent ringing, total time spent talking etc

Call Totals - Total number of calls in, calls out, calls answered, calls lost etc.

Call Totals (%) - Percentage of calls in, calls out, calls answered calls lost etc.

DND Times (%) - Percentage of time spent in the available DND states.

DND Times (Average) - Average time spent in the available DND states.

DND Times (Max) - Maximum time spent in the available DND states.

DND Times (Total) - Total time spent in the available DND states.

DND Totals - The number of times an extension/agent used a DND state.

Report's Call Totals (%) - Breakdown of total statistics across a report.

Report's Call Times (%) - Breakdown of time statistics across a report.

> There are 20 different DND states for users to choose from. The current name for each DND state on the telephone system is displayed in brackets where applicable. This can be changed on the telephone system and may not have been the name of the DND state when the user selected it.

> Not all columns are available in all grouped report templates.

12.2.1 Grouped Statistics - Account Codes

Account codes can be entered on external calls made on the telephone system. The MCS will store any account code entered against a call segment, if more than one code is entered on a call segment then the last account code will be used for calculating grouped report data.

Up to 10 account codes can be added to grouped reports. Each of the 10 codes can be given a user definable name (see the Reporting Settings section for more information).

Code 1 to 10

Each of the codes will appear with either the default name (Code 1 to 10) or the user defined name (Sale, Complaint etc). These columns show the total number of calls that this account code was entered on.

(Available on the following templates: Calls by DDI, Calls by Extension, Calls by Hunt Group, Calls by Start Time, Calls by Telephone Number, Calls by Trunk and Calls by User).

12.2.2 Grouped Statistics - ACD Times

% Time In Busy

The Time In Busy as a percentage of Time On Duty.

License Required: ACD Reporter

% Time In Busy N/A

The Time In Busy N/A as a percentage of Time On Duty.

License Required: ACD Reporter

% Time In Free

The Time In Free as a percentage of Time On Duty.

License Required: ACD Reporter

% Time In Wrapup

The Time In Wrapup as a percentage of Time On Duty.

License Required: ACD Reporter

Avg Time Busy

The average time an agent spends in the busy state. Time In Busy divided by Times In Busy

License Required: ACD Reporter

Avg Time Busy N/A

The average time an agent spends in the busy not available state (DND). Time In Busy N/A divided by Times In Busy N/A

License Required: ACD Reporter

Avg Time Free

The average time an agent spends in the free state. Time In Free divided by Times In Free

License Required: ACD Reporter

Avg Time In Wrapup

The average time an agent spends in the wrapup state. Time In Wrapup divided by Times In Wrapup

License Required: ACD Reporter

Avg Time On Duty

The average time an agent spends logged into the telephone system. Time On Duty divided by Times Logged In

License Required: ACD Reporter

First Logon Time

The first time that an agent logged onto the telephone system.

License Required: ACD Reporter

Last Logoff Time

The last time that an agent logged out the telephone system.

License Required: ACD Reporter

Last Logon Time

The last time that an agent logged onto the telephone system.

License Required: ACD Reporter

Time In Busy

The total time an agent has spent in the busy state.

License Required: ACD Reporter

Time In Busy N/A

The total time an agent has spent in the busy not available state (this is the same as DND).

License Required: ACD Reporter

Time In Free

The total time an agent has spent in the free state.

License Required: ACD Reporter

Time In Wrapup

The total time an agent has spent in the wrapup state.

License Required: ACD Reporter

Time On Duty

The total time an agent has spent logged into the telephone system.

License Required: ACD Reporter

Times In Busy

The number of times the ACD Status of the agent went into the busy state.

License Required: ACD Reporter

Times In Busy N/A

The number of times the ACD Status of the agent went into the busy not available state (this is the same as DND).

License Required: ACD Reporter

Times In Free

The number of times the ACD Status of the agent went into the free state.

License Required: ACD Reporter

Times In Wrapup

The number of times the ACD Status of the agent went into the wrapup state.

License Required: ACD Reporter

Times Logged In

The number of times the the agent transitioned from being logged out to being logged in.

License Required: ACD Reporter

Unlicensed Agents

The number of agents currently logged in that don't have an ACD Reporting User licence.

12.2.3 Grouped Statistics - Call Times (%)

% Answered <= Xs or % Answered > Xs *

The number of Calls Answered within a specific service level as a percentage of Calls Inbound.

% Lost <= Xs or % Lost > Xs *

The number of Calls Lost within a specific service level as a percentage of Calls Inbound.

% Total Hold Time

The Total Hold Time as a percentage of Total Call Time.

% Total Ring Time

The Total Ring Time as a percentage of Total Call Time..

% Total Talk Time

The Total Talk Time as a percentage of Total Call Time..

> * The 6 different call duration values are configured on Default Report Settings section.

12.2.4 Grouped Statistics - Call Times (Average)

Avg Answer Time (In)

The average ring duration for all inbound answered calls. This is calculated by taking the total ring duration on answered calls and dividing by Calls In Answered.

Avg Answer Time (Out)

The average ring duration for all outbound answered calls. This is calculated by taking the total ring duration on answered calls and dividing by Calls Out Answered.

Avg Call Time

The average call duration for all calls. This is calculated by dividing Total Call Time by Calls Handled.

Avg Call Time (In)

The average call duration for all inbound calls. This is calculated by dividing Total Call Time (In) by Calls Inbound.

Avg Call Time (Out)

The average call duration for all outbound calls. This is calculated by dividing Total Call Time (Out) by Calls Outbound.

Avg Lost Call Time

The average amount of time lost calls spend ringing. This is calculated by dividing the Total Ring Time (Lost) by Calls Lost.

Avg Ring Time

The average amount of time calls spend ringing. This is calculated by dividing Total Ring Time by Calls Handled.

Avg Ring Time (In)

The average amount of ring time on inbound calls. This is calculated by dividing Total Ring Time (In) by Calls Inbound.

Avg Ring Time (Out)

The average amount of ring time on outbound calls. This is calculated by dividing Total Ring Time (Out) by Calls Outbound.

Avg Talk Time

The average talk time for all calls. This is calculated by dividing Total Talk Time by Calls Handled.

Avg Talk Time (In)

The average talk time for all inbound calls. This is calculated by dividing Total Talk Time (In) by Calls Inbound.

Avg Talk Time (Out)

The average talk time for all outbound calls. This is calculated by dividing Total Talk Time (Out) by Calls Outbound.

12.2.5 Grouped Statistics - Call Times (Min/Max)

First Call At

The time the first call started ringing.

Last Call At

The time the last call started ringing.

Last Call Answered At

The time of day the last call was answered.

Last Call Ended At

The time of day of the last call that ended.

Max Answer Time (In)

The longest time a single inbound answered call spent in the ringing state.

Max Answer Time (Out)

The longest time a single outbound answered call spent in the ringing state.

Max Call Time

The longest duration for a single call.

Max Call Time (In)

The longest duration of any inbound call.

Max Call Time (Out)

The longest duration of any outbound call.

Max Hold Time

The longest a call was on hold.

Max Hold Time (In)

The longest any inbound call was on hold.

Max Hold Time (Out)

The longest any outbound call was on hold.

Max Ring Time

The longest any call was ringing.

Max Ring Time (Lost)

The longest any lost call was ringing.

Max Ring Time (In)

The longest time and inbound call was ringing.

Max Ring Time (Out)

The maximum time an outbound call spent ringing.

Max Talk Time

The longest time a single call spent in the talking state.

Max Talk Time (In)

The longest time a single inbound call spent in the talking state.

Max Talk Time (Out)

The longest time a single outbound call spent in the talking state.

Min Answer Time (In)

The shortest time an answered inbound call spent in the ringing state.

Min Answer Time (Out)

The shortest time an answered outbound call spent in the ringing state.

Min Call Time

The shortest duration for a single call.

Min Call Time (In)

The shortest duration for a single inbound call.

Min Call Time (Out)

The shortest duration for a single outbound call.

Min Hold Time

The shortest hold time for a single call.

Min Hold Time (In)

The shortest hold time for a single inbound call.

Min Hold Time (Out)

The shortest hold time for a single outbound call.

Min Ring Time

The shortest ring time for a single call.

Min Ring Time (Lost)

The shortest ring time for any lost call.

Min Ring Time (In)

The shortest ring time for any inbound call.

Min Ring Time (Out)

The shortest ring time of all outbound calls.

Min Talk Time

The shortest time a single call spent in the talking state.

Min Talk Time (In)

The shortest time a single inbound call spent in the talking state.

Min Talk Time (Out)

The shortest time a single outbound call spent in the talking state.

12.2.6 Grouped Statistics - Call Times (Total)

Answered <= Xs or Answered > Xs

The total number of inbound calls answered inside each of the 6 service levels.

Lost <= Xs or Lost > Xs

The total number of inbound calls lost inside each of the 6 service levels.

Total Answer Time (In)

The total amount of ring time for all inbound answered calls.

Total Answer Time (Out)

The total amount of ring time for all outbound answered calls.

Total Call Time

The total duration for all calls including ring, hold and talk time.

Total Call Time (In)

The total duration for all inbound calls including ring, hold and talk time.

Total Call Time (Out)

The total duration for all outbound calls including ring, hold and talk time.

Total Hold Time

The total hold duration for all calls.

Total Hold Time (In)

The total hold duration for all inbound calls.

Total Hold Time (Out)

The total hold duration for all outbound calls.

Total Ring Time

The total ring duration for all calls.

Total Ring Time (Lost)

The total ring duration for all lost calls.

Total Ring Time (In)

The total amount of ring time on inbound calls.

Total Ring Time (Out)

The total amount of ring time on outbound calls.

Total Talk Time

The total amount of talk time for all calls.

Total Talk Time (In)

The total amount of talk time for all inbound calls.

Total Talk Time (Out)

The total amount of talk time for all outbound calls.

12.2.7 Grouped Statistics - Call Totals

Calls Answered

The total number of calls answered (inbound and outbound).

Calls Completed

The total number of calls completed (inbound and outbound).

Calls External

The total number of external calls.

Calls Handled

The total number of calls handled (internal and external).

Calls In Ans

The total number of inbound calls that were answered (internal and external).

Calls In Ans External

The total number of inbound calls that were answered (external only).

Calls In Ans Internal

The total number of inbound calls that were answered (internal only).

Calls Inbound

The total number of calls inbound (external only)

Calls In Completed

The total number of inbound calls completed (internal and external).

Calls In External

The total number inbound, external calls.

Calls In Internal

The total number of inbound, internal calls.

Calls In Refused

The total number of inbound calls that alerted but were not answered.

Calls Internal

The total number of internal calls.

Calls Lost

The total number of external inbound calls that weren't answered.

Calls Matched

The total number of external calls matched to a Contact Directory.

Calls Not Matched

The total number of external calls that did not match a Contact Directory record.

Calls Out Ans

The total number of outbound calls that were answered (internal and external).

Calls Out Ans External

The total number of outbound calls that were answered (external only).

Calls Out Ans Internal

The total number of outbound calls that were answered (internal only).

Calls Outbound

The total number of outbound calls (internal and external).

Calls Out Completed

The total number of outbound calls completed (internal and external).

Calls Out External

The total number outbound, external calls.

Calls Out Internal

The total number of outbound, internal calls.

Calls Overflowed In

The total number of inbound calls that overflowed from another device.

Calls Overflowed Out

The total number of inbound calls that overflowed to another device.

Calls Transferred In

The total number of calls transferred to this device

Calls Transferred Out

The total number of calls transferred from this device

Calls With CLI

The total number of inbound external calls received with a Caller ID.

DDI Calls

The total number of external inbound calls that were presented with a DDI.

Recoverable Calls

The total number of abandoned calls that presented a CLI.

Short Calls

The total number of calls that were classified as a Short Call, the talk time (plus hold time) was less than the configured Short Call value.

Unreturned Lost Calls

The total number of calls that were Lost Calls and not subsequently answered on either an inbound or outbound call.

12.2.8 Grouped Statistics - Call Totals (%)

% Calls In Ans

The number of Calls In Answered as a percentage of Calls In.

% Calls In Ans Ext

The number of Calls In External Answered as a percentage of Calls In External.

% Calls In Ans Int

The number of Calls In Answered Internal as a percentage of Calls In Internal.

% Calls In Completed

The number of Calls In Completed as a percentage of Calls In.

% Calls In Ext

The number of Calls In External as a percentage of Calls In.

% Calls In Int

The number of Calls In Internal as a percentage of Calls In.

% Calls In Refused

The number of Calls Refused as a percentage of Calls In.

% Calls Inbound

The number of Calls Inbound as a percentage of Calls Handled.

% Calls Internal

The number of Calls Internal as a percentage of Calls Handled.

% Calls Lost

The number of Lost Calls as a percentage of Calls In External.

% Calls Matched

The number of Calls Matched as a percentage of Calls External.

% Calls Not Matched

The number of Calls Not Matched as a percentage of Calls External.

% Calls Out Ans

The number of Calls Out Answered as a percentage of Calls Out.

% Calls Out Ans Ext

The number of Calls Out External Answered as a percentage of Calls Out External.

% Calls Out Ans Int

The number of Calls Out Internal Answered as a percentage of Calls Out Internal.

% Calls Out Completed

The number of Calls Out Completed as a percentage of Calls Out.

% Calls Out Ext

The number of Calls Out External as a percentage of Calls Out.

% Calls Out Int

The number of Calls Out Internal as a percentage of Calls Out.

% Calls Outbound

The number of Calls Outbound as a percentage of Calls Handled.

% Calls Overflowed In

The number of Calls Overflowed In as a percentage of the Calls In.

% Calls Overflowed Out

The number of Calls Overflowed Out as a percentage of the Calls Out.

% Calls Transferred In

The number of Calls Transferred In as a percentage of Calls In

% Calls Transferred Out

The number of Calls Transferred Out as a percentage of Calls In

% Calls With CLI

The number of Calls With CLI as a percentage of Calls In External.

% DDI Calls

The number of DDI Calls as a percentage of Calls In External.

% Short Calls

The number of Short Calls as a percentage of Calls Answered.

% Unreturned Lost Calls

The number of Unreturned Lost Calls as a percentage of Calls In External.

12.2.9 Grouped Statistics - DND Times (%)

% Time In DND 1 to 20

The amount of time spent in a specific DND message state as a percentage of total time for the report.

License Required: DND Reporter

% Time In DND

The amount of time spent in any DND message state as a percentage of total time for the report.

License Required: DND Reporter

12.2.10 Grouped Statistics - DND Times (Average)

Avg Time In DND 1 to 20

The average amount of time the extension spent in each of the 20 available DND states.

License Required: DND Reporter

Avg Time In DND

The average amount of time the extension spent in any of the DND states.

License Required: DND Reporter

12.2.11 Grouped Statistics - DND Times (Maximum)

Longest Time In DND 1 to 20

The longest time an extension spent in each of the DND states.

License Required: DND Reporter

Longest Time In DND

The longest time an extension spent in any of the DND states.

License Required: DND Reporter

12.2.12 Grouped Statistics - DND Times (Total)

Time In DND 1 to 20

The total time an extension spent in each of the available DND states.

Time In DND

The combined total time an extension spent in any of the DND states.

12.2.13 Grouped Statistics - DND Totals

Times In DND 1 to 20

The number of times an extension entered a specific DND state. There are 20 DND states to select from.

Times In DND

The total number of times an extension went into any of the 20 DND states.

12.2.14 Grouped Statistics - Report's Call Totals (%)

% Of All Calls Answered

The number of Calls Answered as a percentage of all Calls Answered for the report.

% Of All Calls External

The number of Calls External as a percentage of all Calls External for the report.

% Of All Calls Handled

The number of Calls Handled as a percentage of all Calls Handled for the report.

% Of All Calls In

The number of Calls In as a percentage of all Calls In for the report.

% Of All Calls In Ans

The number of Calls In Answered as a percentage of all Calls In Answered for the report.

% Of All Calls In Ans Ext

The number of Calls In Answered External as a percentage of all Calls In Answered External for the report.

% Of All Calls In Ans Int

The number of Calls In Answered Internal as a percentage of all Calls In Answered Internal for the report.

% Of All Calls In Completed

The number of Calls In Completed as a percentage of all Calls In Completed for the report.

% Of All Calls In Ext

The number of Calls In External as a percentage of all Calls In External for the report.

% Of All Calls In Int

The number of Calls In Internal as a percentage of all Calls In Internal for the report.

% Of All Calls In Refused

The number of Calls Refused as a percentage of all Calls Refused for the report.

% Of All Calls Internal

The number of Calls Internal as a percentage of all Calls Internal for the report.

% Of All Calls Lost

The number of Lost Calls as a percentage of all Lost Calls for the report.

% Of All Calls Matched

The number of Calls Matched as a percentage of all Calls Matched for the report.

% Of All Calls Not Matched

The number of Calls Not Matched as a percentage of all Calls Not Matched for the report.

% Of All Calls Out

The number of Calls Out as a percentage of all Calls Out for the report.

% Of All Calls Out Ans

The number of Calls Out Answered as a percentage of all Calls Out Answered for the report.

% Of All Calls Out Ans Ext

The number of Calls Out Ans External as a percentage of all Calls Out Ans External for the report.

% Of All Calls Out Ans Int

The number of Calls Out Ans Internal as a percentage of all Calls Out Ans Internal for the report.

% Of All Calls Out Completed

The number of Calls Out Completed as a percentage of all Calls Out Completed for the report.

% Of All Calls Out Ext

The number of Calls Out External as a percentage of all Calls Out External for the report.

% Of All Calls Out Int

The number of Calls Out Internal as a percentage of all Calls Out Internal for the report.

% Of All Calls Overflowed In

The number of Calls Overflowed In as a percentage of all Calls Overflowed In for the report.

% Of All Calls Overflowed Out

The number of Calls Overflowed Out as a percentage of all Calls Overflowed Out for the report.

% Of All Calls Transferred In

The number of Calls Transferred In as a percentage of all Calls Transferred In for the report.

% Of All Calls Transferred Out

The number of Calls Transferred Out as a percentage of all Calls Transferred Out for the report.

% Of All Calls With CLI

The number of Calls With CLI as a percentage of all Calls With CLI for the report.

% Of All DDI Calls

The number of DDI Calls as a percentage of all DDI Calls for the report.

% Of All Short Calls

The number of Short Calls as a percentage of all Short Calls for the report.

% Of All Unreturned Lost Calls

The number of Unreturned Lost Calls as a percentage of all Unreturned Lost Calls for the report.

12.2.15 Grouped Statistics - Report's Call Times (%)

% Of All Ans <= Xs or % Of All Ans > Xs

The number of calls answered with one of the 6 service levels as a percentage of all of the calls answered in the same service level for the report.

% Of All Lost <= Xs or % Of All Lost > Xs

The number of calls lost within one of the 6 service levels as a percentage of all call lost in the same service level for the report.

% Of All Total Call Time

The Total Call Time as a percentage of the entire Total Call Time for the report.

% Of All Total Hold Time

The Total Hold Time as a percentage of the entire Total Hold Time for the report.

% Of All Total Ring Time

The Total Ring Time as a percentage of the entire Total Ring Time for the report.

% Of All Total Talk Time

The Total Talk Time as a percentage of the entire Total Talk Time for the report.

12.3 Configuration Data - Device Info

The following information fields are available in the Config Data report templates.

Device Number

The number of the device. This could be the trunk, agent ID, extension number or DDI depending on the report run.

Description

The description given to the device on the telephone system.

Node ID

The node number of the telephone system on which the device resides.

12.4 Status List Data

A status list report is a report that lists each status change individually, rather than grouping changes together to get aggregated figures.

There are two templates that provide call list data:

- ACD Data - ACD Status List
- DND Data - DND Status List

For information about the data that these templates provide, refer to the Templates sections.

All of the data columns available on call list reports have been split up into the following categories:

ACD - Information about ACD status changes.

DND - Information about do-not-disturb status changes.

12.4.1 Status List Data - ACD

(All columns below are available on the following templates: ACD Data.)

ACD Status

The ACD status of the agent (Logged on, Free, Busy, Wrap, DND on/off, Logged out).

Agent

The agent ID the event occurred to.

Agent Name

The description of the agent the event occurred to.

DND Message

When the ACD Status is 'DND on', the DND message associated with the event will be displayed.

DND Text

When the ACD Status is 'DND on', the DND text will be displayed if there was any additional information entered by the agent.

Event Time

The time the ACD status event occurred.

Extension

The extension number the ACD status event occurred on.

Hunt Group

When the ACD Status is 'Logged on/Logged off', the hunt group the agent logged into or out of will be displayed.

Hunt Group Name

When the ACD Status is 'Logged on/Logged off', the name of the hunt group the agent logged into or out of will be displayed.

12.4.2 Status List Data - DND

(All columns below are available on the following templates: DND Data.)

DND Status

The DND status of the extension(DND on/off).

DND Message

The DND message associated with the event.

DND Text

The DND text associated to the event. This is optional and will only show if there was any additional information entered by the user.

Event Time

The time the DND status event occurred.

Extension

The extension number the DND status event occurred on.

Extension Name

The description of the extension the event occurred on.

12.5 Real Time Data

The following data fields are only available on Real-Time Views, not in any of the Historical Report Templates.

Active Call Statistics - Data relating to calls that are currently active on the telephone system etc

Miscellaneous - Current Date, Time etc

12.5.1 Active Call Statistics

Call Rate

The number of external calls in the current call rate period.

Calls Active

The total number of active calls (any call whether ringing, hold or in progress)

Calls Busy

The total number of calls in the ringing or connected state

Calls Busy External

The total number of external calls in the ringing or connected state

Calls Busy External In

The total number of external inbound calls in the ringing or connected state

Calls Busy External Out

The total number of external outbound calls in the ringing or connected state

Calls Busy Internal

The total number of internal calls in the ringing or connected state

Calls In Progress

The total number of calls currently in a connected state.

Calls In Progress External

The total number of external calls in the connected state.

Calls In Progress External In

The total number of external inbound calls in the connected state

Calls In Progress External Out

The total number of external outbound calls in the connected state

Calls In Progress Internal

The total number of internal calls in the connected state

Calls On Hold

The total number of calls in the hold state.

Calls On Hold External

The total number of external calls in the hold state.

Calls On Hold External In

The total number of external inbound calls in the hold state.

Calls On Hold External Out

The total number of external outbound calls in the hold state.

Calls On Hold Internal

The total number of internal calls in the hold state.

Calls Ringing

The total number of calls in the ringing state.

Calls Ringing External

Total number of external calls in the ringing state.

Calls Ringing External In

The total number of external inbound calls in the ringing state.

Calls Ringing External Out

The total number of external outbound calls in the ringing state.

Calls Ringing Internal

The total number of internal calls in the ringing state.

Inbound Call Rate

The number of inbound external calls in the last Call Rate period.

Longest Call (Call Time)

The longest call time of any active call on the telephone system.

Longest Call (Talk Time)

The longest talk time of any active call on the telephone system.

Longest Call (Ring Time)

The longest ring time of any active call on the telephone system, this includes connected calls that rang.

Longest Waiting

The longest ring time of a call in the ringing state.

Lost Call Rate

The number of lost calls in the last Call Rate period.

Outbound Call Rate

The number of outbound external calls in the last Call Rate period.

12.5.2 Miscellaneous

Current Date

The current date.

Current Date / Time

The current date and time.

Current Time

The current time.

Current Year

The current year.

Day of Month

The current day of the month.

Day of Week

The current day of the week.

> All dates and times shown relate to the current time on the server running the solution.

13 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

13.1 Remote/Teleworker Connections

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

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

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

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

VPN

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

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

Port Forwarding

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

For more information on Port Forwarding please click here.

MiVoice Border Gateway

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

For more information on the MiVoice Border Gateway please click here.

13.1.1 Connecting Through Firewalls

Port Forwarding

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

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

Port Forwarding for Remote Phone Manager Desktop Connections

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

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

* Only required when the Softphone is running

Port Forwarding for Remote Phone Manager Mobile Connections

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

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

13.1.2 MiVoice Border Gateway

When a MiVoice Border Gateway (MBG) is being used on the telephone system for remote client and/or teleworker connections, there are certain configurations that must be implemented in order to allow Phone Manager Desktop, Phone Manager Mobile, Phone Manager Softphone and/or 69xx Teleworker connections to pass through it.

> This section is not designed as an MBG technical guide but as a indication of areas that need to be configured. For more information on the MBG configuration, please refer to the relevant MBG manuals.

MiVoice Border Gateway Requirements

To use MiVoice Office Application Suite with a MiVoice Border Gateway (MBG) for remote connections, the MBG must be running v10 or higher and be configured in Gateway mode.

MiVoice Office Application Suite Configuration

For the MCS to be able to support teleworker SIP extensions (either Phone Manager Desktop Softphones or 69xx phones), it needs to know two pieces of information:

1. The internal IP Address of the MBG
2. The external IP Address of the MBG

The internal IP address of the MBG needs to be known for two reasons. The first is so that the MCS can identify which 69xx phones it receives requests from are actually Teleworkers. The second is so that it knows how to communicate with the MBG's API for SIP User deployment.

The external IP address of the MBG needs to be known so that it can be passed to Phone Manager Desktop and 69xx phones when they are registering their SIP connections.

Configure the MCS with the MBG's Internal IP Address:

- 'Configuration -> Site Settings -> Phone Systems -> MiVoice Border Gateway', enter the internal IP address of the MBG

Configure the MCS with the MBG's External IP Address:

- 'Configuration -> Site Settings -> Phone Systems -> [Your PBX Name]', enter the external IP address of the MBG into the NAT IP Address property for each node. If the external registration port for SIP has been changed on the MBG, update the NAT SIP Port as well.

Once the MCS has the information above, it will be able to identify teleworker 69xx phones and will be able to pass them the information required to connect to the MBG.

Port Forwarding

There are various ports that are used by the different client elements of MiVoice Office Application Suite. Please review the port forwarding section for the client that requires remote access.

Phone Manager Desktop Port Forwarding on MBG

Phone Manager Desktop uses the following TCP/UDP ports to communicate back to the MCS:

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.

For Phone Manager Desktop to be able to connect back to the MCS, these ports must be forwarded through the MBG to the server running the MCS.

Configuring Port Forwarding for Phone Manager Desktop

To forward the required Phone Manager Desktop ports, 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 server:

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. If the Phone Manager Desktop Softphone is being used, follow the Teleworker guide on SIP User configuration.

> For more information on configuring Phone Manager Desktop Softphone as an MBG Teleworker, please refer to the MBG Teleworker section.

Phone Manager Desktop Configuration

To connect a the Phone Manager Desktop remotely, open the 'Settings' page within Phone Manager and 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

> The External IP Address of the MBG should be entered into the remote section of the Client Locations setting on the MCS server.

Phone Manager Mobile Port Forwarding on MBG

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

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

> * Only required when the Softphone is running. Phone Manager Mobile does note require Teleworker licences or configuration on the MBG.

Configuring Port Forwarding for Phone Manager Mobile

Complete the following configuration on the MBG:

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

If using a Softphone then configure the following port forwarding:

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

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

Phone Manager Mobile Configuration

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

A trusted certificate is also recommended for Phone Manager Mobile connections.

69xx Phone Port Forwarding on MBG

69xx phones use the following TCP port to communicate to the MCS server:

Port	Target	Direction	Description
TCP 8202	MCS Server	Inbound	Used to communicate to the MCS server to provide configuration, user data etc.

Configuring MBG Port Forwarding for 69xx Phones

Complete the following configuration on the MBG:

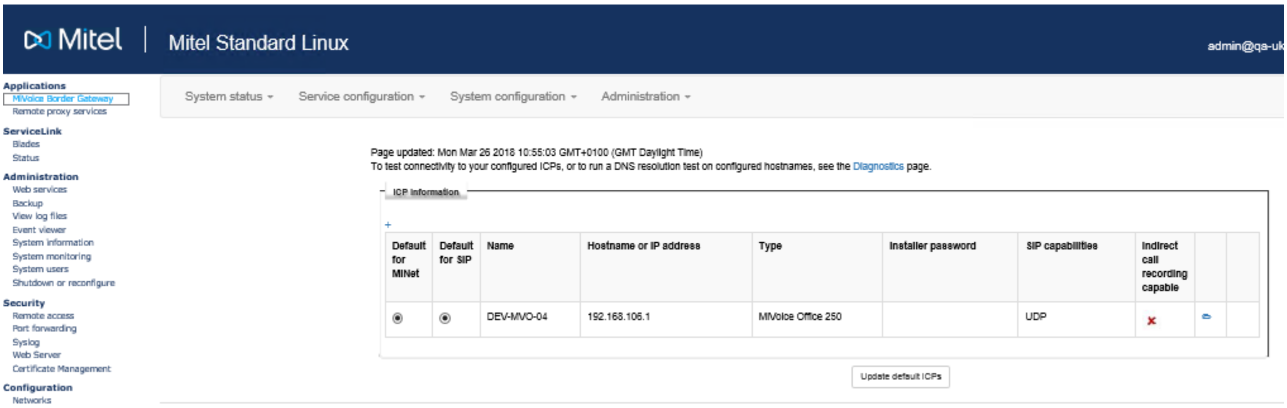
- On the 'MBG Security -> Port Forwarding' page, create the port forwarding rules for TCP 8202 with the Destination Host IP Address pointing to the IP address of the MCS host.

SIP User Teleworker

To use 69xx or Phone Manager Desktop Softphone remotely through an MBG, a SIP User teleworker needs configuring on the MBG.

Add one or more Nodes as ICPs on the MBG:

- On the 'MiVoice Border Gateway -> Service configuration -> ICPs' page, create an ICP instance for each MiVO 250 node that will be supporting teleworker SIP phones.



Ensure the 'Hostname or IP Address' setting used for the ICP matches the IP Address configured for the Node on the MCS server.

MiVoice Office 250 Configuration for Teleworker SIP Users

For Phone Manager Desktop Softphones and 69xx phones connecting through an MBG, the following setting needs enabling against the SIP Peer on the telephone system:

- Use Registered Username = True
- NAT Address Type = Native

If these settings are not configured against each SIP extension to be used as a teleworker, there will be issues with audio through the MBG.

When using a MiVoice Border Gateway, the internal authorisation name must match the extension number of the phone otherwise authentication with the telephone system will fail.

Automatic Teleworker Provisioning

To simplify the deployment of SIP teleworker phones, the MCS can use an API on the MBG to automatically provision SIP Users for SIP extension. This provides the following benefits:

- The default random credentials created on the MiVO 250 for each SIP extension can be passed to the MBG automatically
- The MCS can use randomly generated set-side credentials for teleworker phones
- There is no need to re-type the authorisation credentials into MCS and the MBG, removing a repetitive and time consuming task and reducing the risk of mistakes
- The engineer/administrator deploying the teleworker phone does not need to know the SIP authorisation credentials at any stage

For automated provisioning to work end-to-end between the MiVO 250, MiVO App Suite and MBG, the MiVO 250 must be running at least 6.3 SP1 and any CT Gateway must be running at least 5.0.64.

Enabling the Rest API for Automatic Teleworker Deployment

For the MCS to be able to communicate with the MBG and deploy teleworker SIP Users, it requires some connection information as well as a valid API token from the MBG. This section documents how to configure the MBG to accept API requests and the steps involved in setting up the token exchange. To complete this process, access to the MBG website and the MCS configuration website are required.

> ⚠ Once the Rest API has been enabled on MCS and it has a valid token, the MCS server will take any SIP extension that has been configured with remote authorisation credentials and provision it onto the MBG. Any existing credentials configured for SIP Users on the MBG will be overwritten with those configured on the MCS.

Step 1: Create a new web service consumer on the MBG:

- On the MBG 'Administration -> Web services' page, press 'Start' to enable web services then press 'Add a new consumer' and provide the following information:
    - Active = Yes
    - Name = MiVoice Office Application Suite
    - ConsumerID = MiVOAppSuite
    - Permissions:
        - Base/managetoken = Read/Write
        - MBG/v1/icps = Read
        - MBG/v1/devices = Read/Write
- Make a note of the shared secret then save the new consumer.

Step 2: Complete the token request from MCS to MBG:

- On the MCS 'Configuration -> Site Settings -> Phone Systems -> MiVoice Border Gateway' page:
    1. Check the 'Enable Rest API' box.
    2. Press the 'Request Access Token' button to load the 'Request Access Token' form.
    3. Enter the Name, Consumer ID and Shared Secret to match those created on the MBG in step 1
    4. Press the 'Save & Test API Credentials' button to initiate a token request with the MBG server.
- On the MBG 'Administration -> Web services' page:
    1. Locate the 'Temporary tokens' section at the bottom of the page
    2. Press the 'approve' button against the temporary token request.
    3. Highlight and make a copy of the 'Verifier' code (you may need to refresh the page to see the temporary token)
- On the MCS 'Configuration -> Site Settings -> Phone Systems -> MiVoice Border Gateway' page:
    1. Paste or enter the verifier code into the request window
    2. Press the 'Retrieve Final Access Token' button to complete the token request with the MBG server.

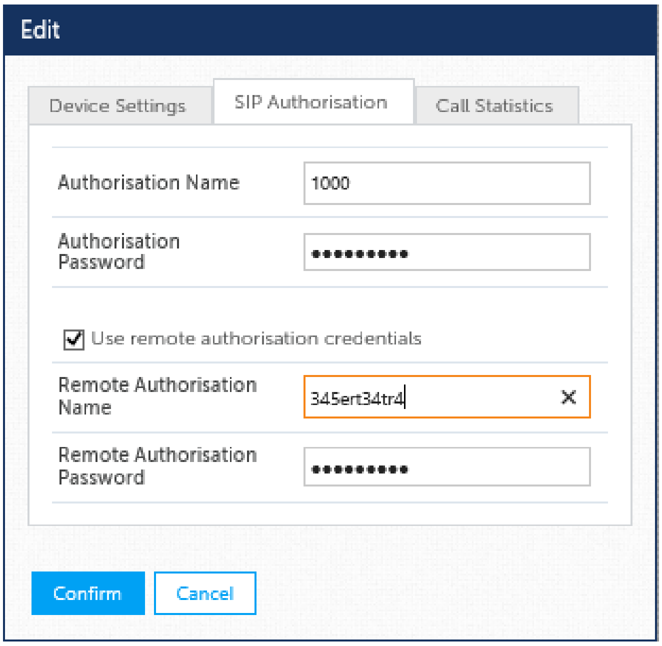
If the verifier is correctly entered, the MCS should be able to successfully request an API token from the MBG. This token will allow the MCS to provision SIP Users on the MBG for a period of 12 months. To avoid having to repeat the above process every 12 months, the token's expiry date can be extended on the MBG by pressing the 'Renew' button against the token in the 'Final tokens' section of the web services page.

> The internal IP address configured in the Nodes section of the MCS website must match the IP Address configured on the corresponding ICP on the MBG website. If they do not match, the MCS will not be able to find the correct ICP when deploying a teleworker phone.

How Automatic Teleworker Deployment Works

Once the Rest API has been configured, MCS will automatically provision teleworker SIP extensions on the MBG.

The MCS will provision any SIP extension that has had the 'Use remote authorisation credentials' setting configured against it:



Provisioning a SIP Teleworker Extension

To instigate the MCS provisioning of a SIP extension on the MBG, navigate to the 'Configuration -> Site Settings -> Phone Systems -> [Your PBX Name]' page. Edit the required SIP extension and then check the 'Use remote authorisation credentials' check box. The MCS will pre-populate the remote authorisation name and password with random values. Pressing save will update the credentials stored for the extension and will start the teleworker provisioning process.

Un-Provisioning a SIP Teleworker Extension

To un-provision a SIP extension from the MBG, follow the provisioning process but uncheck the 'Use remote authorisation credentials' check box. Once save is clicked it will instigate the MCS removing the SIP User from the MBG.

> This will only work for SIP extensions that were previously provisioned by the MCS. If a SIP User was manually added to the MBG it may need to be manually removed. If a SIP extension has been provisioned on the MBG by the MCS, the MBG's ID for the SIP user will be displayed on the SIP Authorisation form of the extension in MCS.

Provisioning Multiple SIP Teleworker Extensions

To provision/unprovision multiple SIP extensions at the same time, a specific form is provided on the MiVoice Border Gateway page of the MCS. Pressing the 'Provision Teleworker Phones' button will load the form. To provision extensions, move them from the left side of the form to the right. To un-provision them, do the opposite. Saving the form down will initiate provisioning with the MBG.

> Any SIP extension provisioned using this method will automatically have a random remote authentication username and password assigned if they do not have them set already.

For information on how to provision SIP Users manually, please refer to the Manual Teleworker Provisioning section.

> Each Teleworker connection on the MBG requires a Teleworker licence.

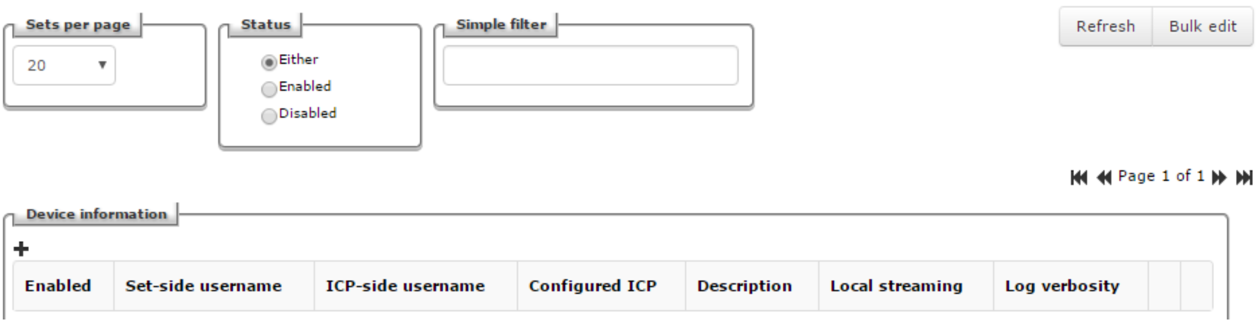
> In addition to configuring SIP Users for teleworker extensions, they must also be configured for any SIP Hot Desk extensions that will be logging into a teleworker phone.

13.1.2.1 Manual Teleworker Provisioning

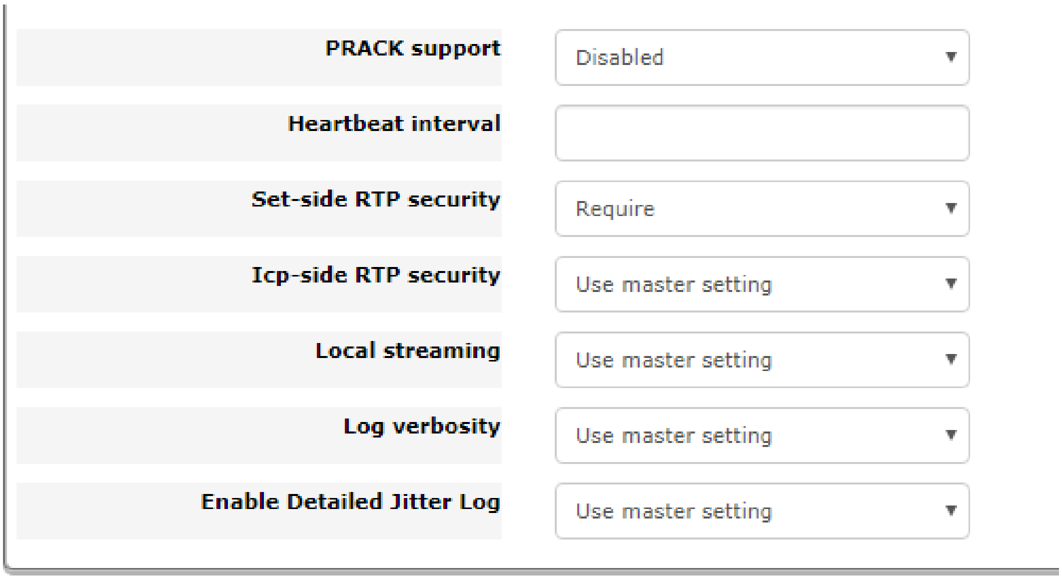
Manually Configure Teleworker SIP Users

For each of the SIP extensions that are to connect as Teleworkers, a SIP Users needs to be created. The section below explains how to do this manually. However, using a provisioning API built into the MBG, the MCS can automatically provision SIP Users along with the necessary authorisation credentials. For more information, please refer to the Automatic Teleworker Provisioning section.

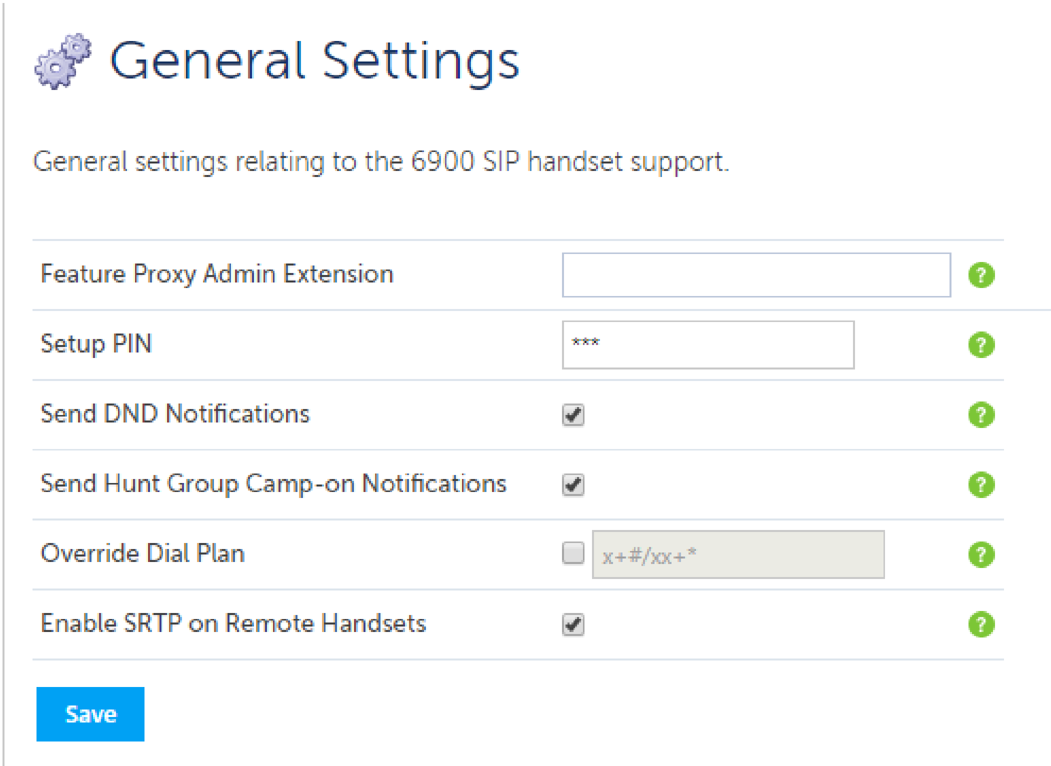
- In the 'MiVoice Border Gateway -> Service Configuration -> SIP Devices', add the required SIP device by pressing the + button below the Device Information label, then configured the following settings:
    1. Enable = True
    2. Set-Side username = This should match the remote authentication username configured for the SIP extension on MCS
    3. ICP-Side username = This should always be the SIP device's extension number
    4. Configured ICP = PBX the SIP extension is configured on (the ICP configured on MBG in previous step)
    5. Set-Side Password = This should match the remote authentication password configured for the SIP extension on MCS
    6. Confirm Set-Side Password = In-bound authentication password
    7. ICP-Side Password = This should match the authentication password for the SIP extension on the PBX
    8. Confirm ICP-Side Password = In-bound authentication password



- It is recommended to enable SRTP (secure RTP)
    1. PRACK support - set as Disabled
    2. Set-side RTP security - set as Require



3. Enable SRTP in the MCS Website (Features->6900 SIP Handsets->General Settings)



⚠ If SRTP is enabled on the MCS without this MBG configuration then the handsets will be able to make calls but not receive them.

13.2 6900 Handset Engineering Guidelines

This section of the engineering guidelines provides information on the architecture and implementation of the 6900 Handsets on the MiVoice Office 250.

Overview

The 6900 handset is Mitel's new premium range of telephones. Currently there are three models of handset available; 6920, 6930 & 6940. From release 5.1, the MiVoice Office Application Suite supports the 6900 handsets and acts a configuration server to allow many of the MiVoice Office 250's features to be used on the 6900's SIP telephones.

SIP Implementation

To connect to the MiVoice Office 250, 6900 handsets operate as a SIP extension. All call control functionality is provided through the SIP connection directly to the telephone system (or via a MiVoice Border Gateway).

Each 6900 handset requires a Cat-F license on the telephone system.

> Out of the box, all 6900 handsets come with MiNET firmware for a MiVoice Business. SIP firmware must be loaded onto the handsets before they will connect to a MiVoice Office 250.

Licensing

In addition to the Cat-F licensing on the telephone system, there are two levels of license on the MiVoice Office Application Suite that are used to control 6900 handsets:

- Mitel 6900 Handsets (Basic), provides access to core functionality (Firmware, Keymaps, Configuration, Paging etc)
- Mitel 6900 Handsets (Advanced), provides access to advanced functionality (Currently this includes the ability to Change Caller ID and Recording Pause/Resume toolbar buttons).

Without a license, the 6900 handset can still be connected to the telephone system but would need to be manually configured and would only support the basic SIP features.

> Licensing may change at any time. Please refer to the latest product bulletins for updates on how 6900 handsets are licensed.

Documentation

In addition to this engineering guide, the following documents contain relevant information to implement 6900 handsets on the MiVoice Office 250:

Document	Description
Mitel Communication Service -Technical Manual / Online Help	Provides information on how to configure the MCS server to support 6900 Handsets, including; Dial Plans, Configuration Profiles, Keymap Profiles Alarm Notification, Page Zones and Image Handling.
6.3 MiVoice Office 250 Features and Programming Guide	Provides information on telephone system SIP configuration and restrictions.
6800/6900 SIP 5.0 Admin Guide	Provides an exhaustive guide to all 6900 handset features including configuration options.
6920[/30/40] SIP 5.0 Quick Reference Guides	Model specific quick reference guides to introduce end-user features.
6920[/30/40] SIP Phone User Guides	Model specific phone guides to cover all model specific configuration & features.

Implementing 6900 Handsets on MiVoice Office 250

The following sections cover various aspects of 6900 handset implementation on the MiVoice Office 250.

- Connectivity, provides information on the architecture of how 6900 handsets, the MiVoice Office 250 and MiVoice Office Application Suite work together.
- Rollout, provides information on how to install 6900 series handsets including MiVoice Office 250 configuration, firmware updates and MiVoice Office Application Suite configuration.
- SIP Hot Desking, provides information on how SIP hot desking works and how it is configured.
- Teleworker/Remote worker, provides information on how 6900 handsets can be implemented in Teleworker/Remote worker scenarios.
- Multi-Node, provides information on how 6900 handsets can be implemented in multi-node environments.

13.2.1 6900 Handset Connectivity

Each 6900 handset connects to both the MCS and MiVO 250 during normal operation:

- A direct SIP connection between the Handset and the MiVoice Office 250 provides:
  - Audio
  - Call Control
  - Message waiting notification
- Further to this a Http/Https Configuration link between the Handset and MCS provides:
  - Firmware Updates
  - Configuration Files
  - Keymaps
  - Messages (Alarm/DND/FWD/Camp-On Notifications)
  - Status Icons (Alarm/DND/FWD status)

Connection Type	Default Ports Used	Description
SIP	TCP 5060	Used for SIP communication to the MiVoice Office 250
	UDP 20000-20500	Used for RTP Audio traffic between the handset and the MiVoice Office 250
Configuration Server	UDP 69	TFTP for initial firmware download and configuration
	TCP 8202/8203	HTTPS/HTTP requests from the handset to the MCS. This includes: • Firmware • Softkeys • Action URIs • Images • Directories
	TCP 80	HTTP traffic from the MCS to the 6900 handset

SIP Connectivity

The handsets connect directly to the MiVoice Office 250 via SIP for call control and audio. Each handset has configuration options for how to connect to the telephone system:

- SIP Auth Name / Password
- SIP Registrar IP / Port

The SIP configuration, including authentication details is requested from the MCS configuration server during startup. The configuration server will then pass any updates to the phone when online if configuration changes are made on the server.

If the 6900 handset has successfully connected to the configuration server, it will have been programmed with the necessary SIP connection information.

If the link to the configuration server is offline for any reason (server reboot, network connectivity, etc.), the 6900 handset will still be able to make/receive calls.

> If required, Network Groups on the telephone system can be used for Peer-to-Peer Media

Configuration Server

MCS acts as a 'Configuration Server' for the 6900 handsets. In performing this role, it provides the phone with the following:

- Firmware Updates
- Configuration
- Keymaps
- Messages & Notifications
- Images
- Directories
- MiVoice Office 250 Features:
    - ACD
    - UCD
    - IC and System Speed Dial Directories
    - Manual Forwarding
    - Paging
    - Account Codes (Optional & All Calls Following)
    - Night Mode Control
    - BLF/DSS Key Updates (Including a new User based status key)

These features are on top of the telephone system's broad range of SIP features.

> Please refer to the Feature Comparison section for more information on differences between 6900 handsets and digital/Minet handsets.

Firmware Updates

MCS will provide firmware updates when they are available/configured for the handset. This can be via TFTP or HTTPS. TFTP updates are generally only used when first configuring a 6900 handset to convert it from MiNET to SIP firmware. Once this has occurred, MCS will instruct the phone to connect via HTTPS only. All future firmware requests will then be performed via HTTPS.

For more information on configuring firmware updates, please refer to the Firmware section of the Mitel Communication Service - Technical Manual.

Configuration

Each 6900 handset has a set of configuration options that control how the handset operates. These configuration options can be set in one of two ways:

- Using the handset (through the settings application on the phone or using it's web user interface)
- MCS Configuration Server

MCS provides configuration profiles so that options can be configured centrally and then applied to multiple handsets.

In addition, MCS controls a subset of the configuration options such as SIP connection details and Dial Plan, to ensure features such as SIP Hot Desking operate correctly, and that the handset operate as closely as possible to their MiNET and Digital counterparts.

Configuration provided by the MCS will overwrite any configuration added locally on the handset.

For more information on Configuration Profiles, please refer to the Configuration Profile section of the Mitel Communication Service - Technical Manual.

Keymaps

Each handset has a range of softkeys that can be configured to perform any one of a number of features. Keymaps can be configured locally on the handsets, however, to take advantage of any of the MCS provided features (ACD, DND, UCD etc), the keys must be programmed via a keymap profile on the MCS.

Although keys are programmed on the phone centrally, there are two types or classes of softkey that can be add be added to a handset:

- Phone based key
- Server based key

The features of phone based keys are provided locally by the handset, with no interaction from the MCS. The features of server based keys rely on updates and responses from the server to operate. Pressing a server based key will cause the handset to request information from the MCS server to action the required feature. Phone based keys will continue to operate if the link to the configuration server is down, server based keys will not.

For more information on Keymap Profiles and features available, please refer to the Keymap Profile section of the Mitel Communication Service - Technical Manual.

Messages & Notifications

Each handset has the ability to show messages and notifications (some will only display in idle mode) and is used by the MCS server to display the following:

- The handset DND status
- Telephone System Alarms
- Local Forward status
- Camp-On notifications
- DND notifications to calling parties where applicable

These messages are automatically sent by the MCS server to the handset and require no configuration.

In addition to the server based messages, the handset will also show the following messages to the user:

- Message waiting indication
- Missed call indication

Images

Handsets have the ability to display server provided images in a variety of scenarios:

- As an Avatar on the idle screen (6940 only)
- Against softkeys
- During a call to show other user's avatars
- Background screen in idle mode
- Custom screen savers

The MCS server provides the handsets with the images. Where possible it will provide avatars for internal extensions that have been mapped to an MCS user and will also match external numbers to users based on external DEE numbers.

Screen savers and background images can be configured on the MCS and assigned to handsets using configuration profiles.

The handset will cache images locally and will request them again when this cache expires.

Directories

Each handset has a feature rich directory facility which allows the user to search for contacts across multiple directory sources at the same time.

The directory sources available include:

- Mobile (if Bluetooth is enabled)
- CSV Imports
- LDAP lookups

The LDAP facility can be used to configure the handsets to lookup an existing customer database.

The CSV import facility is currently used by the MCS to provide the handsets with Internal and System Speed Dial directories from the telephone system.

13.2.2 6900 Handset Deployment

The following list outlines all the steps involved in deploying 6900 series handsets:

> Ensure you have done all of stage 1 and 2 before you do stage 3.

- Stage 1 - MiVoice Office 250 system / MiVoice Office Application Suite Configuration
  - Configure the Encryption Password on the MiVoice Office 250
  - Configure the Encryption Password for each Node on the MiVoice Office Application Suite
  - Configure the IP Address and Port numbers for SIP against each node
  - Prepare Keymap & Configuration Profiles

- Stage 2 - Create 69xx SIP Devices
  - Add a '69xx SIP Device' for each 6900 handset and SIP hot desk phone using the parameters in the MiVO Office 250 configuration section
  - Add SIP credentials to each SIP device on the phone systems page (only if not using 6.3 SP1)

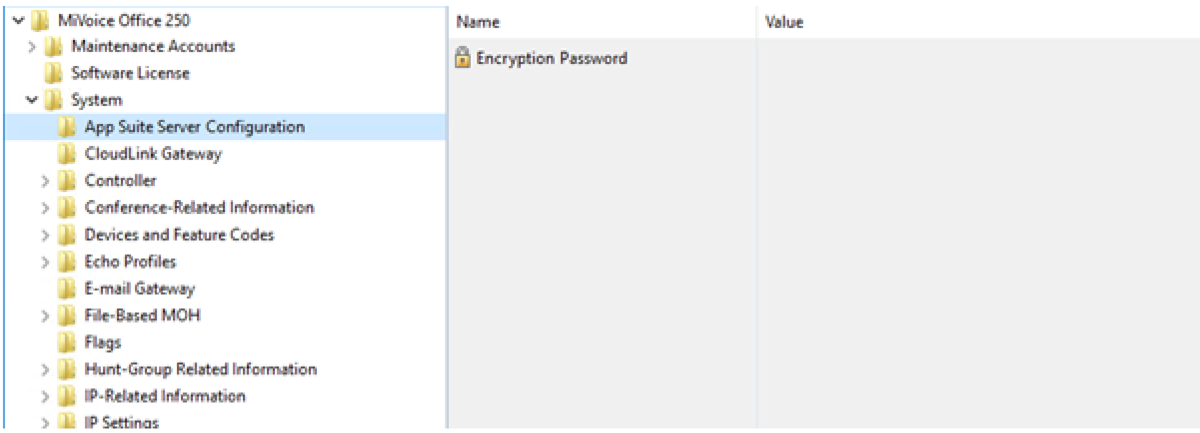
- Stage 3 - Handset Deployment (see Handset Deployment section)
  - Update the handset firmware from MiNET to SIP
  - Initialize the handset with the MCS server
  - Apply keymaps and/or configuration profiles

Stage 1 - MiVoice Office 250/Application Suite Configuration

The following configurations should only need to be performed once. Stages 2 & 3 will need to be repeated for each new 69xx phone deployed.

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

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



Encryption Password

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

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

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

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

Node Configuration for SIP

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

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

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

Keymap & Configuration Profiles

Each handset will require a keymap and configuration profile. The MCS comes with default keymap and configuration profiles with the most commonly selected options already added. These can be customised as required or new profiles can be added to suite the customer's company wide or department needs.

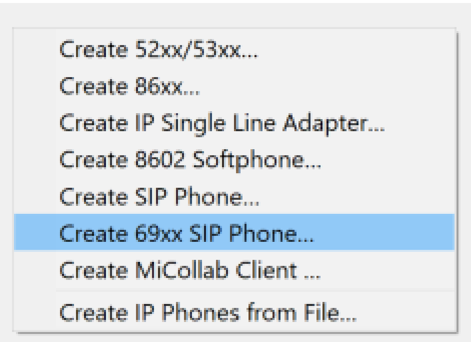
> Having Time Server Settings (Time Server 1-3) in the Configuration Profile used will ensure the Handsets keep good time. Where a configuration is used by local and remote handsets, ensure at least one NTP server specified is a publicly accessible NTP server that a remote handset can access

> Other items to configure on the MCS server include: Page Zones, Background & Screen Saver Images

Stage 2 - Create 69xx SIP Devices

69xx SIP Phone

From release MiVO 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.

If release 6.3 SP1 of the MiVoice Office 250 & Encryption Password feature is not being used, the SIP credentials will need to be manually configured. Please refer to the Manual SIP Configuration section of the Technical Manual for more information.

Stage 3 - Handset Deployment

Once all the preparation work has been completed on the telephone system and MCS, the handsets can be deployed

The information below describes deploying handsets local to the MCS.
We always recommend (where possible) configuring handsets locally to MCS, prior to deploying in a remote location.

For remote deployment of a 6900 Handset where the firmware has not been updated refer to 6900 Handset Diagnostics & Troubleshooting section

There are two methods for deployment:

- Automatically using DHCP
- Manually (on the handset or the handset's web user interface)

Configuration Server Setup - Automatic

The easiest way to provide handsets with updated firmware and register them with the MCS server is to use DHCP.

This method should be used wherever possible, however there are some restrictions you need to be aware of:

- DHCP Option 66 must not already be in use
- Other 6900 handsets (MiNET or SIP) are in use on a different PBX

Configure the DHCP server: add the IP address or Hostname of the MCS server into option 66. When the 6900 handsets are plugged in, the TFTP server will automatically be configured and the registration process (and any firmware updates) will begin. The phone will reboot a number of times as firmware and configuration progresses.

The 6900 Handsets will also pick up the following DHCP options and use them as the configuration server address (in the order listed):

- 43
- 159
- 160
- 66

If any of these options are in use on the DHCP server then it will overwrite the configuration server used on the handset and stop it working. One possible source for causing a conflict is DHCP options for 5300 phones using option 43. These can be changed to use the preferred option 125 to avoid conflict.

> ⚠ By default, option 43 is enabled when using the built in DHCP on the MiVoice Office 250. This should be disabled when using 6900 handsets and MiNET handsets together. Option 125 should be used instead.

The handset will now be registered with the MCS server.

The Phone will have Line 1 and Line 2 showing as the Top Sofkeys, and 'Setup' as the first Softkey along the bottom.

The 'Phones' page within the configuration section of the MCS website can be used to view whether the handset has been identified. The MCS uses the handsets MAC Address to uniquely identify it.

Now bypass Manual Configuration section below and move on to the Initialising Handsets section.

> DHCP is the preferred method to automate Firmware update and Configuration setup as it reduces the number of steps involved.
>
> If you cannot use DHCP then follow the steps for manual setup below

Configuration Server Setup - Manual

Step 1

Out of the box, all 6900 handsets come with MiNET firmware installed. The first step in deploying the handsets is to change this to SIP firmware so that they can talk to the telephone system and the configuration server (MCS).

- Press the settings button (⚙) on the handset, then press the 'Advanced' key along the bottom of the screen.
- At this point you will be prompted to enter the administrator password. The default MiNET password is '73738'
- Navigate to 'Network' and then 'Static Settings' using the navigation keys (D-pad) or the touch screen if using a 6940.
- In the 'TFTP server IP Address' box, enter the IP address for the MCS server then 'Close' to exit the menu, and the handset will restart connecting to MCS, download and update to SIP firmware.

Step 2

Once the phone is running the correct firmware version, the next step is to tell the phone where the configuration server is.

- Add the configuration server details on the phone manually, press the settings button (⚙) on the handset, then press the 'Advanced' key along the bottom of the screen.
- At this point you will be prompted to enter the administrator password. The default SIP password is '22222'.
- Once the password has been accepted, use the navigation keys (D-pad) or touch screen on 6940 to navigate to the 'Configuration Server' section.
- Populate the 'Primary Server' box with the IP address or DNS name of the MCS server. Press 'Save' and then reboot the handset.

After a reboot, the phone will connect to the MCS server. As the phone is connecting over TFTP, the MCS server will provide HTTPS connection information and will then tell the phone to reboot.

> It is possible that there will be more than one reboot at this stage as the firmware update is completed

The handset should now be registered with the MCS server.

The Phone will have Line 1 and Line 2 showing as the Top Sofkeys, and 'Setup' as the first Softkey along the bottom.

The 'Phones' page within the configuration section of the MCS website can be used to view whether the handset has been identified. The MCS uses the handsets MAC Address to uniquely identify it.

Initialising Handsets

Once a handset makes it's first connection request to the MCS, it will be in 'Unassigned' mode. This means the MCS server is aware of the handset, but does not know which SIP extension on the telephone system it should be configured as.

Handsets can be initialised by using either (a) the 'Setup' button on the phone, or (b) editing the handset on the 'Phones' page of the MCS website:

(a) To use the setup process on the phone, press the 'Setup' button and enter the setup PIN (default ***). The handset will then prompt for the extension number. Once the extension number has been correctly entered, the MCS server will pass the handset all SIP, keymap and configuration information it requires.

(b) To use the configuration in MCS, browse to MCS Configuration -> Features -> 6900 Handsets -> Phones. Locate the MAC address of the phone in question and Edit the record to add the SIP extension number.

13.2.3 6900 Handset SIP Hot Desking

SIP Hot Desking is a feature that has been designed specifically for 6900 handsets. Any SIP extension on the telephone system can be configured on the MCS as a SIP Hot Desk Phone. Once this has been done, it can be used to log onto any 6900 handset connected to the MCS server that has been enabled to accept hot desk logons.

> SIP hot desking is different from both agent hot desking and MiVoice Office 250 hot desking. The different types of hot desking cannot be used together.

SIP Hot Desk Features

When logging into a 6900 handset with a SIP hot desk login, the handset will be reconfigured so that it becomes the hot desk extension. The following list shows what configuration gets updated on the handset:

- SIP credentials (Extension No, Username etc)
- Keymap
- Configuration Options

When a SIP hot desk logs in to a handset, the handset will cease to be its base SIP extension and will become the SIP hot desk extension. If the SIP hot desk that has logged in resides on a different node than the handsets fixed extension, the handset will un register as a SIP device on one node and will re-register on the new node where the handset resides.

When the SIP hot desk logs out, the handset will revert back to its fixed extension.

SIP Hot Desk phones can be configured on the MCS for all features that a fixed 6900 handset can:

- Configuration Profiles
- Keymaps
- Alarm Notification
- Page Zones

All of the above features will be applied when a SIP hot desk phone logs on.

If a SIP hot desk phone has not been assigned a Keymap Profile or Configuration Profile directly, the keymap and configuration profiles for the base extension will be used.

Adding a SIP Hot Desk Extension

> A SIP extension to use for Hot Desking is no different in PBX configuration from a SIP Extension used as a base handset extension. Any SIP extension not assigned to a base extension is available for use as a SIP Hot Desk Extension

On the MCS server, Configuration -> Features -> 6900 Handsets

Enable Base extensions for Hot Desking

In the Phones section edit all the base extensions you will want to be able to SIP Hot Desk into and Tick the 'Enable Hot Desking check box'

Enable an SIP Extension to be a Hot Desking device

In the SIP Hot Desking section, press the 'Add' button. In the form that appears, enter the number of the SIP device on the telephone system to configure as a hot desk phone (the device picker will filter out any SIP device which are already have a fixed mapping to a handset).

Once a hot desk phone has been created, it can be used to logon to any handset that has been enabled for accepting hot desk logons.

> ⚠ 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 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.

13.2.4 6900 Handset Teleworker

69xx phones are supported as Teleworkers on the MiVoice Border Gateway (MBG) using a SIP User. The following section outlines the configuration required to deploy a teleworker on MBG.

MiVoice Border Gateway Requirements

To use MiVoice Office Application Suite with a MiVoice Border Gateway (MBG) for remote connections, the MBG must be running v10 or higher and be configured in Gateway mode.

MiVoice Office Application Suite Configuration

For the MCS to be able to support teleworker SIP extensions (either Phone Manager Desktop Softphones or 69xx phones), it needs to know two pieces of information:

1. The internal IP Address of the MBG
2. The external IP Address of the MBG

The internal IP address of the MBG needs to be known for two reasons. The first is so that the MCS can identify which 69xx phones it receives requests from are actually Teleworkers. The second is so that it knows how to communicate with the MBG's API for SIP User deployment.

The external IP address of the MBG needs to be known so that it can be passed to Phone Manager Desktop and 69xx phones when they are registering their SIP connections.

Configure the MCS with the MBG's Internal IP Address:

- 'Configuration -> Site Settings -> Phone Systems -> MiVoice Border Gateway', enter the internal IP address of the MBG

Configure the MCS with the MBG's External IP Address:

- 'Configuration -> Site Settings -> Phone Systems -> [Your PBX Name]', enter the external IP address of the MBG into the NAT IP Address property for each node. If the external registration port for SIP has been changed on the MBG, update the NAT SIP Port as well.

Once the MCS has the information above, it will be able to identify teleworker 69xx phones and will be able to pass them the information required to connect to the MBG.

Port Forwarding

69xx Phone Port Forwarding on MBG

69xx phones use the following TCP port to communicate to the MCS server:

Port	Target	Direction	Description
TCP 8202	MCS Server	Inbound	Used to communicate to the MCS server to provide configuration, user data etc.

Configuring MBG Port Forwarding for 69xx Phones

Complete the following configuration on the MBG:

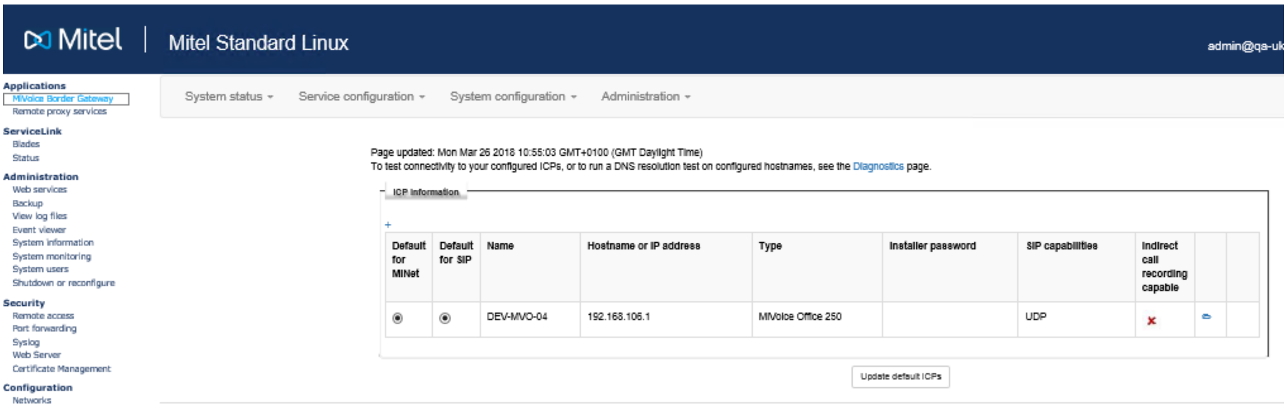
- On the 'MBG Security -> Port Forwarding' page, create the port forwarding rules for TCP 8202 with the Destination Host IP Address pointing to the IP address of the MCS host.

SIP User Teleworker

To use 69xx or Phone Manager Desktop Softphone remotely through an MBG, a SIP User teleworker needs configuring on the MBG.

Add one or more Nodes as ICPs on the MBG:

- On the 'MiVoice Border Gateway -> Service configuration -> ICPs' page, create an ICP instance for each MiVO 250 node that will be supporting teleworker SIP phones.



> Ensure the 'Hostname or IP Address' setting used for the ICP matches the IP Address configured for the Node on the MCS server.

MiVoice Office 250 Configuration for Teleworker SIP Users

For Phone Manager Desktop Softphones and 69xx phones connecting through an MBG, the following setting needs enabling against the SIP Peer on the telephone system:

- Use Registered Username = True
- NAT Address Type = Native

If these settings are not configured against each SIP extension to be used as a teleworker, there will be issues with audio through the MBG.

> When using a MiVoice Border Gateway, the internal authorisation name must match the extension number of the phone otherwise authentication with the telephone system will fail.

Automatic Teleworker Provisioning

To simplify the deployment of SIP teleworker phones, the MCS can use an API on the MBG to automatically provision SIP Users for SIP extension. This provides the following benefits:

- The default random credentials created on the MiVO 250 for each SIP extension can be passed to the MBG automatically
- The MCS can use randomly generated set-side credentials for teleworker phones
- There is no need to re-type the authorisation credentials into MCS and the MBG, removing a repetitive and

time consuming task and reducing the risk of mistakes
- The engineer/administrator deploying the teleworker phone does not need to know the SIP authorisation credentials at any stage

> For automated provisioning to work end-to-end between the MiVO 250, MiVO App Suite and MBG, the MiVO 250 must be running at least 6.3 SP1 and any CT Gateway must be running at least 5.0.64.

Enabling the Rest API for Automatic Teleworker Deployment

For the MCS to be able to communicate with the MBG and deploy teleworker SIP Users, it requires some connection information as well as a valid API token from the MBG. This section documents how to configure the MBG to accept API requests and the steps involved in setting up the token exchange. To complete this process, access to the MBG website and the MCS configuration website are required.

> Once the Rest API has been enabled on MCS and it has a valid token, the MCS server will take any SIP extension that has been configured with remote authorisation credentials and provision it onto the MBG. Any existing credentials configured for SIP Users on the MBG will be overwritten with those configured on the MCS.

Step 1: Create a new web service consumer on the MBG:

- On the MBG 'Administration -> Web services' page, press 'Start' to enable web services then press 'Add a new consumer' and provide the following information:
  - Active = Yes
  - Name = MiVoice Office Application Suite
  - ConsumerID = MiVOAppSuite
  - Permissions:
    - Base/managetoken = Read/Write
    - MBG/v1/icps = Read
    - MBG/v1/devices = Read/Write
- Make a note of the shared secret then save the new consumer.

Step 2: Complete the token request from MCS to MBG:

- On the MCS 'Configuration -> Site Settings -> Phone Systems -> MiVoice Border Gateway' page:
  1. Check the 'Enable Rest API' box.
  2. Press the 'Request Access Token' button to load the 'Request Access Token' form.
  3. Enter the Name, Consumer ID and Shared Secret to match those created on the MBG in step 1
  4. Press the 'Save & Test API Credentials' button to initiate a token request with the MBG server.
- On the MBG 'Administration -> Web services' page:
  1. Locate the 'Temporary tokens' section at the bottom of the page
  2. Press the 'approve' button against the temporary token request.
  3. Highlight and make a copy of the 'Verifier' code (you may need to refresh the page to see the temporary token)
- On the MCS 'Configuration -> Site Settings -> Phone Systems -> MiVoice Border Gateway' page:
  1. Paste or enter the verifier code into the request window
  2. Press the 'Retrieve Final Access Token' button to complete the token request with the MBG server.

If the verifier is correctly entered, the MCS should be able to successfully request an API token from the MBG. This token will allow the MCS to provision SIP Users on the MBG for a period of 12 months. To avoid having to repeat the above process every 12 months, the token's expiry date can be extended on the MBG by pressing the 'Renew' button against the token in the 'Final tokens' section of the web services page.

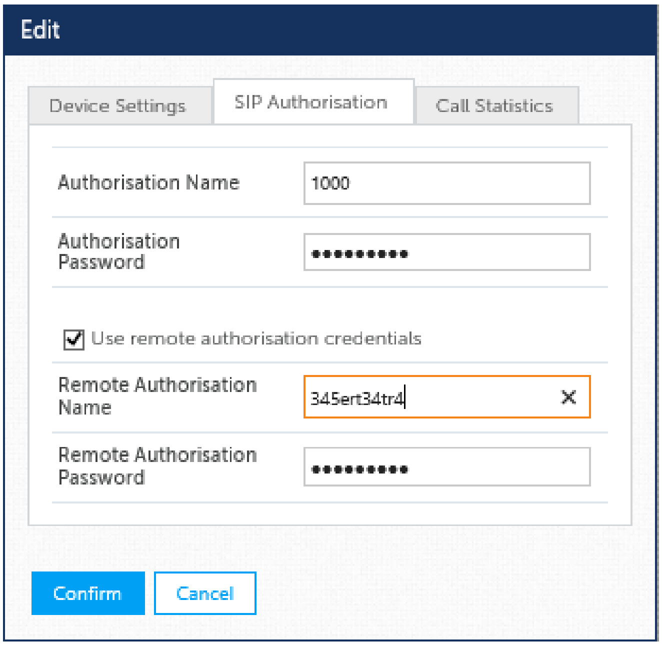
> The internal IP address configured in the Nodes section of the MCS website must match the IP Address configured on the corresponding ICP on the MBG website. If they do not match, the MCS will not be able to find

the correct ICP when deploying a teleworker phone.

How Automatic Teleworker Deployment Works

Once the Rest API has been configured, MCS will automatically provision teleworker SIP extensions on the MBG.

The MCS will provision any SIP extension that has had the 'Use remote authorisation credentials' setting configured against it:



Provisioning a SIP Teleworker Extension

To instigate the MCS provisioning of a SIP extension on the MBG, navigate to the 'Configuration -> Site Settings -> Phone Systems -> [Your PBX Name]' page. Edit the required SIP extension and then check the 'Use remote authorisation credentials' check box. The MCS will pre-populate the remote authorisation name and password with random values. Pressing save will update the credentials stored for the extension and will start the teleworker provisioning process.

Un-Provisioning a SIP Teleworker Extension

To un-provision a SIP extension from the MBG, follow the provisioning process but uncheck the 'Use remote authorisation credentials' check box. Once save is clicked it will instigate the MCS removing the SIP User from the MBG.

> This will only work for SIP extensions that were previously provisioned by the MCS. If a SIP User was manually added to the MBG it may need to be manually removed. If a SIP extension has been provisioned on the MBG by the MCS, the MBG's ID for the SIP user will be displayed on the SIP Authorisation form of the extension in MCS.

Provisioning Multiple SIP Teleworker Extensions

To provision/unprovision multiple SIP extensions at the same time, a specific form is provided on the MiVoice Border Gateway page of the MCS. Pressing the 'Provision Teleworker Phones' button will load the form. To provision extensions, move them from the left side of the form to the right. To un-provision them, do the opposite. Saving the form down will initiate provisioning with the MBG.

> Any SIP extension provisioned using this method will automatically have a random remote authentication

> username and password assigned if they do not have them set already.

For information on how to provision SIP Users manually, please refer to the Manual Teleworker Provisioning section of the MiVoice Office Application Suite Technical Manual.

> Each Teleworker connection on the MBG requires a Teleworker licence.

> In addition to configuring SIP Users for teleworker extensions, they must also be configured for any SIP Hot Desk extensions that will be logging into a teleworker phone.

13.2.5 6900 Handset Multi-Node Implementations

6900 handsets can be used in MiVoice Office 250 multi-node environments. When implementing multiple nodes, there are two options available:

- Single MiVoice Office Application Suite, recommended for multiple nodes at a single location
- Multiple MiVoice Office Application Suites, recommended for nodes at multiple locations

The correct implementation must be chosen depending on the infrastructure and customer requirements. The following section outlines each implementation.

> With either implementation, a CT Gateway is required for the MiVoice Office Application Suite(s) to connect to.

Single MiVoice Office Application Suite

Having a single MiVoice Office Application Suite installation acting as configuration server for all 6900 handsets provides the greatest level of functionality for the customer. Each handset will be provided configuration, keymaps and all other features from a single point. This implementation is recommended for when multiple MiVoice Office 250 nodes are at the same location or when there are resilient links between locations.

With this implementation there is no loss of functionality, all 6900 handset features will work as designed including SIP Hot Desking, which will allow users to hot desk onto any 6900 handset on any node.

Restrictions

This implementation relies on the MiVoice Office Application Suite being able to communicate with all nodes and all 6900 handsets all the time. If there are WAN links involved in the implementation then there is a risk of downtime if the link is down for any period of time.

If the link between sites is down, any 6900 handsets that cannot communicate with the MiVoice Office Application Suite will lose all server provided keys and features. The handset will continue to operate as a SIP phone and will be able to make and receive calls, but the following features will cease to be available until the link is restored:

- Server Based Keys (BLF Keys, DND, Presence Profiles, UCD, FWD, Account Codes etc)
- Screen Savers
- SIP Hot Desking
- Avatar images, local and for calls.
- Phone Status Messages/Icons
- Any configuration or keymap changes while the link is down.

Once the link is restored, the features listed above will work as designed.

Multiple MiVoice Office Application Suites

Having multiple MiVoice Office Application Suite servers provides the greatest level of resilience and is the recommended for implementations where nodes are installed at different locations and are connected using WAN links.

When using this implementation, keymap profiles, configuration profiles, screen savers and all other configurations must be programmed on each MiVoice Office Application Server individually.

However, with this implementation there are restrictions in functionality that must be outlined to the customer.

Restrictions

The following features will not be available when 6900 handsets are using different configuration servers:

- User BLFs
- Avatar images for users on different configuration servers
- Multi-Node SIP Hot Desking

> Paging between handsets will only work when handsets can receive Multicast transmissions. These packets are not routed and so paging will only work between handsets on the same network segment.

13.2.6 6900 Handset Feature Comparison

When using 6900 handsets in conjunction with a MiVoice Office 250, many of the features available are configured through profiles on the MCS server rather than on the telephone system. In addition, many of the features have slightly different names than those traditionally used on the MiVoice Office 250.

This section of the manual is designed to review features of the MiVoice Office 250 and provide information about what they are called and how they are configured. In addition, it highlights features of the MiVoice Office 250 that are not yet available on the 6900 handsets or have restrictions to their use.

MiVoice Office 250 Feature	Supported on 6900 Handsets	6900 Handset Equivalent
ACD Agent	Yes	ACD agents are supported on 69xx phones with softkeys for login/logout and end wrap. Auto answer is not natively supported but can be implemented using the Phone Manager 'Auto-answer hunt group calls' feature.
Account Codes - All Calls Following	Yes	N/A
Account Codes - Optional	Yes	N/A
Account Codes - Forced	No	N/A
Agent Help	Yes	N/A
Calling Party Name / Number	Yes	N/A
Class of Service	Yes	N/A
Do Not Disturb	Yes	Do Not Disturb works but not DND Override
Dynamic Extension Express	Partial	Push and Pull features do not work in relation to SIP devices.
Hot Desking	Yes	SIP Hot Desking can be used in place of Mitel Hot Desking but, they are not interchangeable. You cannot log onto a 6900 handset with a Mitel Hot Desk Phantom or visa versa.
House Phone	Yes	Auto Dial - Configured using a Configuration Profile
Keymaps	Yes	Configured using Keymap Profiles

Language	Yes	Language - Configured using a Configuration Profile
Manual Forwarding	Yes	Accessible to the user via a softkey
Message Waiting Notification	Yes	N/A
Network Time Protocol (NTP)	Yes	NTP is supported but needs configuring in the Configuration Profile used by the 6900 handset (the setting is not inherited from the PBX). In Configuration Profiles set Time Server 1 to 3
Paging	Yes	Paging from 6900 handset works as normal. Paging to 6900 handsets only works from other 6900 handsets.
Record-A-Call	No	This feature does not currently work in conjunction with SIP devices.
Silent Monitor	Partial	A SIP device can be monitored from a MiNET or Digital device but not in the reverse direction.
Supervised Transfer	Yes	Transfer to connect is supported. Transfer to Hold/Ring are not supported.
System Forwarding	Yes	N/A
UCD Hunt Groups	Yes	N/A
Voicemail / Mailbox	Yes	N/A

Where the '6900 Handset Equivalent' column is set to N/A, the feature works with standard MiVoice Office 250 configuration.

MiVoice Office 250 Configuration

When configuring the MiVoice Office 250 to support 6900 handsets, the following DB programming items should be checked.

DID/E&M Receive Busy Instead of Camp-On

If this setting is enabled, when transferring a call from a 6900 handset to an extension that is already busy, it will not be possible to complete the transfer.

Audio for Calls Camped-On/Ringing/On Hold

By default, this setting is configured to the MOH port for the system on each device created on the telephone system. To ensure that the 6900 handsets get audible feedback when ringing other extensions that are busy, ensure there is audio on the MOH port or change this setting to ringback for all devices.

OAI 3rd Party Call Control

When used on the MiVO 250, 69xx phones work in SIP mode and do not support the same feature set as their MiNET/Digital counterparts.

In addition to the unsupported features listed in the previous section, not all the available '3rd Party OAI Call Control' commands are supported in conjunction with 69xx phones.

Due to these 3rd Party OAI Call Control limitations, the following solutions for the MiVO 250 cannot be used in conjunction with 69xx phones:

- Attendant Console
- MiCC Office Client Go / Callviewer / Connection Assistant
- MiCC Office Intelligent Router / Reporter Pro / Realviewer (Call Control Commands)

> ⚠ Attendant Console and CTI Clients such as Client Go, Callviewer and Connection Assistant will not operate with 69xx phones.

Mitel Phone Manager applications will continue to operate when paired with a 69xx phone but without the 'Merge' call feature.

The following OAI Commands can still be used are unaffected by or can be used in conjunction with SIP phones on the MiVO 250:

- Clear Call/Connection (_CC / CX)
- Expanded Extension (_XE)
- Hunt Group Merge Out (_HM)
- Modify Call (_MD)
- Monitor Start/Stop (_MS / _MA / _MP)
- No Operation (_NO)
- Query Agent State (_QA)
- Query Device Information (_QI)
- Query DND (_QD)
- Query Event Filter (_QE)
- Query Forwarding (_QF)
- Query Hunt Group (_QH)
- Query List Extended (_QX)
- Query Message Waiting (_QM)
- Query Network Node Number (_QN)
- Query Night Mode (_QT)
- Query User Destination (_QUD)
- Query User Routing (_QUR)
- Set Agent State (_SA)
- Set Do-Not-Disturb (_SD)
- Set Forwarding (_SF)
- Set Message Waiting (_SM)
- Set Night Mode (_ST)
- Set User Destination/Information (_SUD / _SUI)

- Snapshot Device (_SP)
- Transfer Call One Step (_TO)

> ⚠ Commands not listed here DO NOT work with 69xx or SIP phones (e.g. Make Call (_MC), Hold Call (_HC), Retrieve Call (_RV).

13.2.7 6900 Handset Diagnostics & Troubleshooting

Diagnostics

There may be circumstance where Mitel support ask for information to diagnose faults. The service that handles 6900 handset requests will log to the normal Mitel Communication Service destinations. Logging for this service is enabled/disabled using the standard 'Logging' settings within the MCS website.

For more information, please refer to the Logging section of the Technical Manual.

In addition to the logs generated by the server, each handset can be configured to upload diagnostic information to the server.

For information on enabling this feature on a handset centrally, please refer to the 6900 Handset Phones section of the Technical Manual. Ensure that the Syslog IP address has been configured for the 6900 Handsets in the External Addresses section of the MCS website.

Troubleshooting

No Service showing on the Handset

The most likely cause of this is incorrect match of the device username and password set on the PBX and in the MCS.

This can be identified in the HandsetLifeCycle logs for the handset stored by default in %ProgramData%\Mitel\Mitel Communication Service\Logs\Handset\logs\Handsets\<MAC of handset>

You will see a line similar to below:

14:34:20.7933 : [35] RequestController : SIP Registration Regevent registration params SipUsername=14638,DisplayName=14638,SipAuthName=14638,ProxyUrl=192.168.106.1,ActiveProxy=192.168.106.1,IncomingName=Unknown Name,LocalIp=172.19.23.7,CallDuration=0,RegistrationCode=401,LineIndex=0,RegistrationState=REFUSED

The highlighted items show a 401 error indicating authorisation failure.

Ensure the SIP username and password match for the device between the PBX and MCS device configuration. Changes will be pushed to the handset and it should connect.

Remote Handset Connections

For remote handsets, ensure the following items have been checked:

- MiVoice Office 250
  - SIP extension has configured Use Registered Username and NAT address type set to Native (see 6900 Handset SIP configuration - MiVoice Office 250 section in the Online help or Technical Manual)
  - Check the Set-Side username and password matches the SIP device username and password
- MCS Server
  - Local and remote nodes are configured and the external address of the MBG is in the NAT IP Address section (see 6900 Handset SIP configuration - Node IP Addressing section in the Online help or Technical Manual)
  - Check the Set-Side username and password matches the SIP device username and password in the MCS server (see 6900 Handset SIP configuration - SIP Device Authentication section in the Online help or Technical Manual)
  - Check the ICP-side username and password match the SIP device username and password on the MiVoice Office 250

> If any changes have been made to a remote configuration while the handset has 'No Service' then the change will only take effect once you reboot the handset

Web Recovery Mode

When deploying a 6900 handset or after an environmental change you may find your 6900 handset using SIP firmware is in an unrecoverable state. This can occur if the handset fails to receive a DHCP address or it is in a constant loop and the settings of the handset or the web interface cannot be accessed.

Once the phone has rebooted and failed 10 times in a row it will put itself into 'Web Recovery Mode'.

> To manually place a handset into 'Web Recovery Mode', hold down '1' and '#' while the handset is booting up.

The handset should have an IP address which should be displayed on the screen. Navigate to the phone's web interface using the IP address provided.

Once on the website, select 'Upgrade Software' from the left-hand menu. You will need to browse to the relevant model number's '.st' file (there is a specific file for each model type) and upgrade the phone to the chosen firmware version.

The '.st' files are available from the MiVoice Application Suite server in the following location:

'C:\ProgramData\Mitel\Mitel Communication Service\Net Store\Firmware\[Version]'

Once complete, the phone will reboot and will be back to default.

> If using a Bluetooth handset or other peripherals, these will now need to be re-paired.

Manual Firmware Updates

This section outlines how to perform a manual firmware update on a 6900 handset.

> This should be used to update a 6900 Handset from MiNET to SIP Firmware at a remote location followed by configuring the Configuration Server described in the next section

Requirements:

- A TFTP server (such as TFTPD64)
- The .st firmware file for the model handset you require (These are available from the MCS server %ProgramData%\Mitel\Mitel Communication Service\Net Store\Firmware)
- IP address of the 6900 Handset (use settings and status on handset to find this)
- IP address of the TFTP server

Steps:

1. Place .st firmware file in the TFTP server directory (ensure that no MiNET files are present.
2. Press the gear button to go into setting on the 6900 phone.
3. Select 'Advanced' settings (default password is 73738)
4. Select 'Network' then 'Static' settings.
5. Enter the IP address of the TFTP server then press 'Save' (ensure your IP phone has an IP address assigned)
6. Select 'Restart' from the base settings screen on the phone.
7. The IP phone will attempt to download MiNET firmware on boot up. When not found, it will subsequently download the SIP firmware.

Remote Phone Configuration for SIP Firmware

If you have just updated the firmware on a remote 6900 Handset from MiNET to SIP then complete the following steps to enable the phone to connect to the MCS server

- Add the configuration server details on the phone manually, press the settings button ( ) on the handset, then press the 'Advanced' key along the bottom of the screen.
- At this point you will be prompted to enter the administrator password. The default SIP password is '22222'.
- Once the password has been accepted, use the navigation keys (D-pad) or touch screen on 6940 to navigate to the 'Configuration Server' section.
- Populate the following entries:

  Download Protocol: HTTPS
  HTTPS Server: [external IP Address or external DNS name of the MCS server]
  HTTPS Port: 8202
  Cert Validation: false
- Press 'Save' and then reboot the handset.

After a reboot, the phone will connect to the MCS server. The MCS server will provide over HTTPS connection information and will then tell the phone to reboot.

> It is possible that there will be more than one reboot at this stage as the firmware update is completed

The handset should now be registered with the MCS server.

The Phone will have Line 1 and Line 2 showing as the Top Sofkeys.

Unlike for local deployment as 'Setup' button will not be available and the SIP extension needs to be configured in the MCS server.

The 'Phones' page within the configuration section of the MCS website can be used to view whether the handset has been identified. The MCS uses the handsets MAC Address to uniquely identify it.

Restoring MiNET Firmware

If required, the firmware on the handset can be restored to a MiNET version.

Requirements:

- A TFTP server (such as TFTPD64)
- The MiNET firmware file for the model handset you require

- IP address of the 6900 Handset (use settings and status on handset to find this)
- IP address of the TFTP server

Steps:

1. Place the MiNET firmware file in the TFTP server directory
2. Start the TFTP server
3. Using a web browser, connect to the web page of the phone using the IP address of the phone (Default Username - 'root', Default Password - '73738' on MiNET firmware and Default Username - 'admin', Default Password '22222' on SIP firmware)
4. Select 'Reset' then select 'Restore To Factory Defaults'. At this point the phone will reboot. When it has completed it's reboot, repeat step 3 to log back into the website.
5. Select 'Firmware Update', complete the form:

- Enter the name of the firmware file in the filename box
- Enter the IP address of the TFTP server in the Server box
- Select Download firmware
- Firmware will download and then the phone reboot (note this can take several minutes)

> ⚠ It is important to factory default the phone before restoring to MiNET firmware to avoid complications.

13.3 Phone Manager Softphone

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

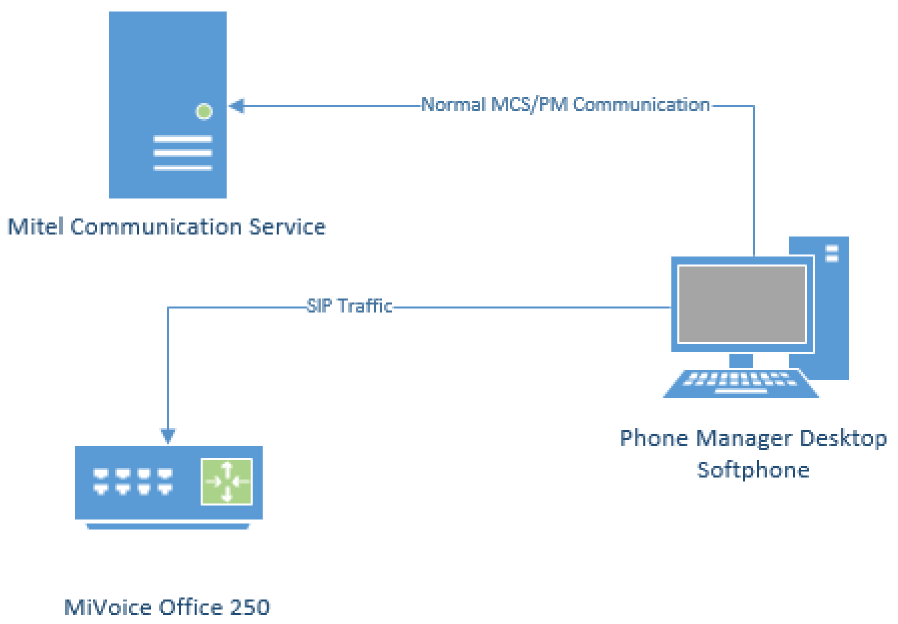
Requirements

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

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

Phone Manager Desktop with Softphone

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



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

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

Connecting from a Different Subnet

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

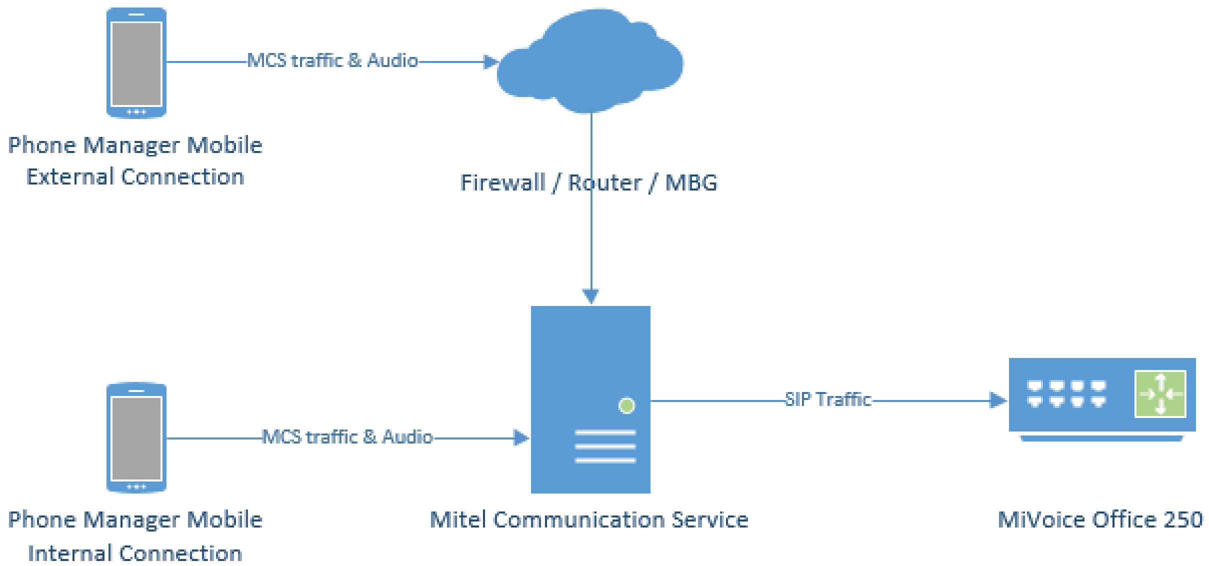
To work around this issue, Auto NAT Detection needs to be disabled on Phone Manager Desktop.

Phone Manager Mobile with Softphone

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

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

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



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

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

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

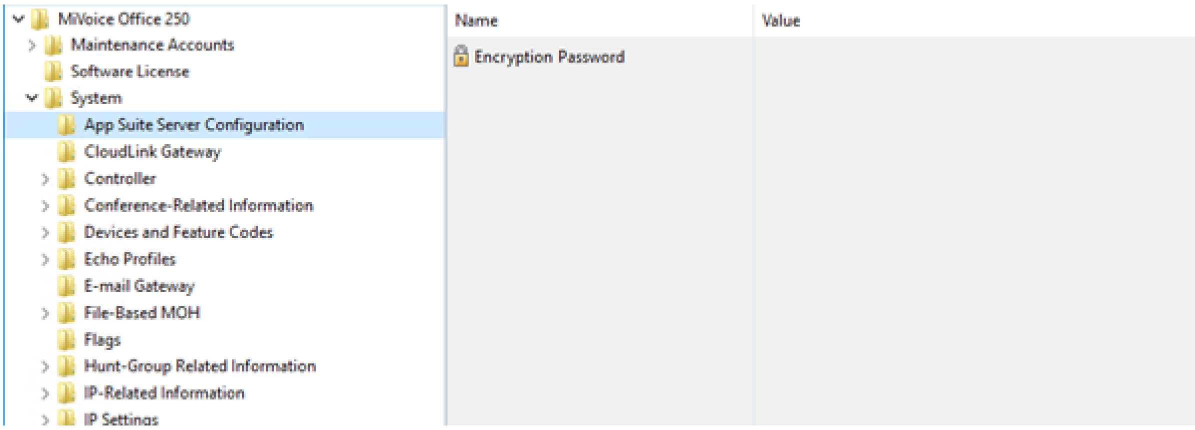
> ⚠ The SIP Proxy service must be on the same network as the PBX with no NAT in between the two.

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

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

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

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



Encryption Password

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

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

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

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

Node Configuration for SIP

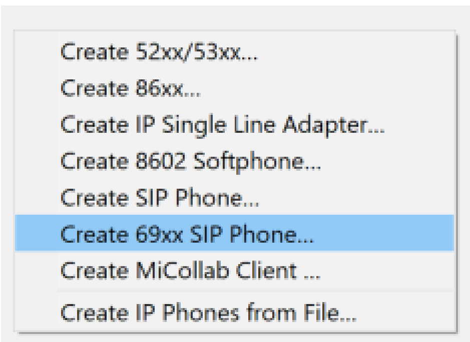
The MCS server needs to provide each 6900 phone and Phone Manager Softphone with the IP address of a SIP server to register with (the MiVoice Office 250). The IP address required will depend on which MiVoice Office 250 node the SIP extension is configured on and whether the phone is local or a teleworker.

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

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

69xx SIP Phone

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

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

SIP Phone Group

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

- Maximum Number of Calls = 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.

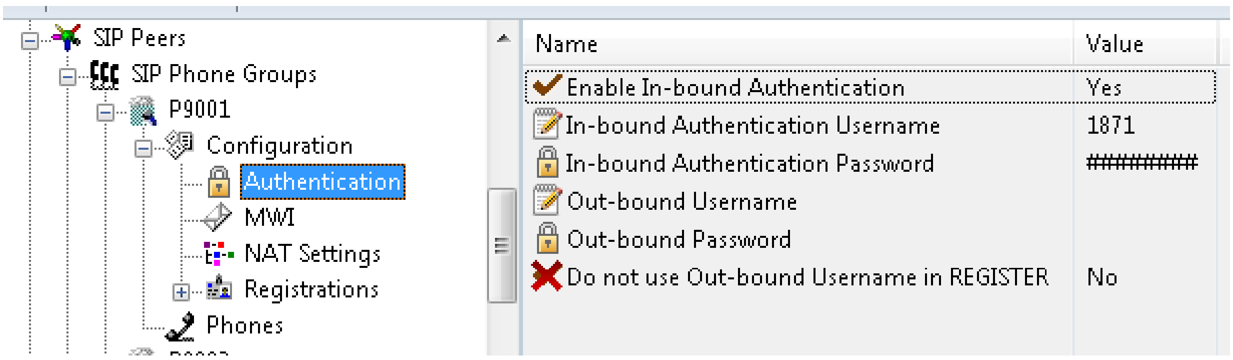
Manual Authentication Configuration

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

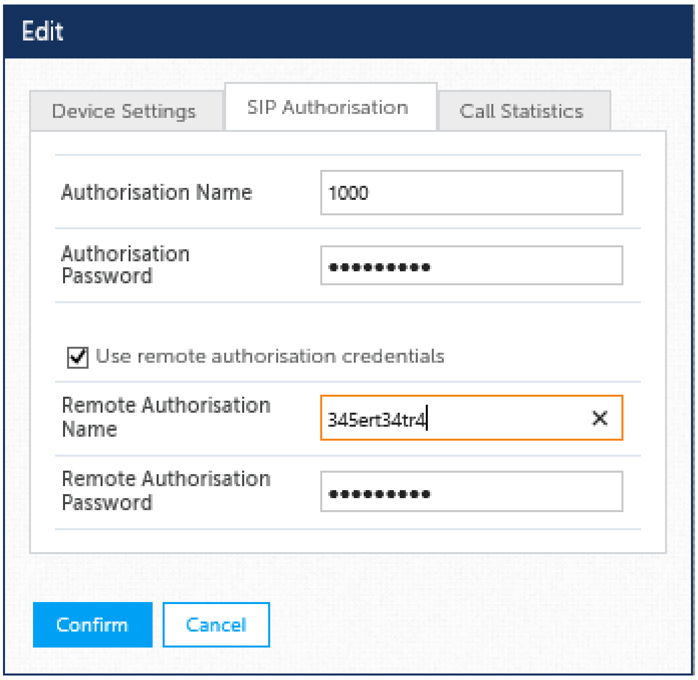
If release 6.3 SP1 or higher is being used, check the App Suite Server Configuration section below.

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

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



This same username and password combination would then need to be set on the device configuration on the Communication Service for this extension.



For information on configuring Teleworker phones, please refer to the Remote Connections engineering guidelines.

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

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

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

Call Configuration

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

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

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

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

It is important to connect only one softphone to each extension number on the telephone systems. Registering more 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.

13.4 Upgrades, Backups, Restoring & Rollback Procedures

The MCS system has various persistent data stores which should be backed up on a regular basis to minimise 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, MiVoice Office Phone Manager Outbound 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.
- 6900 Handset files -> Firmware files, background 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 MiVoice Office Phone Manager Outbound 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 & 6900 Handset Files

MCS stores some data outside the database so as not negatively impact database performance. Currently this is limited to:

- Profile images users upload from Phone Manager Desktop and Phone Manager Mobile clients.
- Firmware files uploaded for 6900 Handsets
- Background images uploaded for 6900 Handsets

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

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

13.4.1 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.

SQL Management Studio

The processes below refer to the 'SQL Management Studio' application. This is no longer included with MiVoice Office Application Suite installations but can be downloaded and installed manually using the following link:

https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms

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.

13.4.2 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.

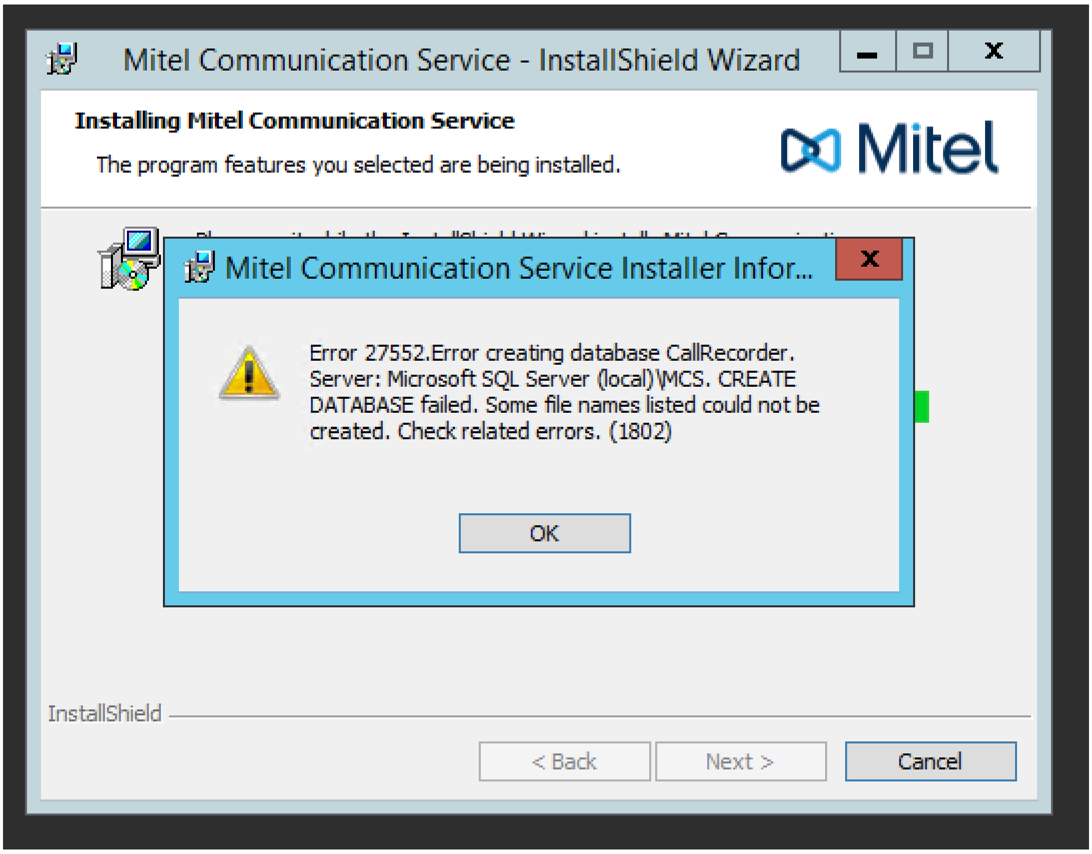
> ⚠ The system will go offline during the upgrade process, no data or call audio will be recorded during this time. It is advised that this process is completed outside of normal operating hours for the system.

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 click 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.

14 Index

Powering connections

mitel.com