MiContact Center Office

FEBRUARY 2017

TECHNICIAN'S HANDBOOK

Release 6.2 SP1

Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

MiContact Center Office Technician's Handbook
Release 6.2 SP1 – January 2017

Contents

Chapter 1

NEW FEATURES

WHAT’S NEW IN RELEASE 6.2 SP1

Support for Hyper-V

MiCC Office 6.2 SP1 introduces support for Hyper-V for deploying and installing MiCC Office on Hyper-V virtual machines. Supported hypervisors are Microsoft Hyper-V 2012 R2
Supported Guest OS are any of the supported Windows Operating systems for running MiContact Centre Office 6.2 SP1 Server (see below)

Windows support

MICC OFFICE 6.2 SP1 NOW SUPPORTS WINDOWS 10
The following are the supported Operating systems for MiCC Office 6.2 SP1:

MiCC Office Server:

- Windows 10 Standard/Professional/Enterprise (64-bit)
- Windows 8.1 Standard/Professional/Enterprise (64-bit)
- Windows 7 Professional/Ultimate SP1 (64-bit)
- Windows Server 2012 R2 Standard, Essentials & Datacenter Editions (64-bit)

MiCC Office client:

- Windows 10 Standard/Professional/Enterprise (32-bit and 64-bit)
- Windows 8.1 Standard/Professional/Enterprise (32-bit and 64-bit)
- Windows 7 Professional/Ultimate SP1 (32-bit and 64-bit)
- Windows Server 2012 R2 Standard, Essentials & Datacenter Editions (64-bit)

Updated DB2 Version

DB2 version 11.1 is installed with MiCC Office version 6.2 SP1. When upgrading MiCC Office, the setup kits automatically upgrade DB2 and the MiCC Office database.

WHAT’S NEW IN RELEASE 6.2

Updated Branding & User Interface

This release of MiContact Center Office sees the product branding change from Customer Service Manager. MiCC Office is the new abbreviation for CSM. Also included in the product is an updated user interface that implements the following concepts:

- Updates to support the latest Windows common controls (buttons, tabs etc.)
- Updates to the default color palette used by the client applications
- Updated icons and graphics to bring the product in line with Mitel Branding

Windows Support

MiCC Office Server:

- Windows 8.1 Standard/Professional/Enterprise (64-bit)

- Windows 8 Standard/Professional/Enterprise (64-bit)
- Windows 7 Professional/Ultimate SP1 (64-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012 R2 Standard, Essentials & Datacenter Editions (64-bit)

MiCC Office client:

- Windows 8.1 Standard/Professional/Enterprise (32-bit and 64-bit)
- Windows 8 Professional (32-bit and 64-bit)
- Windows 8 Standard/Enterprise (32-bit)
- Windows 7 Professional/Ultimate SP1 (32-bit and 64-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012 R2 Standard, Essentials & Datacenter Editions (64-bit)

SMTP Support

SMTP emailing support has been added to Intelligent Router rules and the Auto Reporter features of Reporter. This allows emails to be sent without having to have a MAPI enabled email client running. MAPI support is still available.

SMTP SSL/TLS Support

SSL\TLS support has been added to all areas where SMTP is used; Media Blending, Intelligent Router rules & Auto Reporter. If your mail server supports the SSL\TLS feature, then it can be enabled for use with MiCC Office.

Media Blending Add-in Update

The MiCC Office Callviewer add-in for Microsoft Outlook has been updated to support the latest versions of Outlook (Outlook 2013, 2016 32 bit only).

Backup Utility

A new service based backup utility has been introduced to the MiCC Office Server to automate the process of keeping multiple backups of the solution to help minimize the risk of data loss from hardware or software failure. This new backup utility can store backups on the local server or a network drive.

ACD on SIP

ACD features are now supported on SIP Extensions but only when running MiVoice Office 6.1 SP1 PR1 or higher.

WHAT’S NEW IN RELEASE 6.1 SP1

VSPHERE 5.5 SUPPORT

MiCC Office 6.1 SP1 introduces support for VMware vSphere 5.5 for deploying Virtual MiCC Office appliances and installing MiCC Office on virtual machines. For information about deploying Virtual MiCC Office, see the Virtual Appliance Deployment guide on the Mitel eDocs Web site (www.edocs.mitel.com).

WINDOWS SUPPORT

MiCC Office 6.1 SP1 Now Supports Windows 8.1. Here is a summary of all supported versions of Windows on MiCC

Office Server:

- Windows 8.1 Standard/Professional/Enterprise (64-bit)
- Windows 8 Standard/Professional/Enterprise (64-bit)
- Windows 7 Professional/Ultimate SP1 (64-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2012 R2 Datacenter Edition (64-bit)
- Windows Server 2012 R2 Essentials Edition (64-bit)
- Windows Server 2012 R2 Standard Edition (64-bit)

MiCC Office Client Applications are supported on these versions of Windows:

- Windows 8.1 Standard/Professional/Enterprise (32-bit and 64-bit)
- Windows 8 Professional (32-bit and 64-bit)
- Windows 8 Standard/Enterprise (32-bit)
- Windows 7 Professional/Ultimate SP1 (32-bit and 64-bit)
- Windows Server 2008 R2 SP1 (32-bit and 64-bit)
- Windows Server 2012 R2 (32-bit and 64-bit)
- Windows Server 2012 R2 Datacenter Edition (32-bit and 64-bit)
- Windows Server 2012 R2 Essentials Edition (32-bit and 64-bit)
- Windows Server 2012 R2 Standard Edition (32-bit and 64-bit)

UPDATED DB2 VERSION

DB2 version 10.5.0.4 is installed with MiCC Office version 6.1 SP1. When upgrading MiCC Office, the setup kits automatically upgrade DB2 and the MiCC Office database.

AUSTRALIA SUPPORT

Australian English is now supported in MiCC Office interfaces and selectable during the MiCC Office client applications installation.

MIGRATION OF MiCC Office INSTALLER FROM WISE SCRIPTS TO INSTALL SHIELD

Because Windows 8.0 (and later) does not support Wise scripts, the install/upgrade/uninstall processes must be executed using other technologies. Install Shield creates installers that are supported by all Windows versions.

WHAT'S NEW IN RELEASE 6.1

WINDOWS 8 SUPPORT

MiCC Office server and client applications now support the 32-bit and 64-bit versions of Windows 8. The standalone MiCC Office Server and MiCC Office server applications are supported on these versions of Windows:

- Microsoft Windows 8 Pro
- Windows 8 Enterprise.

MiCC Office client applications are supported on these versions of Windows:

- Windows 8
- Windows 8 Pro
- Windows 8 Enterprise

UPDATED VERSIONS OF RTG APPLICATIONS

The following updated versions of Ready-to-Go (RTG) applications are now supported in MiCC Office version 6.1:

ACT!

MiCC Office version 6.1 supports ACT! versions 12,13, and 14. MiCC Office version 6.1 no longer supports ACT! version 8.

GOLDMINE

MiCC Office version 6.1 supports Frontrange Solutions GoldMine versions 8.0, 8.5 and 9. Searching for a contact based on a telephone number is also enhanced. You can now search or a contact using either the first phone field (primary number) or all phone fields for a contact.

When upgrading to MiCC Office 6.1, all current GoldMine buttons and rules continue to work in the same way as they did in previous versions of the MiCC Office. For example, the phone search will be based on the first (primary) phone number. To be able to search a contact using all phone fields, you must modify or create new buttons and/or rules.

MAXIMIZER

MiCC Office version 6.1 supports Maximizer versions 10.5, 11, and 12.

MICROSOFT OUTLOOK

MiCC Office version 6.1 supports Microsoft Outlook versions 2003, 2007, and 2010.

MICROSOFT EXCEL

MiCC Office version 6.1 supports Microsoft Excel versions 2003, 2007, and 2010.

VIRTUAL MICC OFFICE SUPPORT

Due to an end of life announcement by Microsoft of the Windows 7 Professional (x64) Operating System Retail Version that was previously packaged with the Virtual MiCC Office appliance, a new OEM version of the Windows 7 Professional (x64) OS will be used instead. The key difference is that this new OEM operating system is nontransferable.

For example:

In a load balancing environment, the MiCC Office Server app would have to be pinned to its original hardware

- In the event of a hardware upgrade such as a mother board swap, the license covers only a swap to an equivalent type mother board.
- In these instances the customer will be required to provide a Windows OS license for the MiCC Office server which cannot be purchased from Mitel.

This is an interim solution as a result of Microsoft's end of life announcement. MiCC Office 6.1sp1 release due out in the fall of 2014 we are expecting to rebuild the MiCC Office virtual appliance with Windows operating system v8.1.

Note: This only affects new deployments or installations of the MiCC Office virtual appliance as of March 15, 2014.

UPDATED SMB PROFILES

SMB profiles have been updated and VMware View 5.0 VD is now supported:

When deploying virtual MICC OFFICE, you can choose between different SMB profiles based on call volumes. The profiles available for a MICC OFFICE virtual machine are Small Business, Mid-Enterprise or Enterprise. The naming of the Virtual MICC OFFICE profiles aligns with the naming of other Mitel virtual solutions. Configuration of Virtual MICC OFFICE is based on anticipated call volume.

Call Volume (daily)	**MICC OFFICE Server**	**MICC OFFICE Server, Auto Reporter**	**MICC OFFICE Server, Auto Reporter, Intelligent Router**	**MICC OFFICE Server, Auto Reporter, Intelligent Router, Media Blending**
< 1000	Small Business	Small Business	Mid-Enterprise	Mid-Enterprise
1000 - 5000	Small Business	Small Business	Mid-Enterprise	Mid-Enterprise
5000 - 10000	Small Business	Mid-Enterprise	Mid-Enterprise	Mid-Enterprise
10000 - 25000	Mid-Enterprise	Mid-Enterprise	Mid-Enterprise	Enterprise
25000 - 100000	Mid-Enterprise	Mid-Enterprise	Enterprise	Enterprise

VMWARE 5.0 VIRTUAL STORAGE APPLIANCE

MiCC Office 6.1 supports VMware 5.0 Storage Appliance.
Mitel virtual applications, including MiCC Office, are supported on View virtual desktops running Windows 7.

VMWARE VIEW 5.0 VDI SUPPORT

MiCC Office version 6.1 supports VMware View 5.0 VDI but does not provide VMware View integrated applications. MiCC Office applications are presentation only applications.

vMiCC Office is not available for Windows 8. Mitel virtual applications, including MiCC Office, are supported on View virtual desktops running Windows 7 only.

UPDATED DB2 VERSION

Version 10.1 of DB2 is installed with MiCC Office version 6.1. When upgrading MiCC Office, the setup kits automatically upgrade DB2 and the MiCC Office database.

This new version of DB2 removes the DB2 Control Center application graphical user interface that was available for use with MiCC Office data.

Chapter 2

OVERVIEW

INTRODUCTION

Mitel® MiContact Center Office (MiCC Office) is a Computer Telephony Integration (CTI) application that links the telephone system and the computer, providing a seamless and automated technological partnership.

MiCC Office is ideal for businesses, such as an order entry center, help desk (customer support), telemarketing firm, etc., that experience high call volumes and use a computerized database and/or an automatic call distribution system, although it is also suited to low-volume environments.

MiCC Office is available as a standalone application, and as a virtual appliance, Virtual MiCC Office.

MiCC Office is also supported within a thin client environment such as Microsoft Terminal Services. See “Micc Office In A Thin Client Environment” on page 19 for additional detailed information.

SYSTEM DESCRIPTION

This section describes the MiCC Office product components.

HARDWARE PLATFORM AND OPERATING SYSTEM

MiCC Office requires a Mitel approved hardware platform. The hardware platform must meet certain requirements to run the following operating system and virtualization software.

STANDALONE MiCC Office

MiCC Office Server and DB2 databases are installed directly on the Windows operating system (that is running a physical server). See Installing Micc Office on page 88 for details.

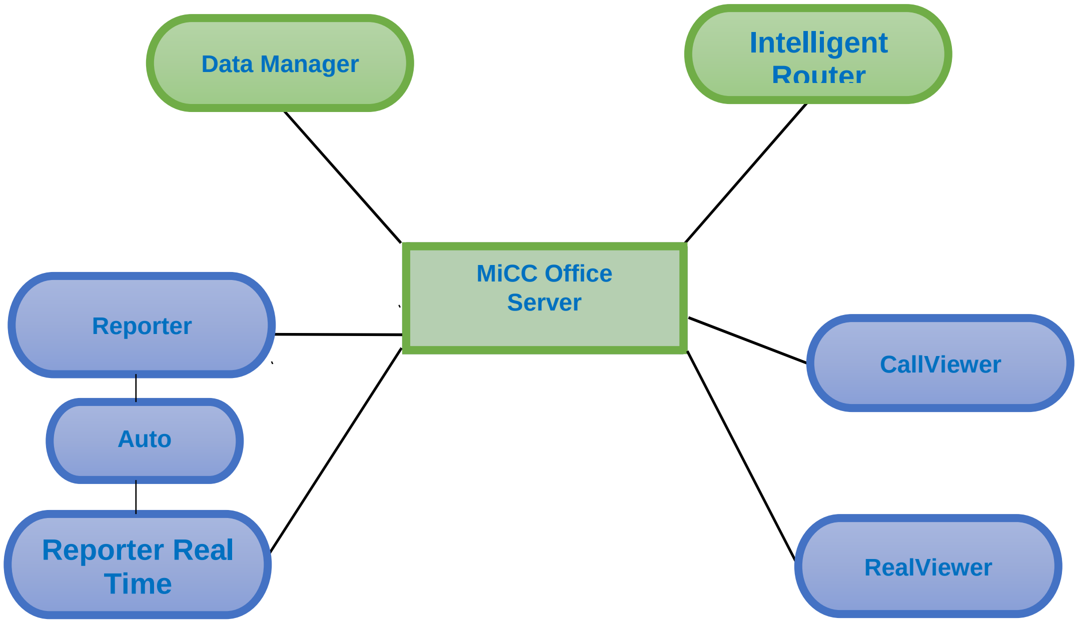
VIRTUAL MiCC Office

The MiCC Office Virtual Appliance can be deployed alongside other Mitel virtual appliances on an ESX/ESXi host within the vSphere environment or in a Hyper-V environment. MiCC Office and the databases are installed in the same Windows virtual machine as the MiCC Office server applications. See the Virtual Appliance Deployment guide for details.

SOFTWARE

MiCC Office software includes server-side and client-side applications. Figure 1 provides an illustration of the various MiCC Office software components.

Figure 1: MiContact Center Office Software Components



SERVER APPLICATIONS

The following applications are installed on the MiCC Office hardware platform, shown in green in Figure 1 above:

- **MiCC Office Server**: The MiCC Office Server is the heart of the system. Server stores all calls and provides real-time information for the other components of the system. The following components provide management and configuration functions for MiCC Office Server:
  - *Server Monitor*: The MiCC Office Server Monitor application displays the real-time status of all the network connections to remote applications, concurrent licensing information, and the status of the telephone system communication. The interface is updated every five seconds.
  - *Control Panel*: The applet provides a dialog box with tabs to control basic MiCC Office Server functions. The tab settings allow you to start and stop the server, change passwords, access log files, configure server settings, and verify license status.
- **Data Manager**: Data Manager connects over the network to the Server and allows you to configure the telephone system connection and other critical settings.
- **Intelligent Router**: Allows you to program routing schemes (and numerous other actions) for calls and other media types based on call information and other statistics. Intelligent Router is required for the optional media blending feature (see "Media Blending" on page 11).

CLIENT APPLICATIONS

The following client applications communicate with the server applications over the internal network and are installed on users' Windows-based computers:

- **CallViewer**: Allows individual users to screen pop information from the company database and manage calls and e-mail messages. CallViewer includes several "look and feel" choices to help you customize the application to suit your need
- **RealViewer**: Allows users to see statistics, at their own computer, based on the activity of the user or their group.

- **Reporter**: Allows users to analyze the call log historically in a variety of ways to make better business decisions. Licensing variations include Reporter Basic, Reporter, and Reporter Pro.
- **Reporter Real-Time**: Allows users to analyze real-time call logs in a variety of ways to make better business decisions. Licensing variations include Reporter Real-Time and Re- porter Real-Time Pro.
- **Auto Reporter**: Provides publishing capabilities for Reporter and Reporter Real-Time. Also allows users to schedule report exports.

The following third-party applications are supported in MiCC Office client applications:

Microsoft Outlook

MiCC Office version 6.2 supports Microsoft Outlook versions 2010, 2013 and 2016 (32bit only).

Microsoft Excel

MiCC Office version 6.2 supports Microsoft Excel versions 2010, 2013, and 2016.

MEDIA BLENDING

As more customers use the Internet for sales, support, and service, call centers are handling more e-mail messages, faxes, and other forms of contact, in addition to phone calls. In turn, call centers must make the migration to become contact centers, and be prepared to deal with a variety of media.

To accomplish this, Intelligent Router provides Media Blending functionality that enables it to route calls, e-mail messages and other media to available agents, so that customers get the most efficient and effective response available, while maximizing agent productivity.

Some important points about Media Blending are:

- All e-mail messages routed by Intelligent Router must go through a Media Blending queue. Refer to the Intelligent Router online Help for setting up the agent's e-mail address and for details on setting up the Media Blending queue.
- Only e-mail messages that are routed through a Media Blending queue are reported on through the use of MiContact Center Office. Refer to Chapter 4 for details about how e-mail messages are handled.
- E-mail messages from Media Blending agents are considered "internal." This is based upon whether the e-mail address is mapped to an agent or not. All other e-mail messages are considered "external."

Rules configured in Intelligent Router define how to route the e-mail messages to available Media Blending agents, or deal with the e-mail messages in an alternative fashion.

For additional information on Media Blending refer to the Intelligent Router online Help.

CALL RECORDING SERVER INTEGRATION

MiContact Center Office supports integration of Call Recording Equipment (CRE). When the call recording Server is installed and configured, specific devices (trunks or stations) are "mapped" to a voice recording channel. When a call is connected to a mapped device, the call is recorded and stored as a **`.wav`** file. After recording, users can retrieve the recording using the Reporter application. Calls made to unmapped devices are not recorded.

If you are interested in integrating a call recording server with your MiCC Office installation, contact Mitel Corporate Sales Engineering for a list of approved CRE vendors.

READY TO GO SOLUTIONS

Ready-to-Go (RTG) solutions are a collection of macro scripts included with the CallViewer installation. Ready to Go solutions provide quick access to frequently-used features by creating actions, rules, and buttons that integrate with third-party products. All of the Ready to Go solutions are automatically copied to the user's computer, so the user can configure the solution when they need it.

Each Ready to Go action consists of a macro script and several parameters that allow the user to configure the action through dialog boxes. Although users can modify the parameters within the action, they cannot alter the Ready to Go script.

CallViewer includes the following embedded RTG macros:

- URL: Dials a number on a Web page.
- Auto Dial: Dials the number in an e-mail message subject line.
- Internal Directory: Displays a list of internal phone numbers from the communications platform.

In addition, CallViewer supports the following third-party applications for integration with Ready to Go solutions:

- Sage® Software ACT!® v12, 13, 14
- Maximizer™ Software v10.5, 11,12
- FrontRange Solutions® Goldmine® v8, 8.5, 9
- Microsoft Outlook® 2010, 2013, 2016

The following RTGs are supported on computers running Windows 7, 8 and 10:

- URL
- Auto Dial
- Internal Directory
- Maximizer v10 with the latest Service Pack release
- Microsoft Outlook 2010, 2013, 2016

SUPPORTED COMMUNICATION PLATFORMS

MiCC Office is supported on the following Mitel communication platforms:

- Mitel MiVoice Office 250 v6.x or later

LICENSING

MiCC Office synchronizes directly with the Applications Management Center (AMC) and uses Mitel software libraries to validate the licenses.

The "Sync" feature in the License Status Tab of the MiCC Office Server application does not force synchronization of the MiCC Office license with the AMC. If the MiCC Office has a current license, synching re-validates the license. This behavior prevents validation failures if there are network problems or if a site manually synchronizes their licenses. If MiCC Office cannot find a valid license or if the license has expired, it attempts to perform a sync operation. If the license validation fails for any reason, the MiCC Office enters the license grace period.

Table 2 describes the MiCC OFFICE licensing principles.

Table 2: MiCC Office Licensing Principles

NAME	MICC OFFICE LICENSE KEY FILE Name	LICENSE
Auto Reporter	AutoReporter	Toggle
Intelligent Router	IntelligentRouter	Toggle
Call Recording	CallRecording	Toggle
Client Go	ClientGo	Tally
Connection Assistant	ConnectionAssistant	Tally
CallViewer	CallViewer	Tally
Reporter Basic	ReporterBasic	Tally
Reporter	Reporter	Tally
Reporter Pro	ReporterPro	Tally
Reporter Real-Time	ReporterRealTime	Tally
Reporter Real-Time Pro	ReporterRealTimePro	Tally
RealViewer	RealViewer	Tally
Agent Reporting License	Agent	Tally
Media Blending Agent	Media Blending Agent	Tally
Media Blending Queue	Media Blending Queue	Tally
Node	Node	Tally

Table 3 describes the vMiCC Office licensing principles.

Table 3: vMiCC OFFICE Licensing Principles

NAME	MICC OFFICE LICENSE KEY FILE Name	LICENSE
Auto Reporter	AutoReporter	Toggle
Intelligent Router (Advanced Routing option)	IntelligentRouter	Toggle
Connection Assistant	ConnectionAssistant	Tally
CallViewer (Advanced Routing option)	CallViewer	Tally
Reporter Pro	ReporterPro	Tally
RealViewer	RealViewer	Tally
Media Blending Agent (Media Blending option)	Media Blending Agent	Tally
Media Blending Queue (Media Blending option)	Media Blending Queue	Tally
Node	Node	Tally

MICC OFFICE MIGRATION LICENSING

A valid MiCC Office license is required to install and migrate Standalone or Virtual MiCC Office. You can obtain a standalone or virtual MiCC Office license by ordering a MAS MiCC Office migration part number. The following sections describe the various deployment scenarios and the part numbers for standalone and virtual MiCC Office migrations. It also includes part numbers to migrate from standalone to virtual when the customer is already on V6 or above.

Standalone CSM\MBD to vCSM\MBD

From version 6.2 onwards a valid license allows standalone or virtual installation

Migration Part Numbers

Note: where the Upgrade part numbers description mentions standalone only, this now will provide for installation in standalone or virtual environment

Starting Position	Upgrade Part Number	Required Steps
CSM starter kit (52002312)	54005730	When the migration part numbers are applied to the CSM starter kit ARID the SRID is converted to either a CSM 6.x s/w only ARID. The Migration part number includes the CSM 6.x base kit entitlement which replaces the original MAS CSM starter kit entitlement, other CSM licenses will remain on the ARID.
MBD Starter Kit (52002311)	54005732	When the migration part numbers are applied to the MBD starter kit ARID the ARID is converted to either a MBD 6.x s/w only ARID. The Migration part number includes the MBD 6.x base kit entitlement which replaces the original MAS MBD starter kit entitlement, other MBD licenses will remain on the ARID.
CSM add-on to MAS (52002314)	54005734	Obtain new server or virtual PC for CSM. Perform CSM backup. Apply migration part that entitles you to a new CSM base pack starter kit with new ARID, move any further licenses from the MAS ARID to the new CSM ARID install CSM, Restore CSM. Once migration is complete apply MAS CSM removal part to the original MAS ARID.
MBD add-on to MAS (52002313)	54005736	Obtain new server or virtual PC for MBD. Perform MBD backup. Apply migration part that entitles you to a new MBD base pack starter kit with new ARID, move any further licenses from the MAS ARID to the new MBD ARID install MBD, Restore MBD. Once migration is complete apply MAS MBD removal part to the original MAS ARID.
MAS add-on to CSM (54005443)	54005734	Obtain new server or virtual PC for CSM. Perform CSM backup. Apply migration part that entitles you to a new CSM base pack starter kit with new ARID, move any further licenses from the MAS ARID to the new CSM ARID install CSM, Restore CSM. Once migration is complete apply MAS CSM removal part to the original MAS ARID.

MAS add-on to MBD (54005443)	54005736	Obtain new server or virtual PC for MBD. Perform MBD backup. Apply migration part that entitles you to a new MBD base pack starter kit with new ARID, move any further licenses from the MAS ARID to the new MBD ARID install MBD, Restore MBD. Once migration is complete apply MAS MBD removal part to the original MAS ARID.
MAS Demo Kit with CSM (52002501 or 52002725)	54005743	Obtain new server or virtual PC for CSM. Perform CSM backup. Apply migration part that entitles you to a new CSM base pack starter kit with new ARID, move any further licenses from the MAS ARID to the new CSM ARID install CSM, Restore CSM. Once migration is complete apply MAS CSM removal part to the original MAS ARID.

CALLVIEWER LICENSE FUNCTIONALITY

Table 4 provides the required settings to enable CallViewer licensed features.

Table 4: CallViewer License Functionality

FEATURES	LICENSE SETTING	
	CONNECTION ASSISTANT	CALLVIEWER
Call Control	All, except for Set DND State	All
DSS	Yes	Yes
Call Log	Yes	Yes
Create User Buttons	Yes	Yes
Edit Feature Buttons	Yes	Yes
Create Ready-to-Go Actions	Yes	Yes
Create User-Defined Actions	No	Yes
Run Ready-to-Go Actions	Yes	Yes
Run User-Defined Actions	No	Yes
Maximum Ready-to-Go /User-Defined Actions	20	250
Maximum User Buttons	15	250
Maximum User-Defined Features	50	250
Maximum Rules	10	250
Maximum Hot Keys	50	Infinite
Maximum DSS Monitors	50	250
Maximum Call Log Items	1000	5000
DDE/Active X Support	Yes	Yes

AGENT REPORTING LICENSE

The Agent Reporting license allows the system to concurrently license the reporting of ACD agent IDs within MiCC Office. For example, if there are five agents licensed for a system and they are all logged in, the sixth agent that logs in is modeled as “Unlicensed”.

When an agent ID is in the “Unlicensed” state, ACD Agent Status Log database records are not generated for those “Unlicensed” devices/agents. The ACD login information for “Unlicensed” agents is not propagated by the server-side to any of the real-time client products (for example, Reporter, CallViewer, etc.). Instead, a single update is sent notifying them that the device and agent is in an “Unlicensed” status, which is displayed in each application accordingly.

Call modeling/agent statistics are not collected for “Unlicensed” agents. Any agents that attempt to log in over the maximum number of agents licensed on the AMC are designated as “Unlicensed.” These agents remain unlicensed until additional licenses become available as specified by the number of licenses purchased. No statistical data is gathered for “Unlicensed” agents.

Note: Agents that log in when there are no agent licenses available, are required to log out and log in again when a license becomes available, before they are able to collect statistics.

MICC OFFICE IN A THIN CLIENT ENVIRONMENT

MiCC Office release 5.1 and above supports deployments within a thin client environment such as Microsoft Remote Desktop Services (previously known as Terminal Services). Microsoft has carried out lab tests with regards to the specification of a Remote Desktop Session (RDS) Host (formerly known as Terminal Sever) for use in a thin client environment. It is recommended that these results be reviewed before implementing MiCC Office.

More information on the lab tests and Terminal Server is available at the Microsoft Remote Desktop Services Homepage (http://www.microsoft.com/en-us/server-cloud/windows-server/remote-desktop-services.aspx).

Note: For Microsoft Windows 2008 Server R2 onwards, Terminal Server has been renamed Remote Desktop Session Host, and Terminal Services has been renamed Remote Desktop Services.

Note: Microsoft Windows Server 2008 R2 installed with Remote Desktop Services is built on the same architecture as Citrix® Server.

To install MiCC Office properly within such a thin client environment it is necessary to first develop a specification for the RDS Host and how the MiCC Office applications should be installed. The information described below is for guidance only.

TYPES OF USERS - MEMORY AND PROCESSOR USAGE

To begin developing the specification, it is necessary to establish the type of users that will be using the Remote Desktop Services environment. Microsoft has identified the following two types of users:

- **Data Entry Workers**: These workers input data into computer systems - example: transcription, typing, order entry, clerical work, and manufacturing.
- **Knowledge Workers**: These workers are defined as those who gather, add value to, and communicate information in a decision support process.

Once the use types have been established, memory and processor usage needs to be determined. This is dependent on which MiCC Office application is being used and to what extent. The table below provides a guide to memory and processor usage for MiCC Office applications.

Table 5: MiCC OFFICE Memory and Processor Usage

MICC OFFICE APPLICATION	MEMORY USAGE	PROCESSOR USAGE
Call Viewer/Connection Assistant	Low	Low
Real Viewer	Low	Low
Reporter (Basic, Pro)	Low/Medium1	Low/High2
Reporter Real Time	Medium/High3	Medium4
Intelligent Router	Low	High5
Auto Reporter	Low	Low/Medium

Notes:

1. Memory usage by Reporter varies, depending on the type of report being run. Reports based on call listings are less memory-intensive than those that are based on extensions and agents.
2. Most of the time, processor usage by Reporter is of a low level. However, when a report is being processed, the application will try to use as much of the processor as it can. Therefore, the user should expect periods where there will be bursts of high activity.
3. Reporter Real-Time is constantly monitoring activity and therefore memory usage is generally high. These levels do vary depending on how intensely the application is being used. A user running the application in a small Contact Center using four deskboard tiles and one extension list will not use as much memory as another who works in a large Contact Center with hundreds of extensions who may be running 50 deskboard tiles and a number of extension lists.
4. Processor use by Reporter Real-Time is of a medium level. However as in No. 3 these levels vary, depending on how the application is being used.
5. Memory usage by Intelligent Router depends on how the application is being used. If media blending is active, the processor usage will be higher.
6. Processor usage by Auto Reporter is dependent on how the application is being used. If the application has lots of schedules, processor usage will be medium.

Low memory use would be the equivalent with the Data Entry Worker, high memory use with the Knowledge Worker, and medium memory use would be in-between these two.

RDS Hosts can run on one to a number of processors. The more processing power available, the greater the number of users that will be able to connect to the server.

After having established the type of users, allowances must be made for any other applications that will be installed on the server, and also any other back-end services that might be running (e. g., Domain Authentication, Exchange Server, Printing Services, etc.). Both the type of users and the type of applications/services running will affect the amount of memory needed and size and number of processors required.

INSTALLING MICC OFFICE IN REMOTE DESKTOP SERVICES ENVIRONMENTS

MiCC Office Release 5.1 and up supports a normal installation that will place all the files in locations compatible with Remote Desktop Services, with no further configuration necessary. See “Installing Standalone MiCC Office” on page 9 for installing MiCC Office.

SUPPORT SERVICES

Note: Technical support personnel may need to view the installation, setup, etc., of the Server using Mitel Remote Support.

If you have questions about any of the MiContact Center Office products, refer to this Technicians Handbook or the online Help. If you need additional support, contact the designated on-site System Manager. If the problem still cannot be resolved, refer to the Notice page in the Front Matter in this manual for technical support contact information.

Chapter 3

SPECIFICATIONS

INTRODUCTION

This section outlines the minimum platform and system requirements. Each module within MiContact Center Office has different hardware/software requirements. Before installing any of the applications, refer to Table 7.

PLATFORM REQUIREMENTS

Platform requirements for MiCC Office are detailed in System Requirements on page 23. For more information about Virtual MiCC Office, see the Virtual Appliance Deployment guide on the Mitel eDocs Web site (www.edocs.mitel.com).

Note: Technical documentation on the Mitel Web site is for registered users and requires that you provide a valid user name and password to view or download it.

The following factors affect the performance of MiCC Office:

- **MiCC Office Server**: The hard drive speed and the network bandwidth available on the MiCC Office server affects MiCC Office performance.
- **RealViewer/Reporter/Reporter Real-Time**: Initialization speed is affected by the number of filters in the Reporter Real-Time and RealViewer client applications. The more filters these client applications have, the slower initialization will be. However, filtering out devices in list tiles will increase the runtime speed.

  The speed of Reporter, Reporter Real-Time, and RealViewer is directly affected by the network link between the client and the server. Although, you can run these applications over a WAN, for optimal performance they should run on same LAN as Server.

SYSTEM REQUIREMENTS

MiCC Office server requires one of the following operating systems:

- Windows 10 Standard/Professional/Enterprise (64-bit)
- Windows 8.1 Standard/Professional/Enterprise (64-bit)
- Windows 7 Professional/Enterprise/Ultimate SP1 (64-bit)
- Windows Server 2012 R2 Standard/Data Centre (64-bit)
- Windows Server 2012 Essentials/Standard/Datacenter (64-bit)

MiCC Office client applications are supported on these versions of Windows:

- Windows 10 Standard/Professional/Enterprise (32-bit and 64-bit)
- Windows 8.1 Standard/Professional/Enterprise (32-bit and 64-bit)
- Windows 7 Professional/Enterprise/Ultimate SP1 (32-bit and 64-bit)
- Windows Server 2012 R2 Standard/Data Centre (64-bit)
- Windows Server 2012 Essentials/Standard/Datacenter (64-bit)

MiCC Office Client applications use TCP/IP to connect back to the MiCC Office Server to provide functionality. Windows shares are used for:

- Accessing the installation files
- Client applications saving log files back to the server

When the MiCC Office Server is installed on Windows Server, the following restrictions apply:

- A Windows Server Client Access License (CAL) must be purchased for every user or device running a MiContact Center Office product.
- The MiCC Office client setup kit is installed to a shared directory with a share name of “MICCO_DISKS.” A Windows Server Client Access License (CAL) must be purchased for every user or device that will access this share.

When installed on Windows Client OS, the following restriction applies:

- The MiCC Office client setup kit is installed to a shared directory with a share name of “MICCO_DISKS.” For example, Windows 7 limits the total number of simultaneous SMB (File and Printer Sharing) connections to 20.

VIRTUALISATION REQUIREMENTS

MiCC Office is supported on the following virtualization platforms when using a guest OS that meets the system server requirements in the section above

VMware ESXi 5.5
VMware ESXi 6.0
Microsoft Hyper-V Server 2012 R2

The minimum hardware requirements for MiCC Office are based on daily call volume, and defined in the following tables:

HARDWARE COMPONENT	ENTRY- LEVEL	MID-RANGE	HIGH-END
CPU	Intel Pentium D 2.8GHz or AMD Athlon 64 X2 2.6GHz	Intel Core 2 Duo 2.6GHz or AMD Athlon II X2 3.0GHz	Intel Core i3 2.9GHz or AMD Phenom II X4 2.4GHz
RAM	2GB	4GB	4GB
Hard Disk	100GB	250GB	300GB
Network	Network Interface Card	Network Interface Card	Network Interface Card
Graphics	VGA 1024 x 768	VGA 1024 x 768	VGA 1024 x 768

DAILY CALL VOLUME (INTERNAL/ EXTERNAL /EMAIL)	MICC OFFICE SERVER ONLY	MICC OFFICE AUTO REPORTER	MICC OFFICE AUTO REPORTER INTELLIGENT ROUTER	MICC OFFICE AUTO REPORTER INTELLIGENT ROUTER MEDIA BLENDING
< 1000	Entry-Level	Entry-Level	Mid-Range	Mid-Range
1000 - 5000	Entry-Level	Entry-Level	Mid-Range	Mid-Range
5000 - 10000	Entry-Level	Mid-Range	Mid-Range	Mid-Range
10000 - 25000	Mid-Range	Mid-Range	Mid-Range	High-End
25000 - 100000	Mid-Range	Mid-Range	High-End	High-End

CALL RECORDING SERVER REQUIREMENTS

Server integrates with various voice recording servers that connect to specific phones (via the station block) or trunks and store call recordings as `.wav` files. You can then play back these files at any time using a version of Reporter that is licensed for call playbacks.

MiContact Center Office supports various voice recording equipment. Please refer to the manufacturer's documentation for detailed specifications and requirements regarding the number of telephony cards and channels supported.

When using station-side recording, the recording channels are bridged to the station circuit. Each channel type (analog or digital) must correspond to the appropriate phone and card type. For example, when connected to a Mitel MiVoice Office 250 telephone system, digital channels can only be used to record Mitel digital phones; analog channels can only be used to record analog phones. When using trunk-side recording, the CRE and the trunk must be connected to the switch using a T-adapter.

Note: The voice recording server supports Integrated Services Digital Network (ISDN) trunks only. You must, therefore, have a T1/PRI or T1/E1/PRI programmed in the system to use trunk-side recording.

Note: The voice recording server records all static and noise transmitted across the phone lines. For this reason, make sure that all phone lines are clear from noise. If you find that the lines contain too much noise, ask the Central Office (CO) if it is possible to obtain conditioned phone lines.

MEDIA BLENDING REQUIREMENTS

MiCC Office Media Blending features require the following:

- **Media Blending Licensing on MiCC Office**: Provides functionality to process calls, e-mails, and other media. Without this licensing option, MiCC Office Server can process only calls.
- **Intelligent Router**: Provides the Media Blending configuration. Intelligent Router provides call routing as standard.
- **A POP3/SMTP Enabled E-Mail Server**: The e-mails processed by Media Blending are retrieved using POP3 and sent via SMTP. These are standard Internet protocols that most e-mail servers support. The e-mail server must support POP3 and SMTP to be able to support Media Blending with Intelligent Router. Examples of e-mail servers that support POP3/SMTP include Microsoft Exchange Server (with Internet Mail Connector or the Small Business Server POP3 Connector), Lotus Domino/Notes, and most UNIX mail servers, etc. Standard TCP or SSL/TLS connections are support as well as authenticated and unauthenticated connections.
- **An E-Mail Client**: Your e-mail server will either use standard POP3/SMTP e-mail clients, or have a preferred e-mail client designed to work with it, (e.g., Microsoft Exchange Server can work with any POP3/SMTP e-mail client), but integrates best with Microsoft Outlook. Each person who deals with routed e-mails needs an e-mail client configured to connect to your e-mail server.
- **ACD Working on the Telephone System**: Media Blending requires that you have ACD agents configured on your telephone system that can log in and out of designated ACD groups. If the call center operators do not currently log in to their handset, then ACD working

may not be activated on the MiVo 250 and a relevant license for this may need to be purchased from the telephone system manufacturer. The telephone system reseller will be able to advise as to whether ACD working is available on the particular telephone system, and what must be in place to activate it.

See "Implementing Media Blending" on page 141 for more information about Media Blending.

CLIENT APPLICATION REQUIREMENTS

Table 7 provides the requirements for the MICC OFFICE client computers.

Table 7: Client Application Requirements

COMPONENT	REQUIREMENT
CALLVIEWER	
CPU	P4, 1.2 Ghz
RAM	512 MB RAM
Network Card	MICC OFFICE Clients must have TCP/IP connectivity to
MiCC Office server Monitor	800 x 600 screen resolution and 256 Colors
Operating System	One of the following supported Microsoft operating systems: • Windows 8 Professional/Enterprise (32-bit or 64-bit) • Windows 7 SP1 Professional/Ultimate (32-bit or 64-bit)
REALVIEWER, REPORTER, REPORTER REAL-TIME	
CPU	P4, 2 Ghz
RAM	2GB
Network Card	MiCC Office Clients must have TCP/IP connectivity to MICC OFFICE server. The link between client and server must be high capacity and low latency.
Monitor	1024 x 768 screen resolution and high-color (16-bit)
Operating System	One of the following supported Microsoft operating systems: • Windows 8 /Professional/ Enterprise.(32-bit or 64-bit) • Windows 7 SP1 Professional/Ultimate (32-bit or 64-bit)

FIREWALL AND ROUTER PORTS

Firewalls generally make filtering decisions based on IP addresses and port numbers. For security reasons, all ports should be disabled except those that are specifically required. Keep the following considerations in mind when opening ports:

- Installing non-tested and non-supported software on Mitel products may open ports and cause security risks.
- Installing Windows components, including Windows updates, on Mitel products may open other ports that are not necessarily open.

MiContact Center Office communicates with different entities, each of which requires a different port. To ensure that those in your network have access to these entities, the gateway/router/firewall must have the ports listed in Table 8 open.

Note that certain MiCC Office applications can send e-mail via MAPI or SMTP. Ports used by MAPI and SSL/TLS SMTP are not covered in Table 8, because it is dependent upon mail server configuration.

Note: Currently only TLS 1.0 and lower is supported for the SSL/TLS SMTP connection.

Note: SMTP Authentication account name has a limit of 31 characters

Table 8: MiContact Center Office Port Assignments

DEFAULT PORT NUMBER	PORT NAME	TCP/ UDP	FUNCTION	DIRECTION
22	AMC	TCP	Allow outbound packets (and replies) for AMC communication	MICC OFFICE server → LAN
25	SMTP	TCP	Used to send outgoing e-mail messages. This is used by Intelligent Router for Media Blending	MICC OFFICE server → LAN
80	AMC	TCP	Allow outbound packets (and replies) for AMC communication **NOTE:** This port (80) only applies to Virtual MICC OFFICE.	MICC OFFICE server → LAN
80	TCP	MiXML	A Mitel web-service-based protocol that exposes configuration management (and other) features to applications	MICC OFFICE server → LAN
110	POP3	TCP	Used to receive incoming e-mail messages. This is used by Intelligent Router for Media Blending	MICC OFFICE server → LAN
135	DCOM	TCP	Used for communication between the recording servers and the MICC OFFICE server.	MICC OFFICE server → LAN
445	Microsoft-DS Server Message	TCP	Protocol used for file sharing in Windows.	LAN → MICC OFFICE server
3986	MICC OFFICE Protocol	TCP	MICC OFFICE applications connect to the MICC OFFICE server on this port	MICC OFFICE clients → MICC OFFICE
4000	OAI	TCP	Used to send OAI information to the MiCC Office server from Mitel MiVoice Office 250/CT Gateway.	MICC OFFICE server → LAN
8222	AMC	TCP	Allow outbound packets (and replies) for AMC communication	MICC OFFICE server → LAN
50000	DB2	TCP	Used by MICC OFFICE applications and the MICC OFFICE server for database access.	MICC OFFICE clients → MICC OFFICE Server

Chapter 4

APPLICATIONS

INTRODUCTION

The MiContact Center Office product consists of both server and client applications that may be included in base licensing or require the purchase of additional licensing. For more information about product licensing, see “Licensing” on page 13.

MiCC Office server applications include:

- MiCC Office Server (Server Monitor and Control Panel Applet)
- Data Manager
- Intelligent Router

MiCC Office client applications include:

- CallViewer
- RealViewer
- Reporter (includes AutoReporter)
- Reporter Real-Time (includes AutoReporter)

This document provides a brief description of features, components, and configuration of the applications. Detailed information about fields, options and instructions are available in the online Help for the specific application.

SERVER

Server stores all calls and provides real-time information for the other components of the system. This section describes the main features provided by Server.

CALL MODELING

MiCC Office Server supports internal and external call modeling, including calls made between nodes across networked telephone systems, depending upon the functionality of the host telephone system and may require a Mitel CT Gateway.

You can configure MiCC Office to model call traffic using a global option that universally enables or disables internal call measurement. Using Data Manager, you can specify whether trunk line and internal calls will be modeled on a per-device basis. Also, you can specify whether only inbound, outbound, or both types of internal calls are modeled on a per-device basis.

CALL SEGMENTATION

Call Segmentation is a configurable feature in Server that improves the accuracy and detail of real-time and historic call reporting. The Call Segmentation feature is highly configurable, enabling you to choose how MiContact Center Office calculates trunk line call statistics for different devices on the telephone system.

Call segmentation feature provides the following functions:

- **Detailed Trunk Call Transfer History**: When a trunk call is transferred several times throughout its duration, the call segmentation feature makes it possible to find out all of the extensions/agents that the trunk call had been transferred through. This enables you to obtain an entire history of a trunk line call throughout the telephone system and see all the different devices that handled the corresponding call using the Call Detail window. Where calls are made or received on SIP Trunks, a SIP Peer Name representing the entire trunk group will be reported, instead of a specific numeric trunk. Multiple calls will show the same SIP Peer Name for the trunk.

- **Accurate Call Duration Measurement Against Devices**: Call statistics such as talk time, average talk time, calls in, etc., can be accurately calculated against each extension or agent even when a trunk call is transferred several times among different extension devices.

- **Detailed Hunt Group Call Measurement**: Call Segmentation gives you more detailed reporting against hunt group devices. For example, a trunk line call can be answered by an agent in one hunt group and then transferred by that agent to a different hunt group. The caller could then abandon the call while they are waiting in the second hunt group queue. The trunk call is therefore “answered” against the first hunt group but “abandoned” in the second, in addition to the call having separate call waiting times against each of the different hunt group queues. Call segmentation allows the tracking of hunt group statistics separately to enable this type of call measurement.

Server performs trunk call segmentation for two different types of scenarios:

- **Device Entry**: The Device Entry segmentation rule segment calls only if they start alerting a hunt group because the call has been transferred or diverted from another device (i.e., it should occur for hunt groups, not extensions). This rule gives Customer Service the ability to measure call totals and ring/wait time separately against different hunt groups.
- **Device Exit**: The Device Exit segmentation rule separates calls only if they are transferred or diverted from an extension device (i.e., it should occur for extensions, not hunt groups). This rule gives Customer Service the ability to measure the call totals and call ring/wait and talk time of a trunk call separately again different extension devices.

CALL SEGMENTATION EXAMPLES

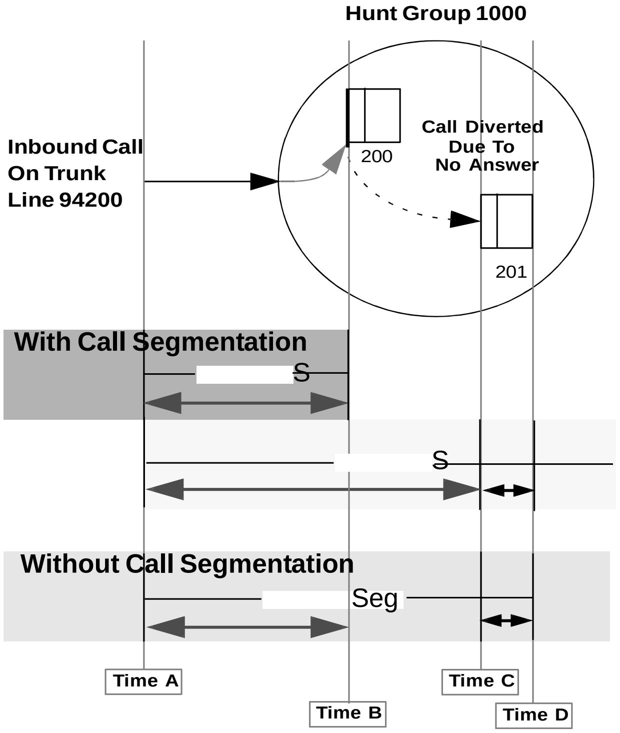
This section provides examples of different call segmentation scenarios which explain how Server calculates the call statistics for each device involved in the call.

Trunk Call – ACD Hunt Group Example

The call flow for this scenario is as follows (see Figure 1):

1. The trunk call alerts hunt group 1000.
2. The hunt group presents the call to device 200.
3. Extension 200 does not answer, and the call is diverted due to no answer to another hunt group member. A hunt group call is diverted due to no answer when the call ring time at the specific hunt group member reaches the group’s No Answer Advance timer setting.
4. The hunt group presents the call to device 201.
5. Extension 201 answers the call.

Figure 1: Trunk Call – ACD Hunt Group Example


Hunt Group 1000
Inbound Call On Trunk Line 94200
200
Call Diverted Due To No Answer
201
With Call Segmentation
S
S
Without Call Segmentation
Seg
Time A
Time B
Time C
Time D

Call Segmentation is performed when the trunk call is diverted from extension 200 to 201 so that a record is made indicating that the call alerted extension 200 but was refused (see Table 1).

Table 1: Device Exit with Call Segmentation

Seg	Start Time	Ring/Wait Duration	Total Duration	Device First Rung	Device Last Rung	Device Answered At	Device Finished At	Trunk Record Creation Reason
1	[Time A]	[Time B] -[Time A]	[Time C] - [Time A]	1000	200	[None]	[None]	“New Trunk Call Started”
2	[Time A]	[Time C] - [Time A]	[Time D] - [Time C]	1000	201	201	201	“Call Diverted Due To No Answer

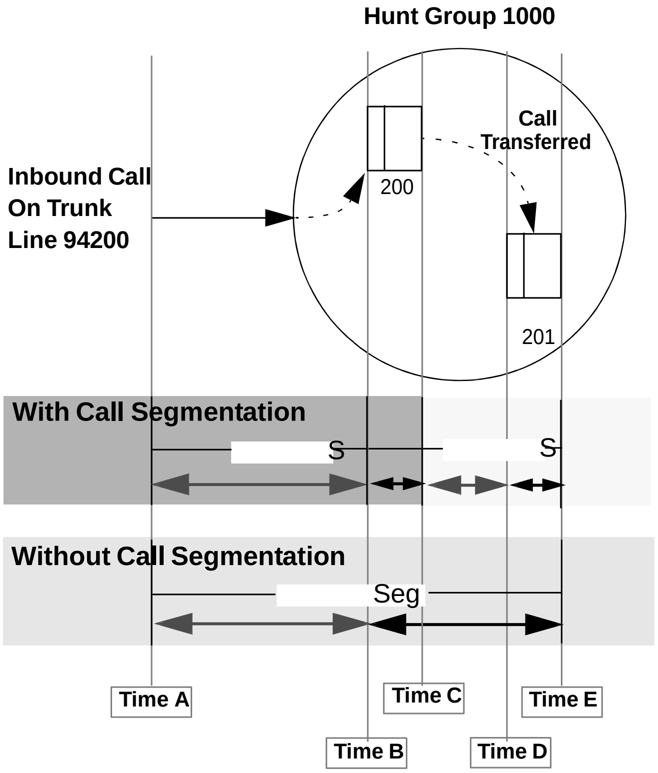
Trunk Call – Extensions Example

The following is another example where a trunk call moves between different extensions.

The call flow for this scenario is as follows (see Figure 2):

1. The trunk call alerts hunt group 1000.
2. The call alerts extension 200.
3. Extension 200 answers the call.
4. The call is transferred to extension 201.
5. Extension 201 answers the call.
6. The trunk call is terminated at extension 201.

Figure 2: Trunk Call – Extensions Example



The call ring/wait and talk time is measured separately for each extension device. The call ring/wait time at hunt group 1000 can also be specifically measured using the first call segment record. If Call Segmentation is not enabled, the call's talk time is only measured for the device where the call terminated (extension 201), but the call ring/wait time at hunt group 1000 is measured correctly (see Table 2).

Table 2: Device Exit with Call Segmentation

Seg	Start Time	Ring/Wait Duration	Total Duration	Device First Rung	Device Last Rung	Device Answered At	Device Finished At	Trunk Record Creation Reason
1	[Time A]	[Time B] -[Time A]	[Time C] - [Time A]	1000	200	200	200	"New Trunk Call Started"
2	[Time C]	[Time D] - [Time C]	[Time E] - [Time C]	201	201	201	201	"Call Transferred To Extension"

DEVICE EXIT AND DEVICE ENTRY TOGETHER

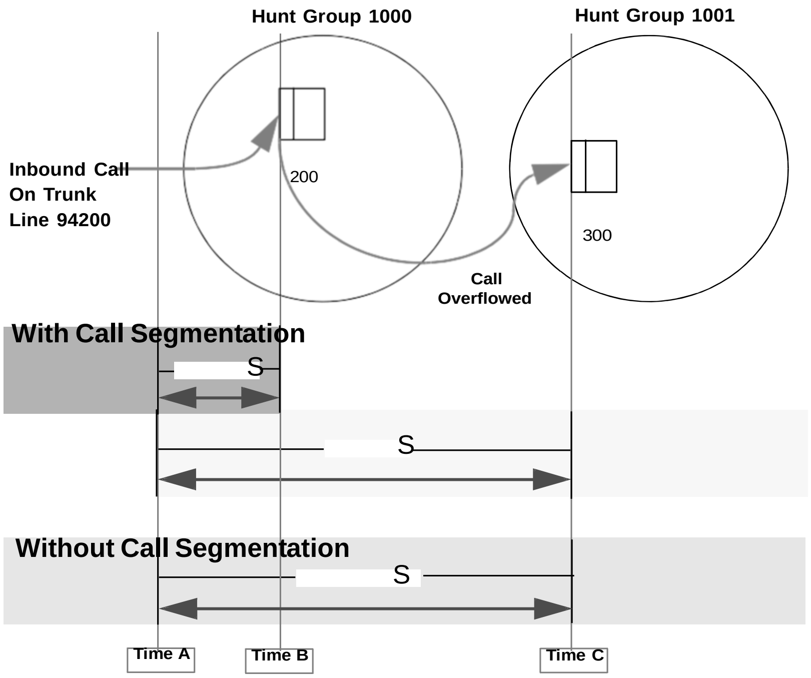
When the Device Entry and Device Exit segmentation rules are satisfied together in a trunk call, the Device Entry rule takes precedence so that the hunt group statistics are calculated appropriately. In the previous example, the Device Entry rule is satisfied when the call starts alerting hunt group 1000. However, the Device Exit rule is also satisfied when the call is transferred from extension 300 to hunt group 1000. The Device Entry rule took precedence so that the corresponding segment record reflects the call statistics of hunt group 1000 in MiCC Office reporting applications.

RING/WAIT TIME RESETTING

When call segmentation occurs for unanswered trunk calls, a programmable setting is required for a device, allowing the installer to choose to reset the call start time for the next call (e.g., the next trunk call segment has its ring/wait time reset to zero).

Note: A trunk call's start time is always reset for the next call segment if the call was in the answered state when it was transferred, which measures the ring/wait time at the "transferred to" device more accurately.

Figure 3: Ring/Wait Time Resetting Example.



The previous diagram shows a trunk alerting hunt group 1000 and then overflowing (recalling) to hunt group 1001. The important concept is how the ring/wait time is measured for hunt group 1001. Ideally, a call center supervisor wants to measure the entire time a caller has been waiting (e.g., Seg 2's ring/wait time = Time C - Time A). However, there might be some cases when the supervisor only wants to see the actual time the caller spent within hunt group 1001's queue (e.g., Seg 2's ring/wait time = Time C - Time B). Because you can configure the call start reset time, Call Segmentation can measure the same call in different ways to suit your call record needs.

SERVER USER INTERFACE (UI) COMPONENTS

MiCC Office Server runs as a Windows service, so you do not need to be logged on to the Server before the software can be used. Running Data Manager will not stop the Server activity.

The MiCC Office Server icon in the Windows Notification area (or system tray) shows the current status of MiCC Office Server (see Table 3).

Table 3: MICC OFFICE Server Icon

ICON	DESCRIPTION
▦	If the MICC OFFICE Server is running and successfully communicating with the telephone system, the gray checkerboard appears in the system tray.
?	If the MICC OFFICE Server is not running or communicating with the telephone system, the icon alternates between the gray checkerboard and a yellow question mark.
🟥	If the telephone system is being initialized (Connecting), the icon appears as gray and shaded red checkerboard.
🟩	When data is received from the telephone system, the icon alternates between the gray checkerboard and a green/gray checkerboard.
🟨	When data is sent to the telephone system, the icon shows yellow in the lower-right quadrant.

Note: The colors of the status icons described above are the defaults. Right-click the MiCC Office Server tray icon, and then select **Activity Settings** to customize the colors.

You can move the mouse pointer over the Server tray icon to see if the service is running. When the Server service is not running, you can start Server from the Control Panel Applet (see “Control Panel Applet” on page 38).

The following interface components provide information and configuration options for Server:

- “Data Manager” on page 36
- “Control Panel Applet” on page 38
- “Server Monitor” on page 39
- Activity Settings

To access Server components, right-click the MiCC Office Server tray icon (▦), and then select the component from the menu.

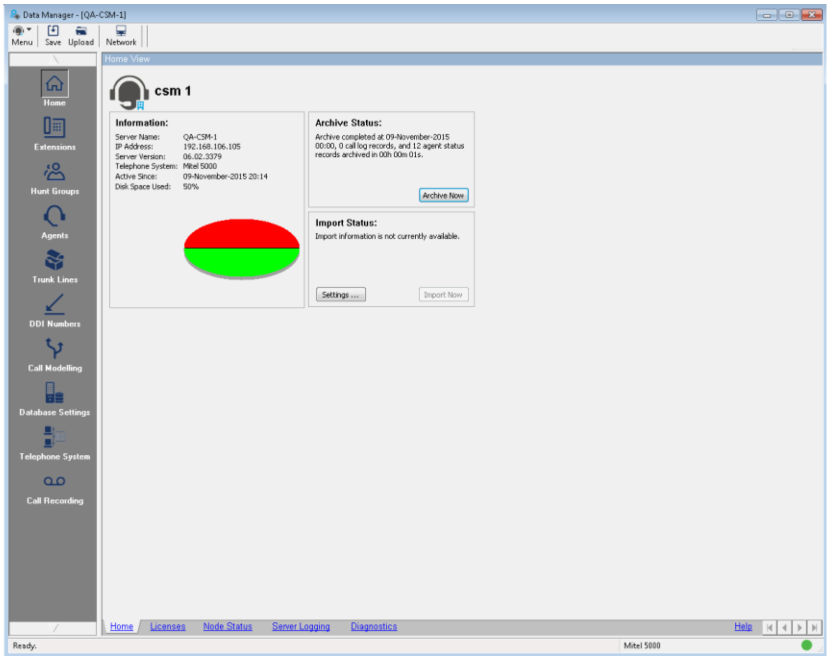
DATA MANAGER

Data Manager is the application used to configure MiCC Office Server. For Server to function correctly with the communications platform, you must enter the required data from the Agents, Hunt Groups, Extension, and Trunk Lines views in Data Manager. Activity that occurs on devices that are not configured in Data Manager is not modeled or stored historically.

To open Data Manager, do one of the following:

- Double click the **Data Manager** icon on the desktop.
- Right-click the MiCC Office Server tray icon (▦), and then select Data Manager.

Figure 4: Data Manager Interface



csm 1

Information:
Server Name: QA-CSM-1
IP Address: 192.168.106.105
Server Version: 06.02.3379
Telephone System: Mitel 5000
Active Since: 09-November-2015 20:14
Disk Space Used: 50%

Archive Status:
Archive completed at 09-November-2015 00:00, 0 call log records, and 12 agent status records archived in 00h 00m 01s.

Import Status:
Import information is not currently available.

Ready.
Mitel 5000

The Data Manager interface consists of the following elements:

- **Main menu and toolbar**: Includes the following options:
  - *Save*[1]: Saves the current configuration data to the file name and location you specify. You can also access the Save feature by clicking the icon on the toolbar.
  - *Upload*[1]: Uploads a configuration file to Data Manager and sends commands to the MiCC Office Server requesting that all extensions, hunt groups, DID numbers, agents and trunk lines be deleted and that all settings be reset to default values.
  - *Network Settings*[1]: When the Data Manager is in the Active Configuration mode, displays the Network Settings dialog, which includes the name of the computer to which Data Manager is connected, and the port used for the connection.
  - *Change Password Level*: Switches between “Full Access” and “Read Only” modes after you supply the relevant password. This option is available only when connected to a Server that has passwords configured.
  - *Help Topics*: Displays the Data Manager online help.
  - *About Data Manager*: Displays information about the MiCC Office Server (software version number, password level, etc.) and the version number of the Data Manager.
  - *Exit*: Closes Data Manager.
- **Main window**: The default view provided in the Main window is the Home View, which shows an overview of the current state of MiCC Office Server and includes tabs for licenses, node status, server logging, and diagnostics. To access a different view, click one of the following options from the panel on the left of the interface:
  - *Home*: Provides an overview of the current state of MiCC Office Server and includes the following tabs:

[1] Also available from the Toolbar.

  - Home
  - Licenses
  - Server Logging
  - Diagnostics
  - Node Status

- *Extensions*: Provides options to Add, Change, and Delete extensions, and to enable internal call modeling on a per-device basis.
- *Hunt Groups*: Provides options to Add, Change, and Delete hunt group records.
- *Agents*: Provides options to Add, Change, and Delete agent records.
- *Trunk Lines*: Provides options to Add, Change, and Delete trunk lines.
- *DID\DDI Numbers*: Provides options to Add, Change, and Delete DID\DDI numbers.
- *Call Modeling*: Provides access to global call modeling options form the following tabs:
  - Telephone Numbers
  - Internal Calls
  - Call Routing
  - Advanced
- *Database Settings*: Used to configure Server to import a summary of your organization's or department’s database so that external calls can be identified either by using the received Caller ID (inbound calls) or by using dialed digits (outbound calls). The Database Settings View contains the following tabs:
  - Database Settings
  - Telephone Import
  - Database View
  - Manage Historic Data
- *Telephone System*: Used to configure the MiCC Office Server to import a summary of your organization's or department's database so that external calls can be identified either by using the received Caller ID (inbound calls) or by using dialed digits (outbound calls).
- *Call Recording*: Used to configure MiCC Office server to communicate with the database on the call recording server.

There are two types of views shown in the Main window:

- **List-based**: List-based views have links at the bottom to add, edit, and remove more devices, for example: agents, extensions, DID\DDI numbers, and hunt groups.
- **Settings-based**: Settings-based views contain one or more tabs of similar settings.

CONTROL PANEL APPLET

The Control Panel applet provides access to basic functions for Server from the following tabs:

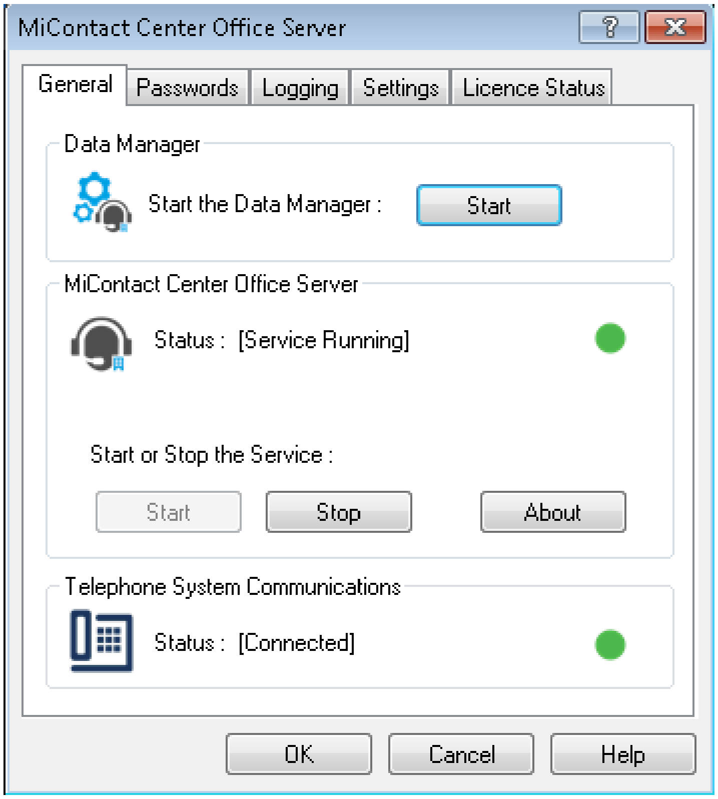
- General Tab
- Passwords Tab

- Logging Tab
- Settings Tab
- License Status Tab

You can start and stop Server from the General tab.

To start or stop MiCC Office Server:

1. Right-click the MiCC Office Server tray icon (▣), and then click **Control Panel**. The MiContact Center Office Server Control Panel appears.


MiContact Center Office Server
General
Passwords
Logging
Settings
Licence Status
Data Manager
Start the Data Manager :
Start
MiContact Center Office Server
Start or Stop the Service :
Start
Stop
About
Telephone System Communications
OK
Cancel
Help

Status : [Service Running]

Status : [Connected]

2. Do one of the following:
   - To start Server, click **Start** in the MiContact Center Office Server section of the General tab.
   - To stop Server, click **Stop** in the MiContact Center Office Server section of the General tab.

SERVER MONITOR

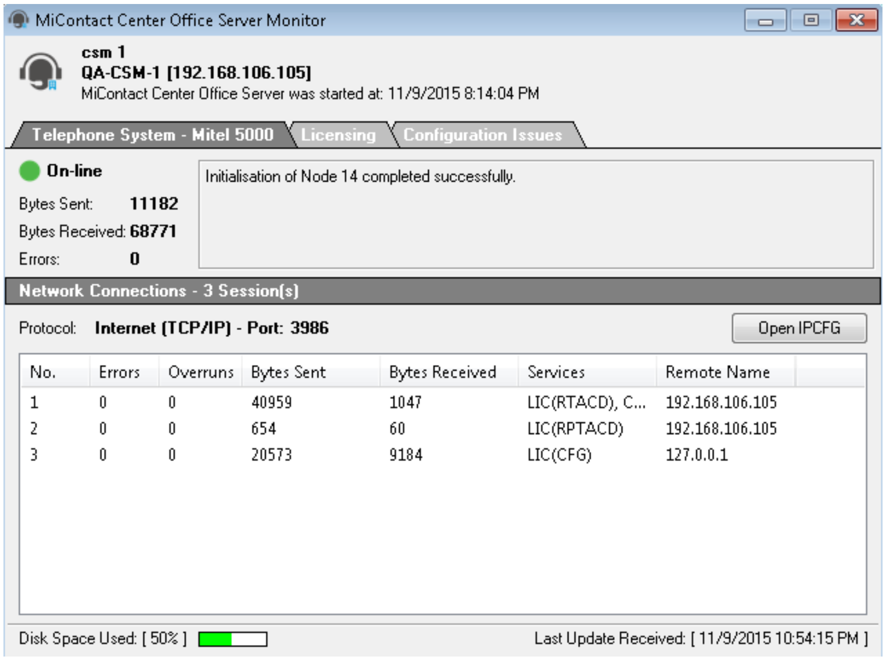
The MiCC Office Server Monitor interface displays the real-time status of all the network connections to remote applications, concurrent licensing information, and the status of the telephone system communication. The interface is updated every five seconds.

To open Server Monitor, do one of the following:

- Double click the **MiCC Office Server Monitor** icon on the desktop.

- Right-click the MiCC Office Server tray icon (▣), and then select Server Monitor.

Figure 5: Server Monitor Interface



MiContact Center Office Server Monitor
Telephone System - Mitel 5000
Licensing
Configuration Issues
Open IPCFG

csm 1
QA-CSM-1 [192.168.106.105]
MiContact Center Office Server was started at: 11/9/2015 8:14:04 PM

On-line
Bytes Sent: 11182
Bytes Received: 68771
Errors: 0

Initialisation of Node 14 completed successfully.

Network Connections - 3 Session(s)

Protocol: Internet (TCP/IP) - Port: 3986

No.	Errors	Overruns	Bytes Sent	Bytes Received	Services	Remote Name
1	0	0	40959	1047	LIC(RTACD), C...	192.168.106.105
2	0	0	654	60	LIC(RPTACD)	192.168.106.105
3	0	0	20573	9184	LIC(CFG)	127.0.0.1

Disk Space Used: [50%]
Last Update Received: [11/9/2015 10:54:15 PM]

The Server Monitor interface includes the following main areas:

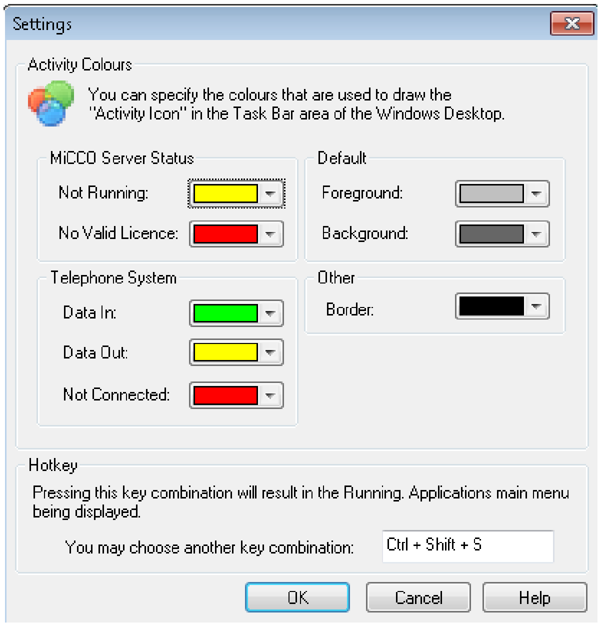
- Main Menu
- Header
- Tabs: Includes:
  - Telephone System Tab
  - Licensing Tab
  - Configuration Issues Tab
- Network Connections
- Status

ACTIVITY SETTINGS

Using the Activity Settings dialog box, you can customize the colors used for the Server tray icon and the default key combination to bring up the Server tray menu.

To access the MiCC Office Server Activity Settings dialog box, right click the MiCC Office Server tray icon (▨), and then select **Activity Settings**.

Figure 6: Activity Settings Dialog Box



Settings

Activity Colours

You can specify the colours that are used to draw the "Activity Icon" in the Task Bar area of the Windows Desktop.

MiCCO Server Status

Not Running: 🟨

No Valid Licence: 🟥

Default

Foreground: ⬜

Background: ⬛

Telephone System

Data In: 🟩

Data Out: 🟨

Not Connected: 🟥

Other

Border: ⬛

Hotkey

Pressing this key combination will result in the Running. Applications main menu being displayed.

You may choose another key combination: Ctrl + Shift + S

The Activity Settings dialog box contains the following main areas:

- **Activity Colors**: You can customize the colors displayed by the MiCC Office Server tray icon based on status. You can also customize the default foreground, background and border colors for the icon.
- **Hotkey**: The hotkey option allows you to change the default key combination used to bring up the tray menu.

INTELLIGENT ROUTER

Intelligent Router is a licensed MiCC Office server application that uses Dynamic Call Mapping™ Technology to perform real-time call routing and call mapping. Using a combination of conditions and rule types, you can program this application to notify supervisors when a call is abandoned, change the status of an agent based on the number of refused calls, record calls to a mailbox, and perform a variety of other actions. If configured, you can also use Intelligent Router to restrict calls made from certain devices to specific numbers.

You can program Intelligent Router to execute different actions whenever a statistic reaches a specific value. Using placeholders, which represent these statistics, you can route calls and e-mail messages based on the information stored in Server or based on real-time information, such as the current date and time. This allows you to map calls and e-mail messages from customers to a specific agent, enable and disable different features during business hours, and forward calls to an overflow device when all agents are busy.

With Intelligent Router, you can view up to four different tiles, each of which is configurable, on the computer running the application. These tiles display real-time information pertaining to rules, actions, trunk line calls, and other statistics, providing the details needed to ensure calls and e-mail messages to Media Blending groups are successfully mapped.

Intelligent Router provides the following features:

- **Historical Call Routing**: The MiCC Office Server provides support for advanced routing conditions in Intelligent Router. It stores a history of the last three extensions or agents that handled a contact with a known identity (as indicated by the presence of Caller ID or an e-mail address), which allows Intelligent Router to automatically route calls and e-mail messages from identified parties back to the last extension or agent that handled the contact.
- **Internal Call Routing**: Internal calls are included in features such as intelligent call routing, abandoned call notification, skill set routing, and agent state control.
- **Routing Conditions**: To support the addition of internal call modeling and media blending, you can apply the same statistics used to monitor these new features in Reporter and RealViewer as routing conditions. To see a full list of the statistics that are available, refer to Intelligent Router online Help.

CONFIGURATION REQUIREMENTS

For Intelligent Router installations, you must program the telephone system to send a specified set of inbound external (trunk) calls to an ACD hunt group containing a single agent ID. This ACD hunt group cannot be an all-ring hunt group (i.e., the calls must be distributed through the group). The type of inbound calls that are routed to the Intelligent Router group (as controlled by the telephone system configuration) is dependent on the particular call routing application.

Intelligent Router is installed during the MiCC Office setup. See "Installing Micc Office" on page 88 for details.

Note: As a precaution, you should program the telephone system to send calls that ring in to this hunt group to overflow after 5-10 seconds to another group that contains agents. This overflow configuration is a safeguard in the event power is lost to the Server computer.

RUNNING INTELLIGENT ROUTER

If you are licensed to use Intelligent Router, it is possible to run Intelligent Router without having to manually log on to the Windows virtual machine.

The following procedure describes how to configure Windows such that a user with an Administrator account automatically logs on when Windows starts.

Before you complete this procedure, you must add Intelligent Router to the Startup Group (see See “Installing Micc Office” on page 88).

To configure Windows Administrator automatic log on:

1. Access the VMware Console and log on to Windows as an administrator on the Windows virtual machine.
2. Refer to Microsoft KB 324737 (http://support.microsoft.com/kb/324737) for information about how to enable Windows automatic log on for a specific user. Perform the steps as described in the KB article, but ***do not*** shut down as instructed in the article.
3. Refer to Microsoft KB 119364 (http://support.microsoft.com/kb/119364) for information about retaining the correct username for automatic logon. Follow the instructions in the KB article. Further clarification is provided below:
    - **a.** When instructed to create a .ini file, use **`Administrator.ini`** as the file name.
    - **b.** When creating the ini file contents, Replace **<USERNAME>TEST** with **Administrator**.
    - **c.** Save the file to `C:\` as described in the article, or choose a more convenient location.
    - **d.** Create a batch file using **`Administrator.bat`** as a file name.
    - **e.** The contents of the batch file should be **`regini`** followed by the full path name to the ini file. For example, if you created the **`Administrator.ini`** file and saved it to the `C:\` location, the contents of the batch file should be **`regini C:\Administrator.ini`**.
    - **f.** Save the batch file to **`C:\Documents and Settings\All Users\Start Menu\Programs\Startup`**.
4. Restart the Windows machine to apply the changes.

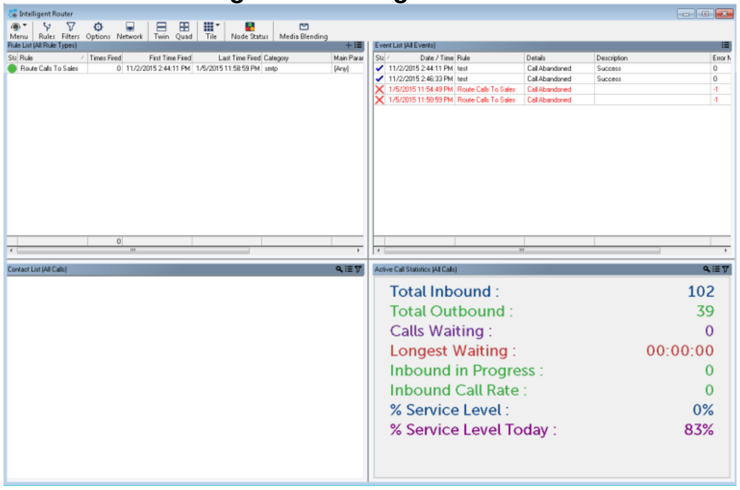
MANUALLY STARTING INTELLIGENT ROUTER

If you close Intelligent Router without restarting the server, you must manually start it using your desktop or the **Start** menu, as described below.

To start Intelligent Router, do one of the following:

- From the Start menu, select All Programs –Mitel MiContact Center Office – **Intelligent Router**.
- Double-click on the Intelligent Router icon () on your desktop.

Figure 7: Intelligent Router



Sta	Rule	Times Fired	First Time Fired	Last Time Fired	Category	Main Parar
●	Route Calls To Sales	0	11/2/2015 2:44:11 PM	1/5/2015 11:58:59 PM	smtp	[Any]

Sta	Date / Time	Rule	Details	Description	Error N
✓	11/2/2015 2:44:11 PM	test	Call Abandoned	Success	0
✓	11/2/2015 2:46:33 PM	test	Call Abandoned	Success	0
✗	1/5/2015 11:54:49 PM	Route Calls To Sales	Call Abandoned		-1
✗	1/5/2015 11:58:59 PM	Route Calls To Sales	Call Abandoned		-1

Total Inbound :	102
Total Outbound :	39
Calls Waiting :	0
Longest Waiting :	00:00:00
Inbound in Progress :	0
Inbound Call Rate :	0
% Service Level :	0%
% Service Level Today :	83%

To display and analyze the information, Intelligent Router uses the following elements:

- **Tiles**: Display various data and are the basic user-interface element of Intelligent Router. With Intelligent Router, you can view up to four different tiles: Rules List, Event List, Contact List, and the Multi-Stat Tile. Each has a unique way of displaying its data, including which items or statistics it can display and how the information is interpreted. In addition, you can apply filters to the Contact List and Multi-Stat Tiles.
- **Statistics**: Include information about the call or group of calls. Everything within Intelligent Router displays as a statistic, including the name of the caller on a given trunk line, the number of inbound calls answered by a given agent, or the total talk time accumulated so far today for every device.
- **Filters**: Let you limit the data you view. With filters, you can limit a tile to display only those devices in a particular group. Or, you can change a particular statistic so that it only applies to calls that rang for more than a given time, for calls that were outbound, etc.
- **Alarms**: Alert you when a statistic falls within a given range. You can configure alarms to flash the associated tile, play a sound, write a message to an alarm log, and/or activate the alarmed tile.
- **Categories**: Allow you to create groups for different rules. You can also assign different color combinations to categories for easy viewing.

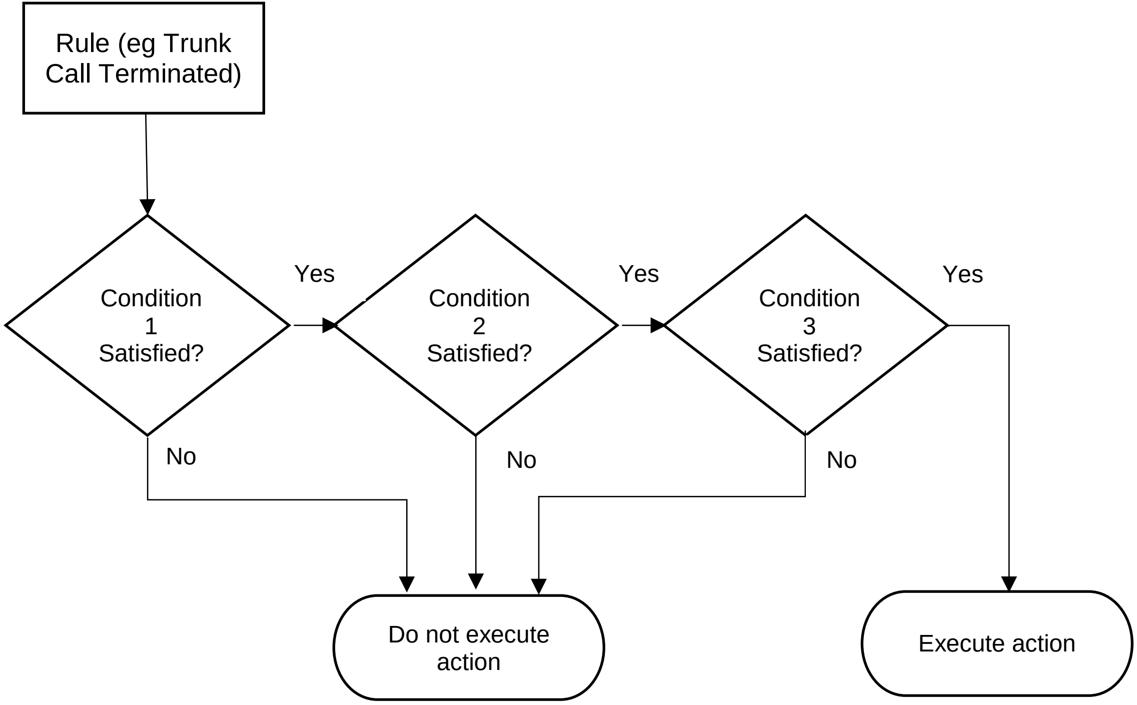
Note: You can only apply Alarms to the Contact List Tile.

- **Global Options**: Affect particular types of statistics and the display.

INTELLIGENT ROUTER FUNCTIONS

Intelligent Router uses a combination of rules, conditions, actions, and placeholders to perform various functions, as illustrated in Figure 8.

Figure 8: Intelligent Router Functions Example



In this example, a rule is evaluated based on three separate conditions. If all conditions are met, the action is executed (i.e., the trunk call is terminated). If any one of these condition is not met, the action is ignored (i.e., the trunk call remains connected).

With the rule, action, condition, and placeholder elements, you can program the application to route calls and/or e-mail messages in real-time based upon the current state of your telephone system. Because this application is highly configurable, you can create an almost infinite number of combinations.

RULES

A rule defines how its associated conditions are evaluated, which determines whether or not the related action is executed. When defining rules, you can select a specific rule type (e.g., call routing, extension/agent status changed, etc.), the type of device affected (i.e., extension/group or agent ID), and other various parameters. After the rule is programmed, you can assign conditions that must be met before the desired action is executed.

ACTIONS

An action is the function performed when the rule is evaluated and all the conditions applied to the rule are met. Intelligent Router supports many different actions, including terminating trunk calls, routing calls, forwarding calls, routing media, etc. Actions also support placeholders, which allow you to configure detailed routing schemes (see the following sections for more details).

CONDITIONS

A condition is a comparison that is made after a rule is evaluated. For example, you can program a condition so that a rule only processes inbound trunk calls with Caller ID. Conditions are based upon statistics and support placeholders, which are described in the following section.

PLACEHOLDERS

Placeholders allow you to assign additional parameters to a condition or action. For example, you can route a call based on the fields assigned in the Telephone Import screen in MiCC Office Server. You can also route calls based on different statistics, including the current time, number of calls, etc. All placeholders represent an Intelligent Router statistic and are displayed within brackets (e.g., [Ring Time @Call]).

When a rule is evaluated, the Placeholder information is replaced with the appropriate value for the specified statistic. For example, [Ring Time @Call] is replaced by the ring time for the trunk call for which the rule was evaluated (e.g., 00h 02m 30s). A Placeholder of [Field 2 @Call] would be replaced with the contents of database field 2 that corresponds to the trunk call's Caller ID or dialed digits (this information is stored in MiCC Office Server).

MEDIA BLENDING

Media Blending provides the ability for e-mail messages sent to e-mail addresses related to hunt groups to be routed to available agents in a similar fashion to calls routed to agents.

Customers send e-mail messages to a Media Blending queue, which is an e-mail address assigned to a hunt group. For example, if the sales team receives calls via hunt group 1000, and receive e-mail messages via "sales@company.com," then hunt group 1000 would be mapped to sales@company.com to form a Media Blending queue.

Intelligent Router handles the e-mail bound for the e-mail address associated with the Media Blending queue. It downloads the e-mail, stores it on the local hard disk, and then deletes it from the mail server. Intelligent Router informs the MiCC Office Server that a new e-mail is queuing. MiCC Office Server then updates the relevant client applications.

With Intelligent Router performing Media Blending on the sales ACD group and e-mail address, e-mail messages to the sales inbox are queued by Intelligent Router. When an agent becomes available in the sales group, they are routed the next sales e-mail. While they are handling the e-mail, the agent is not routed any calls from the sales ACD group. After they reply to the e-mail, they are once again routed calls for sales, or further e-mail messages.

Intelligent Router can be configured so that it will not attempt to route e-mail messages to agents if they are busy (for example, if too many calls are waiting at the sales group, or a required service level is not high enough). This means that agents do not have to be forced to process e-mail messages when calls are waiting, because a caller has a more immediate requirement than a customer who has sent an e-mail.

AUTO RESPONSE TO CUSTOMER

You can configure Intelligent Router to process e-mail messages as they arrive from customers. For example, when a message is received for the technical support group, Intelligent Router can send an automatic response back to the customer so that they are aware their e-mail has been received and is being addressed. The reply can include a variety of statistics. For example, how long e-mail messages are queuing for on average, or the average call wait time on the queue, and the number of e-mail messages or calls in the queue.

Intelligent Router can detect keywords in the subject, and automatically respond with appropriate content. Intelligent Router could monitor the "info@xyz.com" inbox, and send different responses based on which keywords were present in the subject.

If a customer sends an e-mail with the subject "Request Directions," then a response is automatically sent containing directions to the XYZ Company headquarters. If a customer sends an e-mail with the subject “Request PQ-7140 Information,” then a response is automatically sent containing product information on a particular product in XYZ’s product range.

E-MAIL BLOCKING

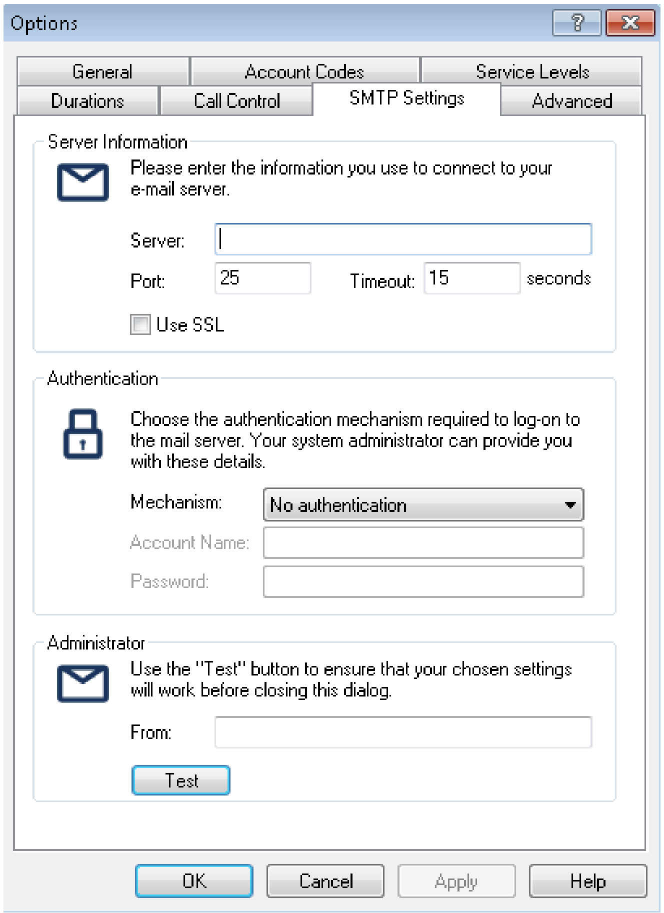
Intelligent Router can stop certain e-mail messages being received by the monitored queues, or stop agents responding to messages with inappropriate terminology.

For example, if messages arrive from an external party with certain keywords in them (e.g., swear words), they could automatically be forwarded to an administrator, or even deleted. Similarly, outbound messages to customers can be checked for profanity, and if such a message is found, it can be forwarded to a supervisor, and sent back to the agent to edit the message accordingly.

SMTP CONFIGURATION

The Intelligent Router command “Send E-mail (Via SMTP)” uses the Simple Mail Transfer Protocol when communicating with an e-mail server. Mitel advises using SMTP in preference to MAPI where possible.

To use the “Send E-mail (Via SMTP)” rule action, the SMTP Settings section must first be configured on the Options form.



Server Information

Please enter the information you use to connect to your e-mail server.

Server:

Port: 25

Timeout: 15 seconds

☐ Use SSL

Authentication

Choose the authentication mechanism required to log-on to the mail server. Your system administrator can provide you with these details.

Mechanism: No authentication

Account Name:

Password:

Administrator

Use the "Test" button to ensure that your chosen settings will work before closing this dialog.

From:

The default port for SMTP is 25 (587 when using SSL) but this can be configured to any port on the server. If authentication is being used then usually the From address will need to be the same as the authenticated user otherwise the SMTP may not route the e-mail.

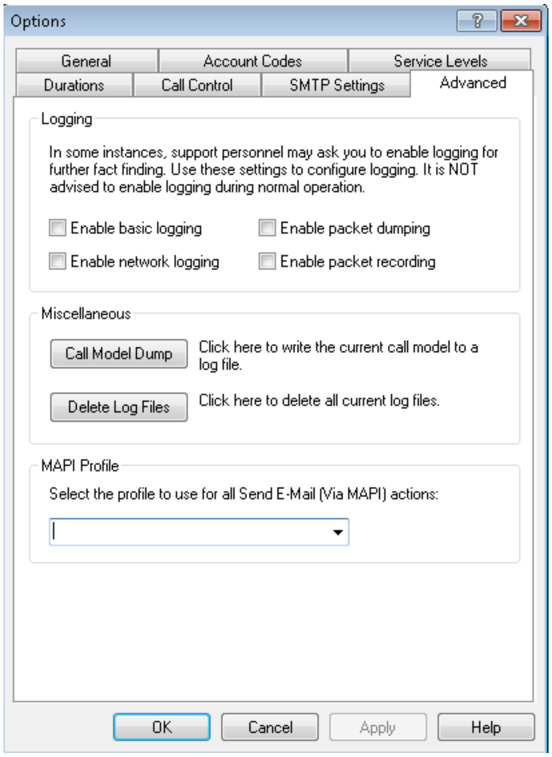
The Intelligent Router shares e-mail settings with MiCC Office Reporter althought the From address is different. The Test button can be used to confirm the settings entered are correct. When testing you will be prompted to enter a target e-mail address for the test e-mail

MAPI PROFILE

The Intelligent Router command “Send E-mail (Via MAPI)” uses extended Messaging Application Programming Interface (MAPI) when communicating with the Outlook e-mail client. Mitel recommends that you create and configure a MAPI profile before using the Send E-mail (Via MAPI) action. This ensures that the outgoing mailbox is properly configured before the action is used.

After you create a MAPI profile, you must configure Intelligent Router to use it for any Send E-Mail (Via MAPI) actions. From the Intelligent Router Options dialog box, click the **Advanced** tab, and then select the MAPI profile from the list.

Figure 9: Intelligent Router Options Dialog Box, Advanced Tab



Logging

In some instances, support personnel may ask you to enable logging for further fact finding. Use these settings to configure logging. It is NOT advised to enable logging during normal operation.

□ Enable basic logging
□ Enable packet dumping
□ Enable network logging
□ Enable packet recording

Miscellaneous

Call Model Dump — Click here to write the current call model to a log file.

Delete Log Files — Click here to delete all current log files.

MAPI Profile

Select the profile to use for all Send E-Mail (Via MAPI) actions:

CALLVIEWER

CallViewer is a software product that provides telephony call control, screen popping, and desktop automation on a Windows-based computer. This application makes extensive use of Caller ID and *Dialed Number Identification Service* (DNIS).

CallViewer will not run correctly until Windows Networking services and protocols are appropriately configured for your LAN and the current MiCC Office Server. This should be done before you install CallViewer.

Note: For ease of use, the term CallViewer is used throughout this section instead of CallViewer/Connection Assistant/Client Go.

COMPONENTS

CallViewer consists of the following components:

- **Look and Feel**: CallViewer provides four "look and feel" options (Legacy, Executive Display, Quick Connect, and Handset) which allow users to choose the way CallViewer appears and which features it includes.
- **User Buttons**: The user can create and edit buttons in the button area. Buttons can be created to perform a variety of tasks using CallViewer's actions. Buttons can be assigned images or text, to allow the user to easily understand the function of buttons that they create.
- **Feature Buttons**: Similar to User Buttons, a feature button is a button that already exists on the client window, but whose functionality you can alter. This allows you to change standard features of the software to adapt to the way you prefer to work. There are also several blank feature buttons available in "feature sets," to provide additional buttons.
- **Built-in Actions**: There are many actions built in to CallViewer to perform common tasks easily, including calling a specific number, transferring a call to voice mail, setting your forward state, etc. These actions are easily configured from the user interface.
- **Hot Keys**: You can create hot keys to perform specific actions, or assign hot keys to buttons that they have created. You can access your preferred actions either just through a hot key, or through a button, or both.
- **Rules**: You can create rules that will fire when specific types of call or telephony events occur at their extension, such as transferring callers to reception if they have not provided Caller ID. Rules.
- **Ready To Go Solutions**: Ready To Go solutions provide integration between CallViewer and several common contact management systems. Configuring a Ready To Go will enable you to screen pop contacts in your contact management system, as well as dial contacts directly from the system. You can also have several instances of the same or different Ready To Go solutions, as well as being able to easily configure your installed solutions.
- **Tray Icon**: CallViewer adds an icon to the Windows tray to indicate the current status of CallViewer, as well as provide access to the main menu and a quick call control menu. The main menu allows you to configure several aspects of CallViewer, including the user's buttons, hot keys, and rules.

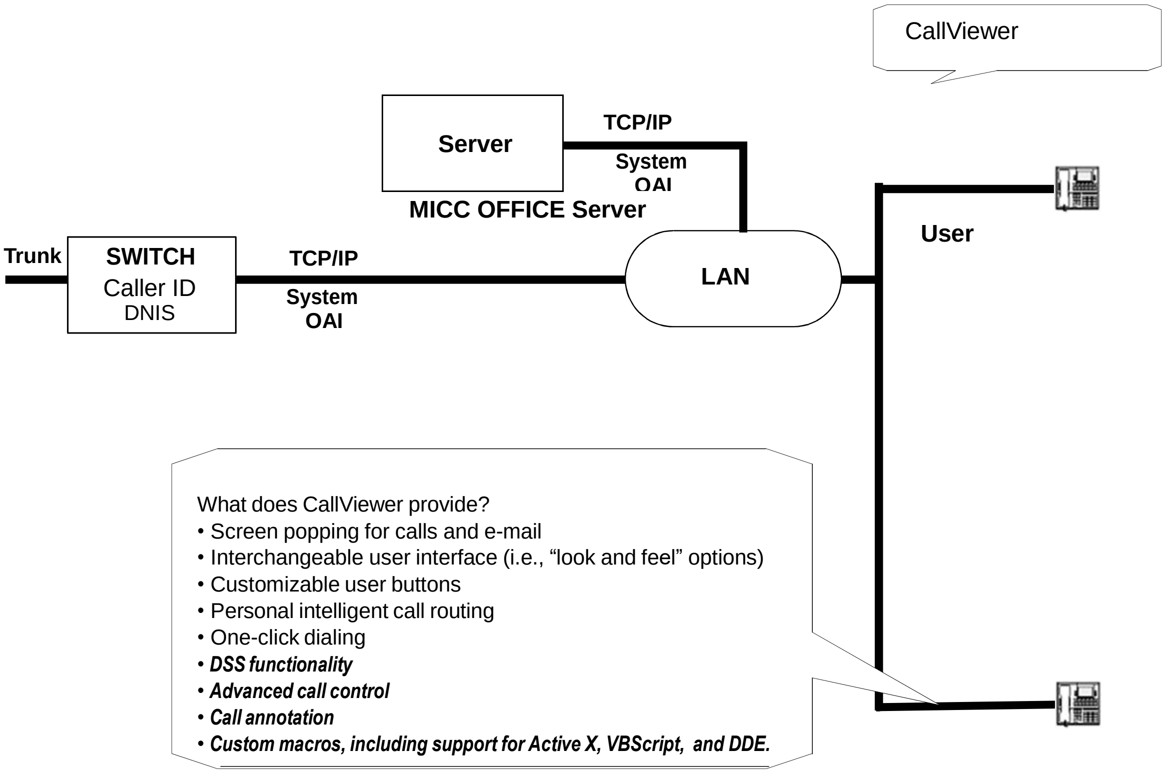
  - **Main Window**: Each look in CallViewer has a main window, which provides the core functionality of that "look," which allows you to access other windows, and provides some common call control functionality.

- **Active Call List**: Several “looks” have an active call list window, which displays a list of calls currently active or on hold at your device. The active call list can be used to perform call control on these calls, or view information about the call.
- **Call History**: Each look has a call history window that replaces the Personal Call Logger from version 3.x. The call history window displays information on recently received or dialed calls, as well as routed media. The call history can be configured to show only the information that you are interested in seeing.
- **Dial Pad**: Several “looks” have a dial pad window that allows the user to dial telephone numbers in a similar fashion to using a standard telephone. There is also a recent dial list showing the last 20 numbers the user made calls to, or received calls from.

USING CALLVIEWER

A CallViewer user has a networked PC connected to the Server, and a telephone connected to the company telephone system. When the user makes outbound calls or receives inbound calls, the dialed number or the Caller ID of the caller, along with other pertinent customer information, appears in the CallViewer user interface. This enables the user to see information about the caller before answering. CallViewer can also “screen pop” the customer information in the company database, allowing the user to save time locating the relevant information.

Figure 11: CallViewer Deployment



What does CallViewer provide?

- Screen popping for calls and e-mail
- Interchangeable user interface (i.e., “look and feel” options)
- Customizable user buttons
- Personal intelligent call routing
- One-click dialing
- ***DSS functionality***
- ***Advanced call control***
- ***Call annotation***
- ***Custom macros, including support for Active X, VBScript, and DDE.***

CallViewer features include:

- **Media Blending**: When an agent is routed an e-mail by Intelligent Router, the e-mail originator's details appear in MiContact Center Office just like a received call. You can also use the Microsoft Outlook integration to better respond to routed media, as well as provide annotations to the e-mail representation in CallViewer, just like they would with a call. See Intelligent Router online Help for details on how Media Blending works.
- **Enhanced User Interface**: CallViewer has been updated to provide enhanced user functionality and customization. You can now choose a “Look and Feel” for the application interface. Each option is highly configurable, allowing you to modify the interface to suit your call handling needs and requirements. Such features as DSS buttons, integrated call logger, personal call router, and advanced call control functions improve your call handling capabilities and performance.
- **Agent Help Support**: The agent-help functionality allows managers to monitor and react to the support needs of their staff in real time when faced with a difficult call that requires the assistance of a manager.
- **DSS Buttons**: DSS buttons allow you to quickly see the call status of your colleagues to determine whether they are on a call, unavailable or free. You can customize the buttons to see more information about a particular extension, including the identity of the caller they

are connected to and their current DND status. DSS buttons can also be used to perform call control operations, such as transferring or picking up calls, for the extensions being monitored.

- **Integrated Call History**: The Personal Call Logger application in Customer Service Manager version 3 has been replaced in version 4 with an integrated call history. The call history provides a personal list of calls that have been made or received – both internally and externally – from your extension. In addition, the call logger also displays e-mail messages that have been routed to you via Media Blending.
- **Integrated Call Management**: CallViewer includes an integrated call management system that allows you to control how calls to and from your extension are handled by using easy-to-configure rules and actions. For example, you may create rules to:
    - Redirect calls without Caller ID to an attendant to avoid unwanted calls
    - Play notification sounds when certain conditions are met, e.g., when an important client or business partner calls
    - Set the destination for calls when you leave at the end of the day
- **Enhanced Call Annotation**: Enhanced call annotation capabilities, allowing you to attach call annotations to routed calls. For example, when you have a call that needs to be transferred to a second party for further information, you can now attach an annotation to the call, giving details of the initial conversation, before transferring it. The annotation is automatically displayed for the second party with the forwarded call, allowing them to review details of the initial conversation before answering the call. Annotations can help you to respond to calls and improve customer service.
- **Tray Bar Call Control**: The CallViewer configuration menu and common call control functions, such as Go Dial, Answer, Release, Hold / Retrieve, and Transfer / Redirect, are available from the main Windows tray bar.

STARTING CALLVIEWER

To start CallViewer, do one of the following:

- Double-click the CallViewer icon on the desktop.
- From the Start menu, select All Programs – **Mitel MiContact Center Office**, and then select **CallViewer**.

When CallViewer starts, if the Network Settings have not been configured or have not been configured correctly, Startup Wizard begins. You can use the **Network Settings** dialog box to change CallViewer's network settings after installation.

MiCC Office provides three levels of passwords:

- **Administrator**: This is the highest level of password. Anyone who has this password can configure the Server, as well as have full access to all features in all modules.
- **Supervisor**: This password level has restricted access to software features, such as not being able to control what device the Client is associated with.
- **User**: This password level has further restricted access to software features, such as not being able to create actions.

CallViewer features can be limited by specifying passwords on the Server. If the Server has all password levels set, you will need to enter a password to access CallViewer when you connect to such a Server. If some password levels are not set, CallViewer will default your access to the highest unsecured password level; on an unsecured Server, this automatically makes any user an administrator.

CONFIGURING CALLVIEWER WITH STARTUP WIZARD

When you launch CallViewer for the first time, the Startup Wizard helps you configure various common options step-by-step.

> **Note:** If you want to run the startup wizard at a later time, right-click the CallViewer tray icon(☎) and select **Startup Wizard**.

The following screens display during setup:

- **Welcome Page**: This page begins a sequence of Startup Wizard pages used to collect some configuration defaults for the software.
- **Devices Page**: Enter the extension number and the voice mail number used for this installation of CallViewer. The devices can be changed later using the Options dialog, on the **Devices** tab.
- **Enter the name of the MICC OFFICE Server you want CallViewer to connect to**: Choose one server option from the following choices:
  - *Run in simulation mode*: When enabled, no connection is made to a MiCC Office Server and the software runs in simulation mode. Enable this option when you need to simulate calls to test macros that you have written.

    > **Note:** Simulation mode is only used with the MiContact Center Office Developer SDK when creating user-defined actions.

  - *Connect to this MiCC Office Server*: When enabled, CallViewer uses the server that you specify in the text box below this option. This is the default option when information is available for the server connection.
- **Look and Feel Page**: Choose which look you prefer for CallViewer from the drop-down list. For each selection, you see a sample picture and a description of the features included. The following example shows the Executive Display.

  > **Note:** You can change to another “Look and Feel” selection at a later time if you choose. Refer to the CallViewer online Help for details.

- **Ready To Go Page**: Select and configure a Ready To Go solution so that you can quickly access another application from within CallViewer. The following example shows the Ready To Go Solutions choices.

If you choose to install a solution, you can determine when CallViewer screen pops the database, using the following options:

- **Automatically screen pop when call is answered**: *When enabled*, the chosen database screen pops when a call is answered at the CallViewer extension. *When disabled*, the chosen database screen pops when a call starts to alert.

> **Note:** The application you intend to use for screen popping must be open while you are using screen popping from CallViewer. For example, to screen pop Outlook, it must be running on the PC where CallViewer is being used.

- **Screen pop application for…**: Choose inbound calls, outbound calls, or both inbound and outbound calls. Inbound calls will also screen pop routed e-mail messages.

You do not need to set up the Ready To Go (RTG) options using the Startup Wizard. You can also create a Ready To Go action when defining a new rule or button. You can also edit the settings of a Ready To Go solution created using the Startup Wizard using the Action Manager.

- **Dial Rules Page**: The dial rules affect how a number is altered before being passed to the MiCC Office Server to be dialed. Choose one of the following options:
  - *Calculate dial rules via CallViewer MiCC Office Server*: When enabled, all dial rules are calculated at the MiCC Office Server using previously configured options. This is the default setting.
  - *Specify dial rules for this installation*: When enabled, all dial rules are calculated by CallViewer using rules configured here or from the Options feature. To support canonical format dialing (i.e., the format that Outlook uses to store numbers), you need to use local rules that are correctly configured. Then you can dial numbers in the form “+country (area) number,” for example, “+44 1293 608200.”

    The dial rules configuration includes tabs for General, Local, Long Distance, and International settings. Each tab contains a “test” section) so you can try out the settings before finishing the configuration.

    To set the dial rules, complete the following steps:

1. On the **General** tab, program the *Outbound Dial Prefix*, which is the number you need to dial to reach an outside line, for example, 8 or 9. This information is critical for external outbound dialing.
2. On the **Local** tab, program the following:
    - *Local area code:* Enter your area code (e.g., 480).
    - *Local toll calls:* Enter any prefixes, within your area code, that may require the long distance code. You can enter partial prefixes to indicate a range (e.g., 8 would indicate 800-899).
   - *Always dial the local area code on local calls*: When enabled, the local area code is always prefixed to the number being dialed, when dialing a local number.
     - *The local area code is prefixed with '0' for non-international calls:* When enabled, this setting will prefix the local area code being dialed with a “0” for non-international calls entered using canonical format. For example, a UK number such as 01293 608200 would be entered in canonical form as +44 1293 608200, and would be dialed as such from a non-UK country, but in the UK the “0” needs to be prefixed to the local area code, and so this setting would need to be enabled. This setting only takes effect when dialing numbers in canonical form.

3. On the **Long Distance** tab, program the following:
   - *Long distance code:* Enter the code required to dial outside your area code (e.g., 1 for the US).
   - *Don't dial long distance code:* Enter a comma-separated list of area codes that do not require the long distance code.
4. On the **International** tab, program the following:
   - *International dial code:* Enter your international dial code (e.g., 011 for the US).
   - *Country code:* Enter the country code where you are calling from, e.g., "44" for UK, "1" for US.
   - *Replace '+' with international* dialing *code:* When enabled, a '+' in the number to be dialed is changed to the international dialing code the caller enters.

The Test section appears on each tab, and contains a **Sample telephone number** text box where you can type digits to test. As you type the number to test, the **Actual number dialed** field updates as you type, to reflect the number that would be dialed by CallViewer.

Click **Test** to apply the dial rules to the sample telephone number and produce a result in the Actual number dialed display. The type of call (internal, local, long distance, or international) is also displayed to help you determine which rule you may need to adjust for correct dialing.

Note: The Actual Number Dialed area is for display only; you cannot edit the contents.

- **Import Your Previous Configurations Page**: This page appears only if you are upgrading from an earlier release of CallViewer (version 3.x or before), if legacy macro files or hot key settings are detected, and there are no current actions or hot keys defined for the current installation.

If you have existing Ready To Go (RTG) macros in use in CallViewer, you should **NOT** upgrade your old macros and buttons, but instead recreate them with the new Ready To Go integrations. This also applies to automatic macros, which are now defined by rules. If you have existing RTGs in use, but also have other macros, you may want to perform the upgrade, but then delete the RTGs and recreate then using the new versions.

The import page contains the following options:

- **Import existing button macros***:* This option is enabled if existing macro files from an earlier release are installed on this computer. When enabled, upon successful completion of the Wizard, the Wizard imports the existing button macros as new actions bound to new buttons.
- **Import existing automatic macros***:* This option is enabled if the previous option is enabled. When enabled, upon successful completion of the Wizard, the Wizard imports the existing automatic macros as new actions bound to new rules.

Import existing hot keys*:* This option is enabled if existing hot keys from an earlier release are configured and enabled on this computer. When enabled, upon successful completion of the Wizard, the Wizard imports the existing hot keys as new hot keys in this installation.

- **Finished Page**: To complete the CallViewer configuration, click **Finish** in the Startup Wizard.

To automatically configure the Server, click **Auto Configure**. The product will automatically attempt to find a MiCC Office Server on the network. After the Server has found a MiCC Office Server, and the information in this screen is updated, click **OK** to exit this screen and save the changes. To cancel unwanted changes, click **Cancel**.

When you are finished configuring the network settings, click **OK** to save your changes. To cancel unwanted changes, click **Cancel**.

REALVIEWER

RealViewer is an application that shows real-time call statistics, enabling you to see current details against all or selected call criteria on the telephone system.

RealViewer requires an available license. If a RealViewer license is not available, Call Summary, which does not support custom filters and certain statistics, is invoked.

REALVIEWER VS. CALL SUMMARY

Like RealViewer, Call Summary displays Deskboard tiles with real-time call statistics. Unlike RealViewer, however, Call Summary does not support custom filters. In addition, Call Summary supports only a limited number of statistics. All tiles in Call Summary use the All Calls filter, which cannot be edited or deleted.

Call Summary is automatically installed as a component of RealViewer and is initiated if a RealViewer license is not consumed (e.g., a license is not available). If the application title bar indicates Call Summary, but you have RealViewer installed, there are no available RealViewer licenses.

If you request a RealViewer license and one is not available, you are given the option to permanently use a Call Summary license.

Note: Unless specified otherwise, the information in this chapter applies to both Call Summary and RealViewer.

REALVIEWER BASICS

Before you can begin using the product, you should understand the following basic concepts:

- **Statistics**: Everything displays as a statistic, whether this is the number of a given trunk line, the number of inbound calls answered by a given agent, or the total talk time accumulated so far today for every device.
- **Filters**: RealViewer lets you limit the data you view based on filters. These enable you to display statistics for a list of extensions from a particular group. Or, you can change a particular statistic so that it only applies to certain calls, such as calls that rang longer than a specified time, outbound calls, abandoned calls, etc.
- **Tiles**: A tile is the user interface element that displays a single statistic. Filters are applied to these tiles to limit the information it considers when calculating the statistic. Several tiles can be displayed at a time, each with their own filters.
- **Alarms**: Alarms alert you when a statistic falls within a given range (e.g., when there are more than *n* number of calls in the queue). These are applied to tiles based on the associated statistic and can be configured to flash the associated tile, play a sound, write a message to an alarm log, and/or activate the alarmed tile.
- **Global Options**: There are also several global options, such as the Short Call Level, which will affect all statistics of a particular type.

- **Call Summary**: If no RealViewer licenses are available or if you do not want to consume a license, Call Summary is initiated. Call Summary provides the basic functionality of RealViewer but does not support custom filters. In addition, the number of available statistics is limited in Call Summary.

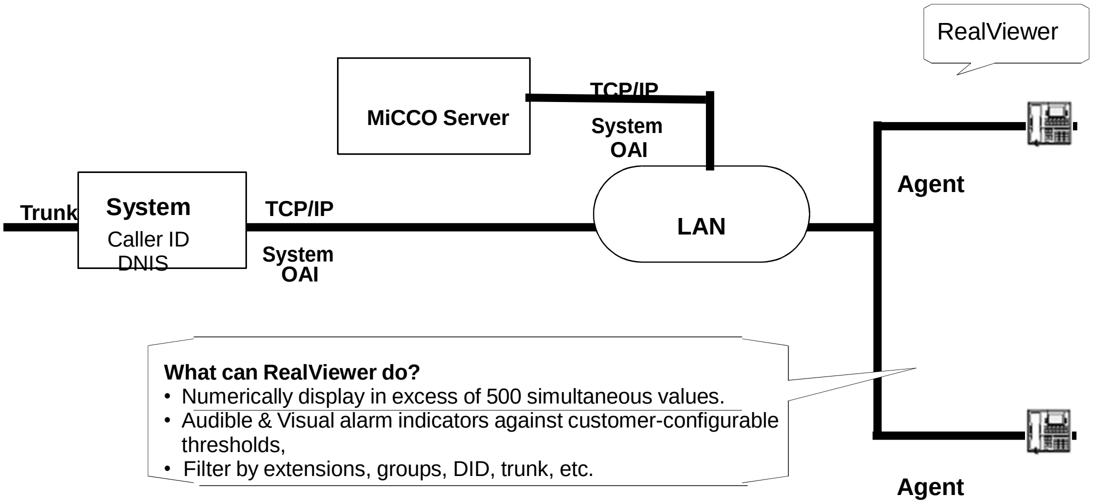
Each of these areas plays an important role in how RealViewer calculates and displays call information.

USING REALVIEWER

Using RealViewer, you can view statistics, such as the Longest Waiting Inbound Call Today, either across the telephone system, for a group of extensions, or for a particular event. You can also view the number of agents currently in the busy state, for example, or the number of inbound calls currently waiting to be answered. In addition, you can filter information based on group, DID number, telephone number, etc.

RealViewer supports internal call modeling and media blending. With media blending, e-mail messages can be routed, handled, and filtered just like calls.

Figure 12: RealViewer Deployment



What can RealViewer do?
- Numerically display in excess of 500 simultaneous values.
- Audible & Visual alarm indicators against customer-configurable thresholds,
- Filter by extensions, groups, DID, trunk, etc.

The following features are included with RealViewer:

- **Tile Statistics**: To support the addition of internal call modeling and advanced media blending, RealViewer includes over 180 updated statistics and over 130 new statistics that can be used to configure tiles, as shown in the example below. To see a full list of the statistics that are available, refer to RealViewer online Help.
- **Filter Options**: You can also filter tiles using several new filter settings including:
  - Select media from external, internal or a routed e-mail
  - Call transferred from agent

- Call transferred to agent
- Call annotation
- E-mail Subject
- Agent Help

STARTING REALVIEWER

To start RealViewer, do one of the following:

- Double-click the RealViewer icon on the desktop.
- From the Start menu, select All Programs – **Mitel MiContact Center Office**, and then select **RealViewer**.

When the product starts, if the Network Settings have not been configured yet or have not been configured correctly, Startup Wizard attempts to automatically find a Server on your LAN using a self-configuration mode.

CONFIGURING REALVIEWER WITH STARTUP WIZARD

RealViewer will not run correctly until the application has been appropriately set up for the current network and Server configuration.

If this is the first time RealViewer has been run after installation, the RealViewer Startup Wizard runs. The Startup Wizard is not run for Call Summary installations.

The wizard will help you locate a MiCC Office Server if one cannot be found, and it will ask you some simple questions to help create a default RealViewer screen.

When using the RealViewer Wizard, you can navigate by using the following buttons:

- **Next**: Advances you to the next screen.
- **Back**: Returns you to the previous screen.
- **Cancel**: Stops the Wizard and returns you to the main screen. If the Wizard was invoked due to missing settings, clicking Cancel will close RealViewer completely.
- **Help**: Displays the online Help information for that screen.

The following screens are displayed during setup:

- **Welcome Page**: This page begins a sequence of Startup Wizard pages that is used to collect some configuration defaults for the software. Click **Next** to continue.

- **Search for MiCC Office Server**: Choose from one of the options below, and click **Next**.
  - **Network Settings**: This is the default choice if RealViewer finds existing settings in the registry for a server to which to connect. The existing settings will remain unchanged.
  - **Connect to this Server**: Select this option to use the server that you specify in the text box below this option.

- **RealViewer Style:** This page allows you to choose the style of RealViewer screen that you would like to create.

REPORTER

Reporter Basic, Reporter, and Reporter Pro are used to run historical reports on call, e-mail, and agent activity information, which is stored within a database on the MiCC Office Server. These reports can be run by specifying various criteria (e.g., reports can be filtered by Caller ID, DID number, trunk line, extension or agent groups, time, date, call cost, etc.).

The following features are available in Reporter:

- **Report Statistics**: To support the addition of internal call modeling and advanced media blending, Reporter includes over 170 updated statistics and over 90 new reporting statistics for configuring reports. Depending on the license used, these include:
  - Call / E-mail List Statistics
  - % Of Call / E-mail Total Statistics
  - Historic Routing Statistics
  - Agent Statistics

  To see a full list of the new statistics that are available, refer to Reporter online Help.
- **Report Filters**: In addition to updated call statistics, you can also filter reports by several new filter settings, including:
  - Whether media is external, internal or routed e-mail
  - Call transferred from agent
  - Call transferred to agent
  - Call annotation
  - E-mail Subject
- **Report Templates**: The following report templates for Media Blending statistics include:
  - E-mail List, General
  - E-mails by Domain
  - E-mails by Half Hour
  - E-mail Summary by Day / Week / Month
  - E-mails by Hunt Group
  - E-mails by Agent
  - E-mails by Talk Time
- **DND Status Reporting**: Reporter Pro supports advanced Do-Not-Disturb (DND) status reporting, allowing managers to monitor how much time their staff are spending on non-telephone based activities. DND reporting is available by extension or agent, both historically and in real time.

When Reporter or Reporter Pro is installed on a computer, Reporter Real-Time, which provides real-time call and agent reporting, is also installed (see “Reporter Real-Time” on page 65). Reporter also include the Auto Reporter application (see “Auto Reporter” on page 63).

AUTO REPORTER

To access the Auto Reporter configuration window, do one of the following:

- Click the Auto Reporter button ( ) on the main toolbar.
- Press the F8 key on your keyboard.

Auto Reporter provides the following options:

- **Report Schedules**: Allows you to configure report schedules. This displays the main window.
- **Sites**: Allows you to add and edit sites.
- **Events**: Allows you to see the results of recently scheduled reports.

The Auto Reporter component provides the following features:

- **Scheduled Reporting**: Allows you to schedule reports to be run at intervals ranging from every 15 minutes to once a month. Reports can be automatically displayed, printed, exported, publish to the Internet, or e-mailed.
- **Batch Reporting**: Allows you to batch several reports together and perform the same action on all reports at once. For example, you can print your monthly reports all at the same time or publish key reports to the Internet every day.
- **Report Publishing**: Allows you to manually or automatically publish your reports to the Internet for viewing in a Web browser or on a WAP-enabled device. Your reports can be accessible no matter where you are.
- **E-Mailing Reports**: Allows you to e-mail exported reports to your colleagues either automatically or at the touch of a button.

To successfully publish reports and statistics, you need access to a Web server. For this server, you can use a company Web server, your own PC, or even an Internet Service Provider (ISP). While this document will cover some of the various Web server configurations, be careful. An invalid Web server configuration can result in a non-functional Web server.

Note: Consult your system administrator or Web site administrator before you configure Auto Reporter. If possible, it is recommended that your system administrator or Web site administrator assist you in the configuration process.

STARTING REPORTER

To start Reporter, do one of the following:

- Double-click the **Reporter** icon on the desktop.

From the Start menu, select All Programs – **Mitel MiContact Center Office**, and then select **Reporter**.

When the product starts, if the network settings have not been configured yet or have not been configured correctly, a self-configuration mode will be invoked to attempt to automatically find a MICC OFFICE Server on your LAN.

CONFIGURING REPORTER WITH STARTUP WIZARD

Reporter will not run correctly until the application has been appropriately set-up for the current network and MiCC Office Server configuration.

If this is the first time Reporter has been run after installation, Reporter will ask for the following options to be configured:

- **Welcome**: Click **Next** to begin the installation.
- **Search for MiCC Office Server**: Choose from one of the options below, and click **Next**.
  - *Network Settings*. This is the default choice if Reporter finds existing settings in the registry for a server to which to connect. The existing settings will remain unchanged.
  - *Connect to this MiCC Office Server*: Select this option to use the server that you specify in the text box below this option.
- **Call Costing Page**: Enter all the local dial codes for your area, separating each with a comma. Click Next.

  Note: The call costing functionality provided by Reporter is based on limited information provided by Telcos. Additionally, carriers can update their tariffs at any time. For this reason, changes in tariffs or network carrier discounts cannot always be reflected.

- **Report Upgrade Page**: Select one of the following options:
  - *Upgrade reports to process external and internal calls*: If displayed, select this option to use the report filter option “Only process calls (external and internal)” for all existing reports from an earlier Reporter installation. Choosing this option excludes e-mail messages from the upgraded reports, however, you can create additional reports that include e-mail messages.
  - *Upgrade reports to process external calls only:* Select this option to use the report filter option “Only process external (trunk) calls” for all existing reports from an earlier Reporter installation. Choosing this option effectively maintains the functionality of the previous version reports, because version 3.x reports only considered external calls.
  - *Do not upgrade reports*: Select this option to leave the reports as they were in the previous version (i.e., do not apply any of the filtering capability that is new to v4.1). Choosing this option causes the upgraded reports to take into account e-mail messages and internal calls.

  Note: This option causes reports to include all media types, however, it will not change report names, so a report such as “Calls by Extension” will also process e-mail messages.

- **Auto Reporter Site**: This page appears only if a default site has not already been created, you have Internet Information Server (IIS) or Personal Web Server installed on your computer and the application detects it. This allows you to create an Auto Reporter site using the default settings.
- **Finished Page**: To complete the Reporter configuration, click **Finish** in the Startup Wizard.

You can modify these configurations at any time while running Reporter.

REPORTER REAL-TIME

Reporter Real-Time is an application that shows real-time external call and routed e-mail statistics, allowing you to see real-time details against all or selected call and e-mail criteria on the telephone system. Not only will it show the current extension, agent, and trunk activity, it will include detailed information such as the caller's identity, DID\DDI number used, etc.

With Reporter Real-Time, you can tell who is involved in a call or e-mail (including the distant end), how long the call/e-mail took to answer, and how long the call has been in progress. You can also add a Direct Station Selection (StationViewer) tile that allows you to monitor the current call activity of extensions and/or agents.

Although Reporter Real-Time is installed when you install Reporter, you need to have purchased the "Enhanced Reports/Reporter/Real-Time" Reporter module, which also enables Reporter type reports in Reporter, to use Reporter Real-Time. Reporter is a tool for building call reports from the call log database that the MiCC Office Server automatically produces.

To support internal call modeling and advanced media blending, Reporter Real-Time includes over 180 updated statistics and over 130 new statistics that can be used to configure tiles. To see a full list of the statistics that are available, refer to Reporter Real-Time online Help.

Reporter Real-Time provides the following features:

- **Filter Options**: You can also filter tiles using several new filter settings including:
  - Select media from external, internal or a routed e-mail
  - Call transferred from agent
  - Call transferred to agent
  - Call annotation
  - E-mail Subject
  - Agent Help
- **DSS Button Appearance**: You have great flexibility in configuring the appearance of DSS Buttons, including:
  - The size of the button
  - What information appears on the button
  - The colors used to display the button

Reporter Real-Time and Reporter have several different variations that are either enabled or disabled, based upon the software license that has been purchased by the end user.

STARTING REPORTER REAL-TIME

To start Reporter Real-Time, do one of the following:

1. Double-click the **Reporter Real-Time** icon on the desktop.
2. From the Start menu, select All Programs – **Mitel MiContact Center Office**, and then select **Reporter Real-Time**.

When the product starts, if the network settings have not been configured yet or have not been configured correctly, a self-configuration mode will be invoked to attempt to automatically find a MICC OFFICE Server on your LAN.

CONFIGURING REPORTER REAL-TIME WITH STARTUP WIZARD

If this is the first time Reporter Real-Time has been run after installation, Reporter Real-Time will invoke a configuration wizard containing the following pages:

- **Welcome to Reporter Real-Time**: This displays basic information about Reporter Real-Time and the configuration wizard. Click **Next** to continue.
- **Search for MiCC Office Server**: Choose one server option from the following choices and then click **Next**:
  - **Network Settings**: This option visible and is the default choice if Reporter Real-Time finds existing settings in the registry for a server to which to connect. Select this option if you want the existing settings to be left unchanged.
  - **Connect to this MiCC Office Server:** Select this option to use the server that you specify in the text box below this option. This is the default option when information is available for the server connection.
- **Extension for Call Control**: This page allows you to program the supervisor information. Enter the supervisor’s ***extension device number*** (not agent ID) and the supervisor’s Mailbox.
- **Finished**: This is the last page of the wizard. You can review your choices by using the **Next** and **Back** buttons. After you are satisfied with your selections, click **Finish**.

You can modify these configurations at any time while running Reporter Real-Time.

FILTERS

Filtering is a feature provided in Reporter, Reporter Pro, RealViewer, and Intelligent Router. This allows you to filter information based on different parameters, such as how long a call was active, what ACD hunt group the call rang, what DID number the call used to access the switch, etc. You can choose to filter calls by trunk or by device.

Filtering calls by device considers each individual device that a call is handled by, whereas filtering by trunk only considers each call once regardless of how many devices handled it. Filtering by device is often used to measure individual agents or extensions, while filtering by trunk is used to measure statistics against DID numbers or trunk lines, e.g., to measure the effectiveness of a marketing campaign. Further information can be found in the “Calculating Statistics by Device” on page 17 section.

Every report or tile is filtered by the All Calls filter by default. The All Calls filter does not exclude any calls when filtering, and cannot be edited or deleted.

In Reporter Real-Time and RealViewer, a filter can be applied to each tile, and the same filter can be applied to multiple tiles. In Reporter, a filter is applied to a report, and the same filter can be applied to multiple reports.

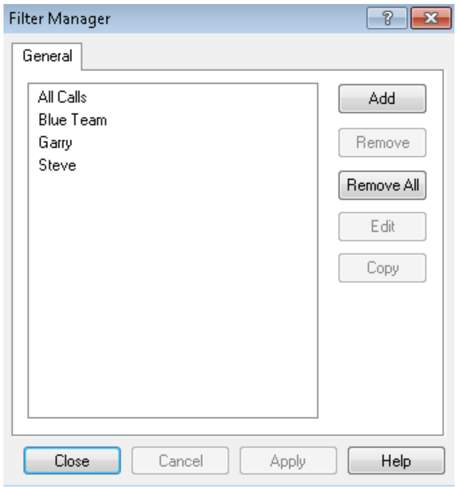
You can create as many filters as you require, limited only by available memory. You can also edit a filter after creating it, to immediately see the effects of the changes you make.

Note: In Reporter Real-Time and RealViewer, the greater the number of different filters that you apply to tiles increases the time it takes for the application to start.

The Filter Manager lists the currently available filters and provides access to programming options. To display the Filter Manager, do one of the following:

1. Click the Filter Manager button (⛛) on the toolbar.
2. Press **CTRL + F**.
3. Select **Filter Manager** from the main menu.

Figure 13: Filter Manager



If you have Administrator permission, you can add, remove, edit, and copy filters, using the buttons described below.

- **Add**: Displays the Add Filter dialog box so you can create a new filter. You can also add a filter by clicking the Filter button on a tile or report, and choosing **Add Filter**.
- **Remove**: Removes the currently selected filter. You are prompted for a confirmation before the filter is removed. If you remove a filter, any tiles or reports using that filter will default to the All Calls filter.
- **Remove All**: Deletes all filters listed except the All Calls filter. You are prompted for a confirmation before the filters are removed. If you remove all of the filters, any tiles or reports using those filters will default to the All Calls filter.
- **Edit**: Displays the Edit Filter dialog box so you can edit the selected filter. (You can also access the Edit Filter dialog box by double-clicking on the filter you want to edit).
- **Copy**: Copies the current filter and immediately includes it in the filter list. The name of the copied filter is the same as the original filter except it includes "(1)" after the name. For example, a copy of the Sales filter would result in Sales (1).

ADDING A FILTER

Filters allow you to limit the information provided by a statistic.

To add a new filter:

1. Open the Filter Manager, and click **Add**. Or, you can click the Filter button (⏷) in a tile or report caption and click **Add Filter**. The Add New Filter screen appears.
2. Select the tab corresponding to the information you want to use as the filtering parameters, and program the information. Tabs include:

- General (see "General" on page 44)
- Call Route (see "Call Route" on page 46)
- ACD Hunt Groups (see "ACD Hunt Groups" on page 47)
- Direction & DID (see "Direction and DID" on page 48)
- Duration (see "Duration" on page 50)
- Call Status (see "Call Status" on page 52)
- Information (see "Information" on page 53)
- Transferred Calls (see "Transferred Calls" on page 55)
- Miscellaneous (see "Miscellaneous" on page 56)

Note: Any of the text-based fields can accept wild cards (e.g., "`*@Mitel.com`") or comma separated lists (e.g., "200-204,207,209") to define the extensions, groups, or agents you want to include in the filter. The list you enter can include ranges or individual extension items wherever you can specify a device. For example, if you entered "200-204,207,209," the filter would include extensions 200, 201, 202, 203, 204, 207, and 209. You may not enter "abc-def" for a device field range because letters are not valid in that context. You can also use the drop-down list to select extensions or agents, which are intelligently added to or removed from the list.

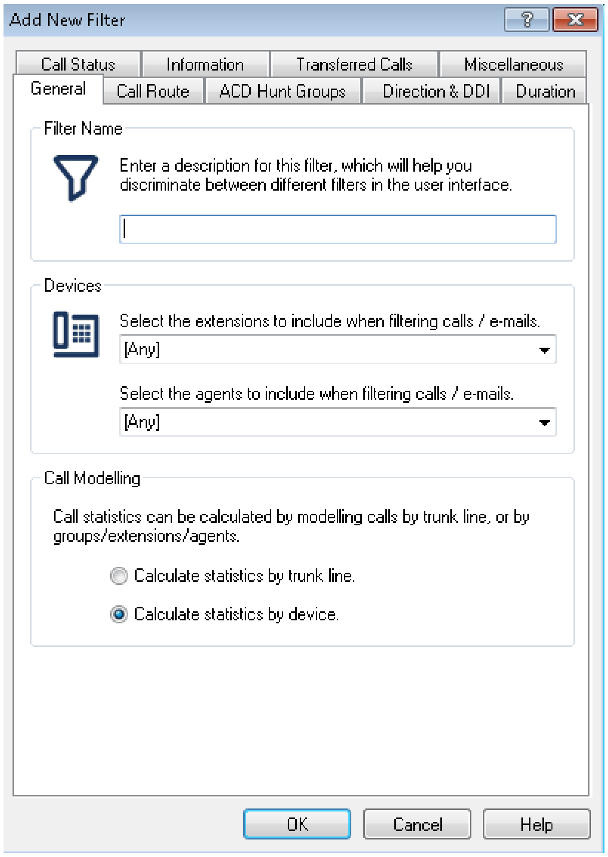
3. Click **OK** when finished, or click **Cancel** to exit without saving changes. If you added a filter through the Filter Manager, you are returned to the Filter Manager screen. If you added a

filter using the tile or report buttons, you are returned to the main application window.

GENERAL

The **General** tab allows you to create a filter for calls on certain extensions or agent devices.

Figure 14: Add New Filter: General Tab



Filter Name

Enter a description for this filter, which will help you discriminate between different filters in the user interface.

Devices

Select the extensions to include when filtering calls / e-mails.

[Any]

Select the agents to include when filtering calls / e-mails.

[Any]

Call Modelling

Call statistics can be calculated by modelling calls by trunk line, or by groups/extensions/agents.

○ Calculate statistics by trunk line.

● Calculate statistics by device.

This tab includes the following fields:

- **Filter Name**: Type a unique description of the filter. This will be displayed in the Filter Manager and on any tile's caption that uses the filter. The description should provide enough information so you can easily identify what the filter displays.

  > **Note:** A filter and a rule cannot have the same name. This includes putting spaces before or after an existing rule name. For example, you cannot have "check email" as a rule and "<*space*>check email" as a filter.

- **Extensions to filter on**: Type a comma-separated list of extensions to include in the filter. Any calls that ring, are answered, or terminate at one of these extensions will be included in the filter. You can use such a filter to apply to an extension list tile to define which extensions you want to see.
- **Agents to filter on**: Type a comma-separated list of agents to include in the filter. Any calls that ring, are answered, or terminate at one of these agents will be included in the filter. You can use such a filter to apply to an extension list tile to define which agents you want to see.

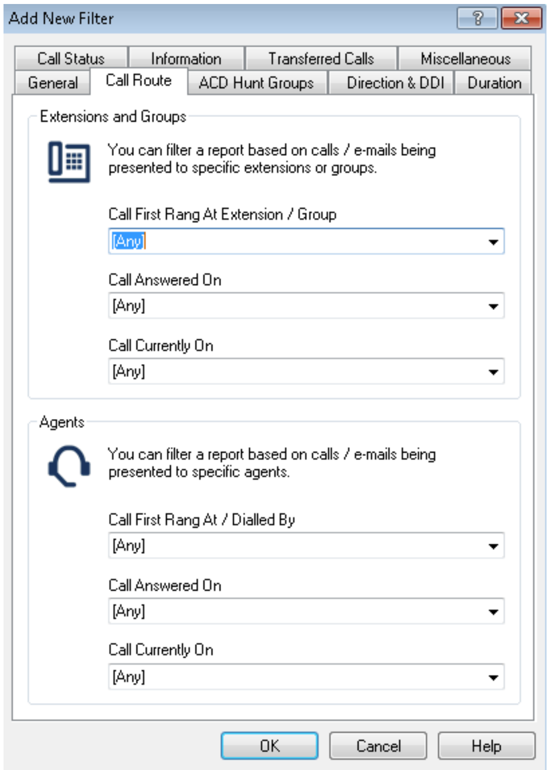
- **Calculate statistics by trunk line**: Calculates statistics by modeling calls on the trunk line where the call was active, ignoring transferred calls in the calculation. For example, a call that rang at group 1001, was answered at 210, and transferred to group 10001 would be considered one call. Select this option when you want to know the actual call traffic entering the phone system from the telephone company (e.g., to measure how many calls have originated through DID numbers or from different sets of trunk lines). In Reporter this is disabled, and is defined on the **Filter** tab of the report's properties. In Reporter, the defaults depend on the type of report you are creating, whereas in other modules the defaults are by device, and you should change it if the information you want is more trunk-related.

- **Calculate statistics by device**: Calculates statistics by modeling calls on devices (extensions, agents, or hunt groups) on which the call was active, including transferred calls in the calculation. For example, a call that rang at group 1000, was answered at 210, and transferred to group 1001 would be considered two calls: one that initially rang 1000 and one that rang 1001. Select this option if you want to measure the number of calls that alerted a particular hunt group or extension. In Reporter this is disabled, and is defined on the **Filter** tab of the report's properties. In Reporter, the defaults depend on the type of report you are creating, whereas in other modules the defaults are by device, and you should change it if the information you want is more trunk-related.

CALL ROUTE

The **Call Route** tab allows you to filter calls and e-mail messages based on the route that the call or e-mail took through the system, including where it first alerted, and where it was completed.

Figure 15: Add New Filter: Call Route Tab



You can filter a report based on calls / e-mails being presented to specific extensions or groups.

Call First Rang At Extension / Group: [Any]

Call Answered On: [Any]

Call Currently On: [Any]

You can filter a report based on calls / e-mails being presented to specific agents.

Call First Rang At / Dialled By: [Any]

Call Answered On: [Any]

Call Currently On: [Any]

The **Call Route** tab includes fields which are defined for extensions or agents as follows:

Extension Fields

- **Call First Rang At Extension/Group**: Includes any calls that rang at an extension or group specified in the list. Enter a comma-separated list of extensions to include in the filter or use the drop-down list. If you want to measure call-based statistics for a hunt group, enter the hunt group number (or numbers) in this field.
- **Call Answered On**: Includes any calls that are answered at an extension specified in the list. Enter a comma-separated list of extensions to include in the filter or use the drop-down list.
- **Call Currently On/Call Finished On**: Includes any calls that are currently on or that were finished at an extension specified in the list. Enter a comma-separated list of extensions to include in the filter.

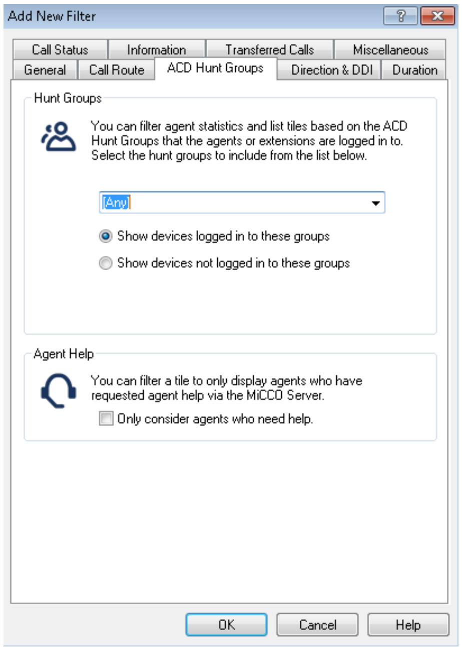
Agent Fields

- **Call First Rang At/Dialed By**: This agent-related field includes any calls that rang at or were dialed by an agent specified in the list. Enter a comma-separated list of agents to include in the filter or use the drop-down list. Agents will be in this field only if they were called directly (e.g., a call transferred directly to them), or if they initiated an outbound call.
- **Call Answered On/Call Answered By**: This agent-related field includes any calls that are answered at an agent specified in the list (see the previous Call Answered On/Call Finished On information for details).
- **Call Currently On/Call Finished By**: This agent-related field includes any calls that are currently on or that were finished by an agent specified in the list (see the previous Call Currently On information for details).

ACD HUNT GROUPS

The **ACD Hunt Groups** tab allows you to filter an agent list to display only agents logged in or out of specific hunt groups, and allows you to filter agent statistics, for example, Time In Busy or Total Time on Duty, for particular groups.

Figure 16: Add New Filter: ACD Hunt Groups Tab



You can filter agent statistics and list tiles based on the ACD Hunt Groups that the agents or extensions are logged in to. Select the hunt groups to include from the list below.

(Any)

● Show devices logged in to these groups

○ Show devices not logged in to these groups

You can filter a tile to only display agents who have requested agent help via the MiCCO Server.

☐ Only consider agents who need help.

The options on the **ACD Hunt Groups** tab are not designed to filter call information, only agent state information. It also can be used to filter agents in an agent list, based on which groups they are logged in to. If you specify only ACD hunt groups for a filter, it will produce the same result as applying the All Calls filter to a tile showing call statistics.

In CallViewer agents can indicate that they require help using the Agent Help LED. The agent is highlighted on the agent list tile so that the supervisor can quickly identify who is requesting help. Using the Agent Help section of this tab, you can also create a filter to only consider agents who currently require help.

Note: If you want to create a filter for call-based statistics, e.g., Calls In, Calls Answered, etc., you should also enter the list of hunt groups on the **Call First Rang At** field on the Call Route page.

- **Hunt Groups**: Enter the ACD Hunt Groups to which the list will be restricted. Enter a comma-separated list of hunt groups to include in the filter or use the drop-down list to select and clear hunt groups.
- **Show Devices Logged In To These Groups**: Select this option to display only agents who are logged into the selected hunt groups in the list. This option applies only to what appears in an agent list to which this filter is applied.
- **Show Devices Not Logged In To These Groups**: Select this option to display only agents who are not logged into the selected hunt groups in the list. This option applies only to what appears in an agent list to which this filter is applied.

✓ If you want to see agents in an agent list regardless of whether they are logged in or logged out of a group, use the Agents field on the **General** tab to list the agents who can log in to the necessary groups.

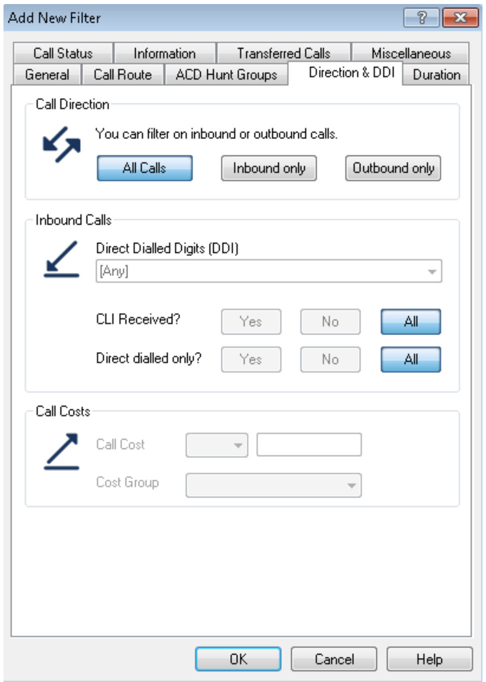
- **Only consider agents who need help** (RealViewer, Intelligent Router, and Reporter Real-Time only): When this option is selected, only agents who currently have enabled their agent help LED in CallViewer will be considered. When this option is not selected, agents are considered regardless of their agent help LED status.

Note: This setting does not apply to any agent help functionality provided by the telephone system.

DIRECTION AND DID

The **Direction and DID** tab allows you to filter calls based on whether they are inbound or outbound and the DID number used for inbound calls.

Figure 17: Add New Filter: Direction & DID Tab



You can filter on inbound or outbound calls.

Direct Dialled Digits (DDI): [Any]

CLI Received? Yes No All

Direct dialled only? Yes No All

This tab contains the following fields:

- **Filter Inbound/Outbound**: Click **All Calls** to include calls regardless of their direction in the filter. Click **Inbound only** to only include inbound calls in the filter. When this is clicked, the Inbound Calls section will be enabled so that you can specify further information on inbound calls to include in the filter. Click **Outbound only** to only include outbound calls in the filter.
- **Direct Inward Dialing (DID)**: Enter a comma-separated list of DID numbers to include in the filter. Any calls that are presented to a DID number in this list will be included in the filter.
- **Caller ID Received?**: Click **Yes** to only include calls where the Caller ID number is received. Click **No** to only include calls where the Caller ID number is not received. Click **All** to include calls regardless of whether or not they are received with Caller ID.

  Note: Routed e-mail messages are considered as having Caller ID, which is actually the address. Therefore, filtering on Caller ID will include e-mail messages, unless they are filtered out by media type; filtering for no Caller ID, will exclude all e-mail messages.

- **Direct Dialed Only?**: Click **Yes** to only include calls which are directly dialed. Click **No** to only include calls which are not directly dialed. Click **All** to include calls regardless of whether or not they are directly dialed.

  Note: Routed e-mail messages are considered as having been directly dialed, therefore, filtering on Direct Dialed Only will include e-mail messages, unless they are filtered out by media type; filtering for no Direct Dialed Only, will exclude all E-mail messages.

- **Call Cost** (Reporter only): Select a comparison type for the call type. For example, to report call costs that are greater than $5.00, select >. Enter a call cost (e.g., 5) in the adjacent field. The call cost is always entered in the main currency unit of $0.00. To enter fraction of a currency unit, such as $.50, enter 0.50.

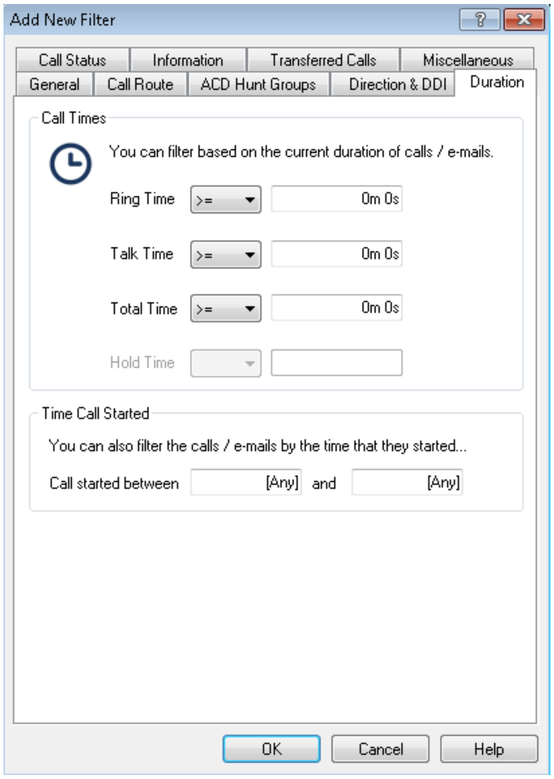
Note: Using the = comparison for call cost is not advisable. Computers often store numbers carried out to different decimal places (e.g., 0.50 may be stored as 0.499999999). If this occurs, the equivalence operator will not work because 0.4999999 does not equal 0.50. Use >= or <= where appropriate instead. Also, call costing calculations are based on limited data input and therefore may differ from the actual call charges made by the Telco.

- **Cost Group** (Reporter only): Select the cost group that you want to use as a filter. A cost group includes Local, National, International, etc.

DURATION

The Duration page allows you to filter calls based on how long the call has been ringing or active

Figure 18: Add New Filter: Duration Tab



You can filter based on the current duration of calls / e-mails.

Ring Time >= 0m 0s

Talk Time >= 0m 0s

Total Time >= 0m 0s

Hold Time

You can also filter the calls / e-mails by the time that they started...

Call started between [Any] and [Any]

This tab includes the following fields:

- **Ring Time**: Filters calls based on how long they have been ringing (or how long they rang). E-mail messages are considered "ringing" for the time they have not been routed to an agent. Use the drop-down box to select how you want to filter the call's ring time. To only include calls/e-mail messages that are ringing for *longer* than a specified time, select **>=**. To only include calls/e-mail messages that are ringing for *less* than a specified time, select**<=**. Then specify the ring time that you want to use for comparison. The time can be entered as either "?h ?m ?s," or as "hh:mm:ss." Valid examples include "5m" or "05:00" for 5 minutes, "15s" or "00:00:15" for 15 seconds, etc. This filter is affected by the **Yes, this device is treated as 'not answered'** and **Yes, this device is treated as 'not yet rung'** flags in Server.

- **Talk Time**: Filters calls based on how long the call was actively connected (i.e., from the time the call was answered to the time it was terminated or diverted/transferred from the device). For e-mail messages, talk time is considered the time the e-mail waited between being routed to an agent and the time a reply was sent. Use the drop-down box to select how you want to filter the talk time. To only include calls that are connected for *longer* than a specified time, select **>=**. To only include calls that are connected for *less* than a specified time, select **<=**. Then specify the talk time that you want to use for comparison. The time can be entered as either "?h ?m ?s," or as "hh:mm:ss." Valid examples include "5m" or "05:00" for 5 minutes, "15s" or "00:00:15" for 15 seconds, etc. This filter is affected by the **Yes, this device is treated as 'not answered'** and **Yes, this device is treated as 'not yet rung'** flags in Server.

- **Total Time**: Filters calls and e-mail messages based on how long the call/e-mail has been active (i.e., since it started ringing) regardless of whether or not it has been answered. Use the drop-down box to select how you want to filter the total time. To only include calls and e-mail messages that are active for *longer* than a specified time, select **>=**. To only include calls/e-mail messages that are active for *less* than a specified time, select **<=**. Then specify the total time that you want to use for comparison. The time can be entered as either "?h ?m ?s," or as "hh:mm:ss." Valid examples include "1h" or "1:00:00" for 1 hour, "34m 27s" or "00:34:27" for 34 minutes 27 seconds, etc. This filter is affected by the **Yes, this device is treated as 'not answered'** and **Yes, this device is treated as 'not yet rung'** flags in Server.

- **Total Hold Time**: Filters calls based on the time that they spent on hold. E-mails are not included in Total Hold Time. First select whether you want to include calls that were on hold for longer than a given time (>=) or less than a given time (<=). Then specify the duration to compare against. Durations can be entered as "hh:mm:ss" or as "?h ?m ?s". For example, "00:01:30" is the same as "1m 30s" or "90s".

> **Note:** The Total Hold Time option is disabled for the RealViewer and Reporter Real-Time modules.

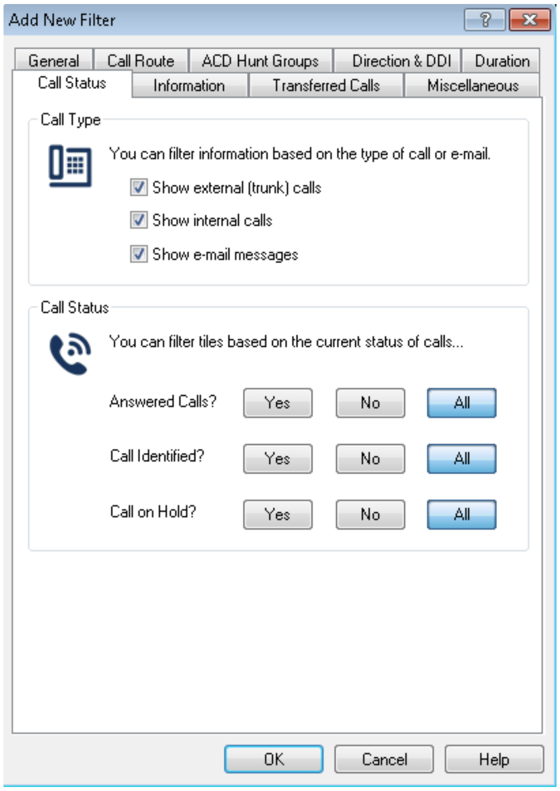
- **Call Started Between**: This will filter calls based on a specified start and end time, calculating the statistics only for calls that started within this range. Enter the start and end times in your regional format (e.g., "08:00" or "8:00:00 AM"). Filtering by time only affects historic call summary statistics, such as Inbound Calls Answered and Total Talk Time, and time based agent statistics including % Free Time. It will also be used to filter similar statistics in the Extension, Agent, and Trunk list (Reporter Real-Time only). It does not, however, affect real-time statistics, such as Agents Logged In, Calls Waiting, and Total Talk Time Now.

> **Note:** This setting is available only in Reporter Real-Time and RealViewer. In Reporter, use the Date / Time properties of the report to define the time period for which the report should be run.

CALL STATUS

The **Call Status** tab filters calls based on their status and/or whether or not the call information was identified by the Server.

Figure 19: Add New Filter: Call Status Tab



Call Type

You can filter information based on the type of call or e-mail.

☑ Show external (trunk) calls

☑ Show internal calls

☑ Show e-mail messages

Call Status

You can filter tiles based on the current status of calls...

Answered Calls? Yes No [✓ All]

Call Identified? Yes No [✓ All]

Call on Hold? Yes No [✓ All]

This tab contains the following fields:

- **Show external (trunk) calls**: When enabled (default), external calls are included in the filter.
- **Show internal calls**: When enabled (default), internal calls are included in the filter.
- **Show e-mail messages**: When enabled (default), e-mail messages are included in the filter.

Note: If all three of the options above are not selected, all types of media are filtered out, and no statistics can be calculated.

Unless Internal Call Modeling is turned on, filtering on Internal Calls will have no effect. If no media blending is configured, filtering on e-mail messages will have no effect.

- **Answered Calls?** (not available in Reporter): Click **Yes** to only include answered calls in the filter. Click **No** to only include unanswered calls in the filter. Click **All** to include calls regardless of whether or not they are answered. This filter is affected by the **Yes, this device is treated as ‘not answered’** and **Yes, this device is treated as ‘not yet rung’** flags in Server.

  - **Call Identified?** (not available in Reporter): Click **Yes** to include only calls and e-mail messages that have been matched against the MiCC Office Server Import. Click **No** to include only calls and e-mail messages that have not been matched against the Server Import. These calls would normally appear as “New Contact” in Reporter Real-Time or CallViewer. Click **All** to include calls and e-mail messages regardless of whether or not they have been matched against the Server Import.

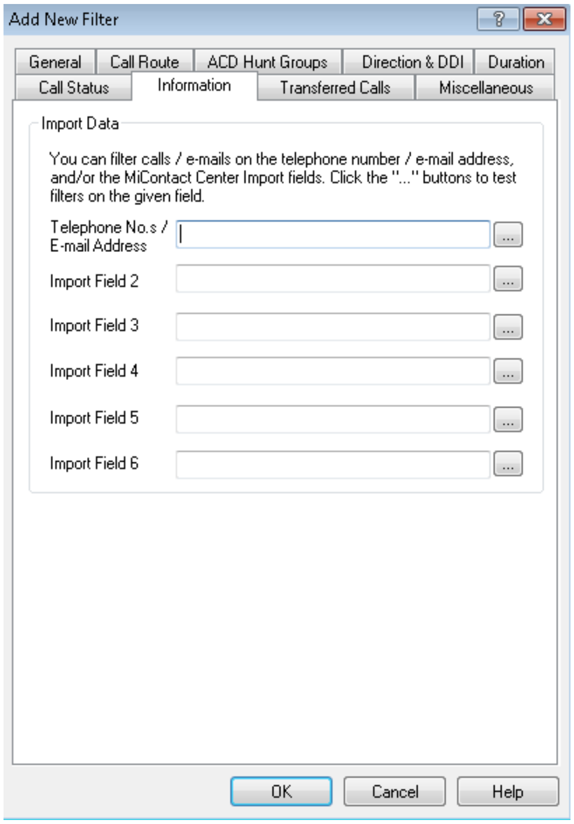
- **Call on Hold?** (not available in Reporter): Click **Yes** to only include calls that are currently on hold. Click **No** to only include calls that are not currently on hold. Click **All** to include calls regardless of whether or not they are on hold.

Note: The **Calls on Hold?** option will affect only currently active calls, as historical calls will normally not be on hold.

INFORMATION

The **Information** tab allows you to filter calls based on the telephone number or the various fields of the MICC OFFICE Server import.

Figure 20: Add New Filter: Information Tab



You can filter calls / e-mails on the telephone number / e-mail address, and/or the MiContact Center Import fields. Click the "..." buttons to test filters on the given field.

Note: MiCC Office only stores the Server Import Field 2 in the historic call database. Filtering on other fields from the Import will only affect currently active calls.

This tab includes the following fields:

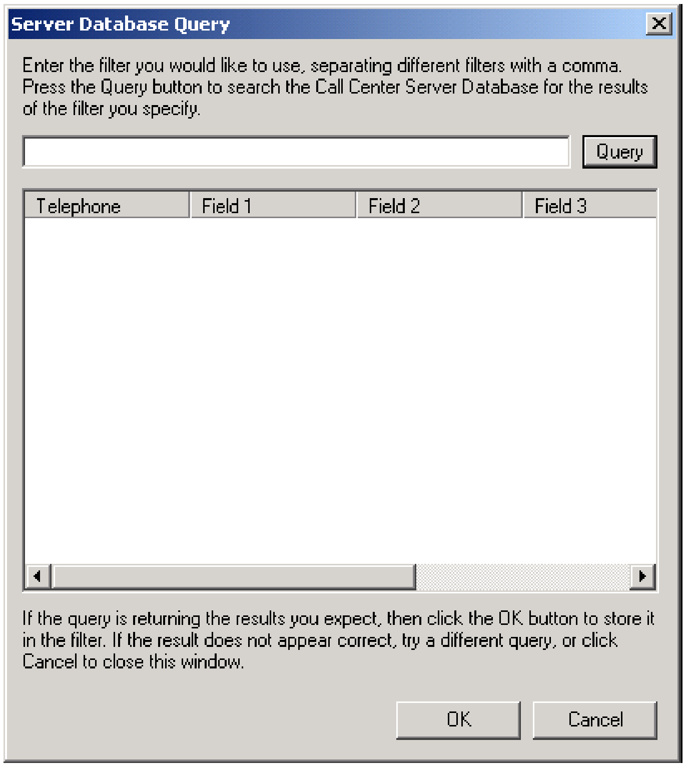
- **Telephone Numbers**: Enter a comma-separated list of telephone numbers and/or e-mail addresses to include in the filter. This type of filter will filter telephone numbers that call in or dial out. To only include people calling in from a number in this list, you should filter on Inbound calls only.

- **Import Field 2 to Import Field 6**: Enter a comma-separated list of a string to include in the filter. Wildcards can also be used in the filter. The meaning of the filter depends on what data is being imported into Server. Fields 2 through 6 are customer-specific and contents depend on what the Import file on your Server contains. Usually, Import Field 2 is the name of the company calling; so, Import Field 2 could be filtered on “Alpha*” to include calls from companies such as “Alpha Beta Gamma Ltd.” or “Alphacentauri Industries PLC.”

Note: You cannot filter on Import Field 2 to Import Field 6 in Reporter.

To see what data you can include in an Import Field filter:

1. Click the ellipsis (...) button next to an appropriate filter field. The Database Query dialog box appears.



Server Database Query

Enter the filter you would like to use, separating different filters with a comma. Press the Query button to search the Call Center Server Database for the results of the filter you specify.

Telephone	Field 1	Field 2	Field 3

If the query is returning the results you expect, then click the OK button to store it in the filter. If the result does not appear correct, try a different query, or click Cancel to close this window.

2. Enter the information for which you want to search (e.g., to search for a company called ABC Company, enter “ABC Company”).

3. Click **Query**. The application will query the information stored in the MiCC Office Server and display any matching information in the window.

Note: If you do not get any results when running a query, the database may include spaces before the record information. Try inserting a space or a wildcard (*) before the first letter (e.g., “*ABC Company”).

You can use a wildcard (*) with a partial name to search for a match (e.g., “AB*” will return ABC Company and any other records starting with “AB”).

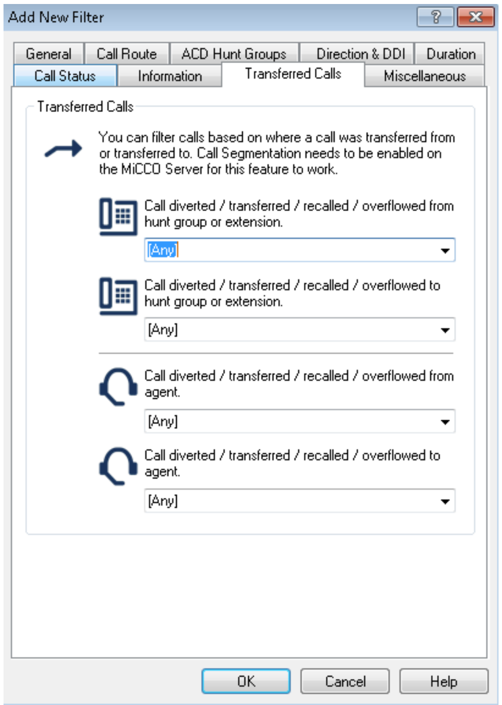
4. Click **OK** to save the record information to the filter, or click **Cancel** to exit without saving changes. You are returned to the Add New Filter screen.

> **Note:** The Database Query feature will not work unless you have successfully performed a Telephone Number import to the MiCC Office Server.

TRANSFERRED CALLS

The **Transferred Calls** page allows you to filter calls based on the transfer origination or destination extension, group, or agent.

Figure 21: Add New Filter: Transferred Calls Tab



Transferred Calls

You can filter calls based on where a call was transferred from or transferred to. Call Segmentation needs to be enabled on the MiCCO Server for this feature to work.

Call diverted / transferred / recalled / overflowed from hunt group or extension.
[Any]

Call diverted / transferred / recalled / overflowed to hunt group or extension.
[Any]

Call diverted / transferred / recalled / overflowed from agent.
[Any]

Call diverted / transferred / recalled / overflowed to agent.
[Any]

This page includes the following fields:

- **Calls diverted/transferred/recalled/overflowed from hunt group or extension**: Enter a comma-separated list or range that indicates the group(s) and/or extension(s) that transferred the call to another destination or use the drop-down list. The default value is [Any], meaning that filtered calls can be transferred from any hunt group or extension, or not transferred at all.

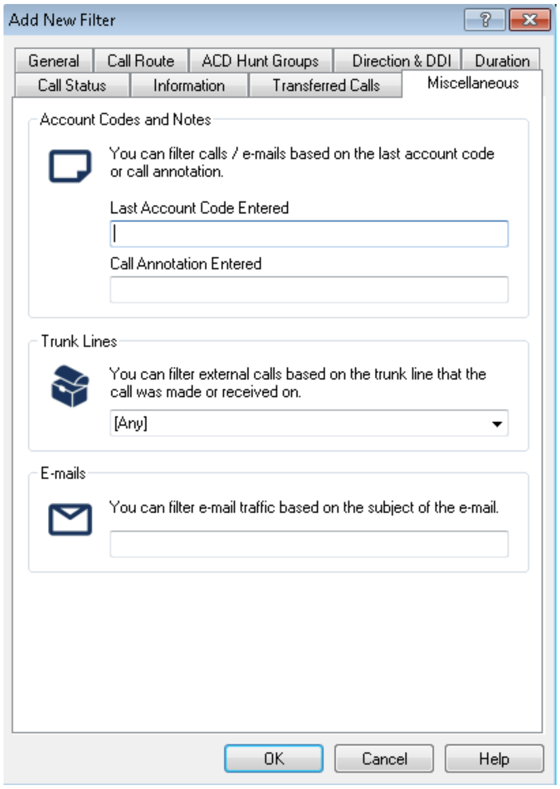
- **Calls diverted/transferred/recalled/overflowed to hunt group or extension**: Enter a comma-separated list or range that indicates the destination group(s) and/or extension(s) of the transfer or use the drop-down list. The default value is [Any], meaning that filtered calls can be transferred to any hunt group or extension, or not transferred at all.
- **Call diverted / transferred / recalled / overflowed from agent**: Enter a comma-separated list or range that indicates the agent(s) that transferred the call to another destination or use the drop-down list. The default value is [Any], meaning that filtered calls can be transferred to or from any agent, or not transferred at all.
- **Call diverted / transferred / recalled / overflowed to agent**: Enter a comma-separated

list or range that indicates the destination agent(s) of the transfer or use the drop-down list. The default value is [Any], meaning that filtered calls can be transferred to or from any agent, or not transferred at all.

MISCELLANEOUS

The **Miscellaneous** tab includes filter options that do not apply to the other tabs.

Figure 22: Add New Filter: Miscellaneous Tab



You can filter calls / e-mails based on the last account code or call annotation.

You can filter external calls based on the trunk line that the call was made or received on.

[Any]

You can filter e-mail traffic based on the subject of the e-mail.

The Miscellaneous tab includes the following fields:

- **Last Account Code Entered**: Includes any calls where the last account code entered against the call matches the list of account codes entered in the filter. Enter a comma-separated list or range of account codes to include in the filter. Each item can contain wildcards, where a “*” means none or more characters.
- **Call Annotation Entered**: Includes any calls where the call annotation entered contains the specified text. You can enter comma-separated text strings; annotations with any string that matches a call's annotation will be included in this filter. If you enter a wildcard, where a “*” means none or more characters, partial matches will be included. If you do not enter a wildcard, only exact matches are included, although they are not case-sensitive.
- **Trunk Lines**: Enter a comma-separated list or range of trunk lines to include in the filter or use the drop-down list. Internal calls and e-mail messages are excluded.
- **E-mail Subject**: Includes any e-mail that contains the specified text as an e-mail subject. You can enter comma-separated text strings; e-mail subjects with any string that matches an e-mail's subject will be included in this filter. If you enter a wildcard, where a “*” means none or more characters, partial matches will be included. If you do not enter a wildcard, only exact matches are included, although they are not case-sensitive.

EDITING A FILTER

To edit a filter, open the Filter Manager by clicking the Filter Manager button (▽) or selecting **Filter Manger** from the main menu (🎧). Select the filter that you want to edit, and click **Edit**. Or, double-click on the filter that you want to edit. After you have completed editing a filter, any tiles that are using the filter are automatically updated.

Note: You cannot edit the All Calls filter.

REMOVING A FILTER

To remove a filter, open the Filter Manager by clicking the Filter Manager button (▽) or selecting **Filter Manager** from the main menu (🎧). Select the filter that you want to remove, and click **Remove**. At the prompt, click **Yes** to delete the filter or **No** to cancel the action. If you click **Yes**, the filter will be removed, and any tiles using the filter will revert to the default "All Calls" filter, which cannot be removed.

Note: Once removed, the filter cannot be retrieved.

Chapter 5

INSTALLATION AND CONFIGURATION

INTRODUCTION

The MiContact Center Office (MiCC Office) Server application is a CTI (Computer Telephony Integration) that bridges the gap between a computer network and the Mitel telephone system. Communicating with the phone system via a TCP/IP network connection, the Server provides CallViewer, RealViewer, Reporter, Reporter Real-Time, and Intelligent Router applications with call and agent data.

MiCC Office is a licensed product that is installed in the following configurations:

- As a standalone application (see "Installing Standalone MiCC Office" on page 9)
- As a virtual appliance, Virtual MiCC Office (see "Install Virtual MiCC Office" on page 22 and the Virtual Appliance Deployment Guide)

This chapter provides the procedures necessary to complete the MiCC Office installation and configuration for Standalone MiCC Office.

This chapter also provides the necessary procedures to migrate MiCC Office from an existing MAS environment to a standalone environment. See "Migrating from a MAS Environment" on page 34 for details.

INSTALLATION AND CONFIGURATION OVERVIEW

Have the following information and supplies available before you begin the installation and configuration process for MiCC Office:

- The IP address for the communication system that MiCC Office will connect to.
- The following telephone system information:
  - *If connecting to a single-node Mitel MiVoice Office 250*, the OAI socket password.
  - *If connecting to a multi-node Mitel MiVoice Office 250*, the CT Gateway IP address and OAI password.
    For details, refer to the *CT Gateway Installation Manual* (part number 835.2161).

Note: For details about configuring the telephone system, refer to the Mitel MiVoice Office 250 system documentation for the information.

Standalone MiCC Office is downloadable from Mitel Online.

The following high-level procedure describes the installation and configuration process for a standalone MiCC Office.

To install and configure MiCC Office:

1. Configure the communication platform connection (see "Configuring the Communication Platform Connection" on page 4).
2. Configure the communication platform to communicate with MiCC Office (see "Configuring the Telephone System" on page 7).
3. Configure the telephone system (see "Configuring the Telephone System" on page 7).

4. Install standalone MiCC Office (see “Install the MiCC Office Standalone Software” on page 10).

5. Configure MICC OFFICE Server (see “Configuring MiCC Office Server” on page 40).

CONFIGURING THE COMMUNICATION PLATFORM CONNECTION

For MiCC Office Server to function correctly, it needs to be correctly configured to communicate with the telephone system installed on site.

For MiCC Office Server to function correctly, it needs to be correctly configured to communicate with the telephone system installed on site. This section describes how to connect the MiCC Office hardware platform to each of the MiCC Office -supported Mitel communication platforms. All connections are made using a direct TCP/IP connection. Supported connection configurations include:

- Connect to a single-node Mitel MiVoice Office 250 communication platform.

- Connect to a multi-node Mitel MiVoice Office 250. This type of configuration uses the CT Gateway. The following pages provide installation examples of those configurations previously listed.

SINGLE NODE CONNECTION SINGLE-NODE CONNECTION

When using direct TCP/IP, you can connect the MiCC Office Server to a single communication platform node (Mitel MiVoice Office 250) or a CT Gateway.

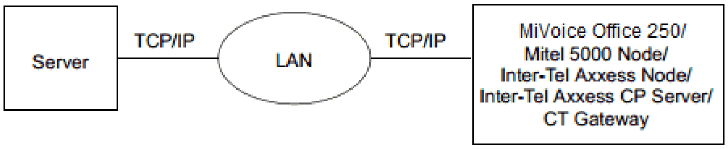


Figure 1: Single Node Connection

MULTI-NODE CONNECTION

MiCC Office supports connections to Mitel MiVoice Office 250.

MITEL MiVoice Office 250 MULTI-NODE CONFIGURATION

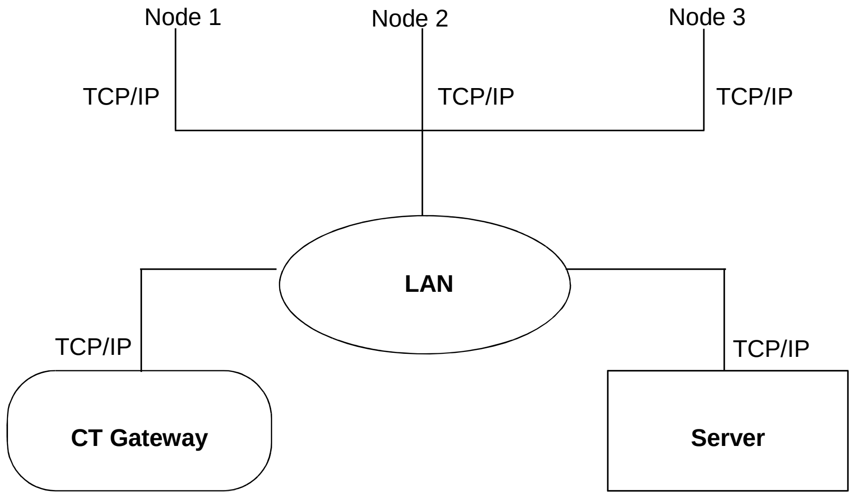
NOTICE

When MiCC Office starts, it checks the software version of each node via the CT Gateway. If any nodes are running Mitel MiVoice Office 250 v4.0 (or later) system platform software, we recommend that all nodes are running on the same software version. In addition, the CT Gateway software must be v5 or later or MiCC Office will fail to initialize the node.

The CT Gateway is a Mitel application that unifies the System OAI stream, allowing MiCC Office Server to communicate with several Mitel MiVoice Office 250 telephone systems at the same time. Each node in a communications network functions individually as far as the

System OAI streams are concerned. The CT Gateway receives the OAI streams from multiple nodes and consolidates them into a single stream for the Server application. The CT Gateway sends and receives all of its data via TCP/IP connections. The figure below shows MiCC Office Server connected to a multi-node system via a CT Gateway.

Figure 2: Multi-node Mitel MiVoice Office 250 Connection



The CT Gateway can operate in default mode or multi-node aware mode.

Default Mode

The CT Gateway's "Default Mode" is designed to allow a single CTI application to interact with many OAI protocol streams transparently (i.e., as if they all came from one node). Default Mode does not allow the attached CTI application to detect the status of each switching node. For example, four nodes might be functioning correctly while one node might have been reset. Because the CT Gateway's Default Mode models all nodes as one telephone system, even if only one node goes down, the CT Gateway detects this as the entire system being down. In addition, it may take Server several minutes to initialize the entire system when a "downed" or inoperable node becomes operational again.

Node Aware Mode

An external CTI application can request that the CT Gateway operate in Node Aware mode. This allows the CTI application to detect the state of each individual node and separately initialize each node at different times. Node Aware mode also allows the application to continue monitoring the remaining functional nodes, even when other nodes in the same system are in an offline or inoperable state.

The CT Gateway's Node Aware Mode is used when the MiCC Office Server Number of Nodes license, as depicted by the MiCC Office license that is equal to or higher than two node licenses.

Feature Licensing and OAI Version

When installing MiContact Center Office with the CT Gateway application, there are some important considerations related to how the CT Gateway views differences in OAI protocol version and premium feature licensing across all the detected nodes.

The CT Gateway follows the protocol of enabling features according to the lowest common premium feature license and the lowest OAI protocol version detected by Server. This means that if only one node does not have the System OAI Third-Party Call Control licensing enabled, MiCC Office Server operates in Event Only mode. Additionally, the node running the lowest OAI protocol version dictates the OAI features available in Server.

When connecting to the CT Gateway, the Server installation routine contains an option to configure the settings that will be used when communicating with the telephone system, although these settings can be changed after the product installation. The default TCP/IP port number of the CT Gateway is 4000. It is recommended that you verify this port number with the person who installed the CT Gateway.

For CT Gateway's connectivity to each individual node there are other node-specific configurations required, such as purchasing the System OAI Events and System OAI Third-Party Call Control licensing, as well as enabling the System OAI Level 2 Sockets option in Database Programming.

CONFIGURING THE TELEPHONE SYSTEM

For MiCC Office to function correctly, the telephone system also needs to be configured. This section describes the additional configuration required for Server to connect to the telephone system.

CONFIGURE A MITEL MIVOICE OFFICE 250 PLATFORM

For MiCC Office to communicate with a Mitel MiVoice Office 250 communication platform, you must enable the System OAI socket connection and System OAI Third-Party Call Control in Database (DB) Programming. Refer to the communication platform's installation manual and DB Programming online help for details about configuring settings in Database Programming.

INSTALLING MICC OFFICE

The version of MiCC Office is packaged as a zip file. The zip file contains the server setup kit and also contains DB2 files for Windows. The server setup kit is also used to upgrade MiCC Office.

BEFORE YOU BEGIN

Gather and record all relevant and necessary information such as passwords, IP addresses, license keys, and Application Record IDs before beginning the installation.

Download the standalone zip file containing the MiCC Office installation files from Mitel Online (MOL), and extract the installation files from the zip file.

INSTALL IN A VIRTUAL ENVRONMENT

Virtual MiCC Office can be installed manually on a Microsoft Windows 64-bit machine running within a Hyper-V or VMWare virtual environment (see Virtualisation Requirements on 23).

You can use any of the supported operating systems in this environment (see System Requirements on page 23).

Install the Guest OS according to your virtual environment, then follow the install guide for installing in a standalone environment below.

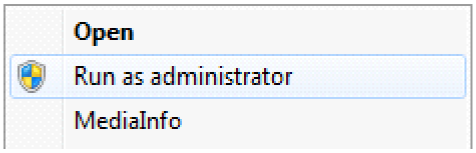
INSTALL THE MICC OFFICE SOFTWARE

To install the version of MiCC Office Server, first launch the Server Setup Wizard, then configure the MiCC Office Setup Wizard.

Note: Installing the MiCC Office software on a domain controller or exchange server is not supported.

LAUNCH THE SERVER SETUP WIZARD

1. Launch the server setup kit with administrator privileges.



The *User Account Control* prompt displays. Click **Yes** to run the server setup.

Note: You must run the Server Setup Wizard as an Administrator. If the setup kit is launched by a user who is not a member of the local Administrators group, the user must enter the password for the local administrator user to continue with the installation.

2. If installing MiCC Office Server over a network, the *Security Prompt Warning* page displays. Select

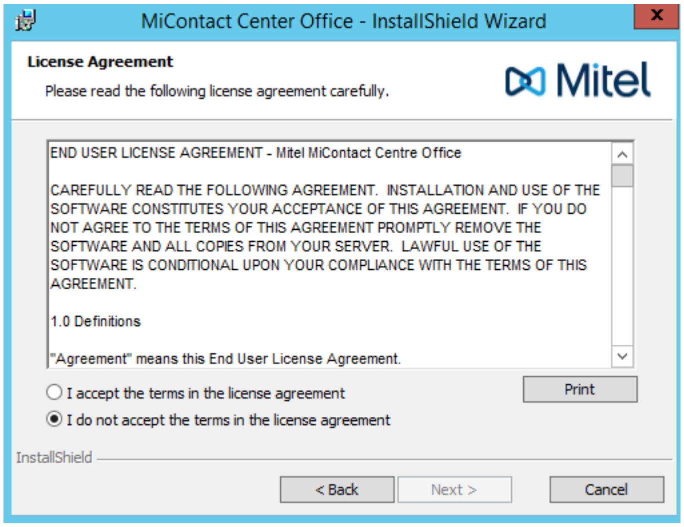
Run to install MiCC Office.

3. *The Mitel MiContact Center Office - InstallShield Wizard* prompt appears.

To install the required packages, click **Install**. A restart may be required after each package installation.

CONFIGURE THE MICC OFFICE

1. The *Welcome* page begins the MiCC Office Setup Wizard. After it opens, click **Next**.
2. The install displays a message if it detects an older version of MiCC Office. The older version of MiCC Office must be removed before the install can continue. MiCC Office settings are preserved. Click **Yes** to uninstall.
3. A message may appears asking for you to stop the MiCC Office server service and close any applications running on the computer. Click **OK** after you have stopped the service and closed all applications.
4. The *License Agreement* page displays. Read the Microsoft License Agreement, select the **I accept the terms in the license agreement** option, and then click **Next**.


MiContact Center Office - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

END USER LICENSE AGREEMENT - Mitel MiContact Centre Office

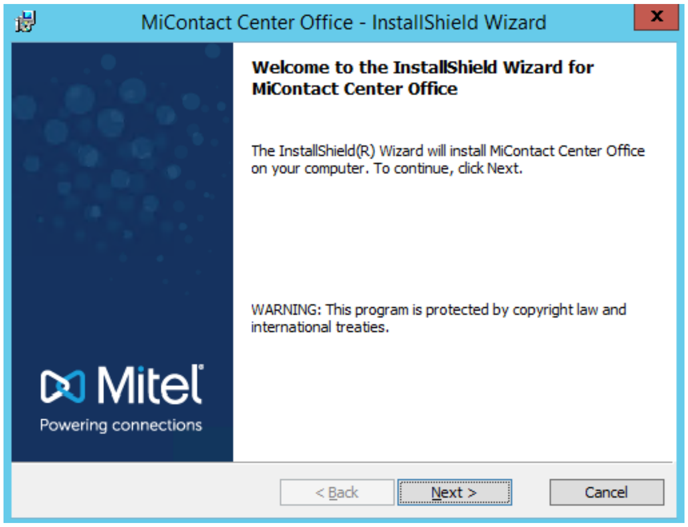
CAREFULLY READ THE FOLLOWING AGREEMENT. INSTALLATION AND USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT.

1.0 Definitions

"Agreement" means this End User License Agreement.

○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement


MiContact Center Office - InstallShield Wizard

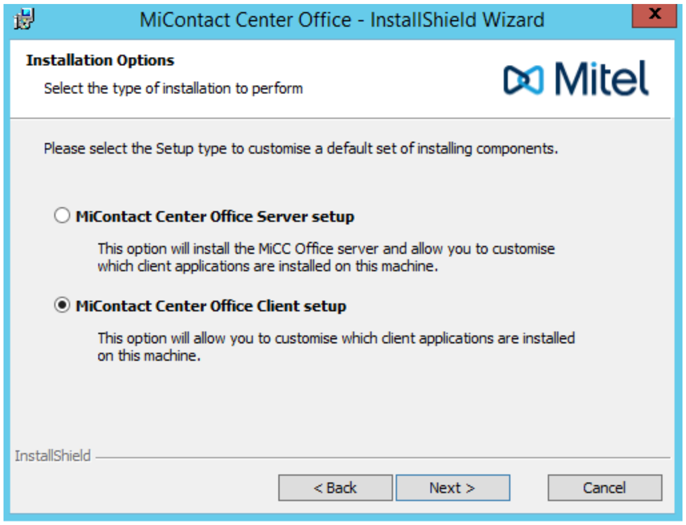
Welcome to the InstallShield Wizard for MiContact Center Office

The InstallShield(R) Wizard will install MiContact Center Office on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5. Choose one of the following setup types for the installation:

- Select **MiCC Office Server setup** to install the MiCC Office server and choose the client applications to enable (by default Reporter and RealViewer will be installed). Click **Next**.
- Select **MiCC Office Client setup** to choose the client applications to enable. Click **Next.**



MiContact Center Office - InstallShield Wizard

Installation Options

Select the type of installation to perform

Please select the Setup type to customise a default set of installing components.

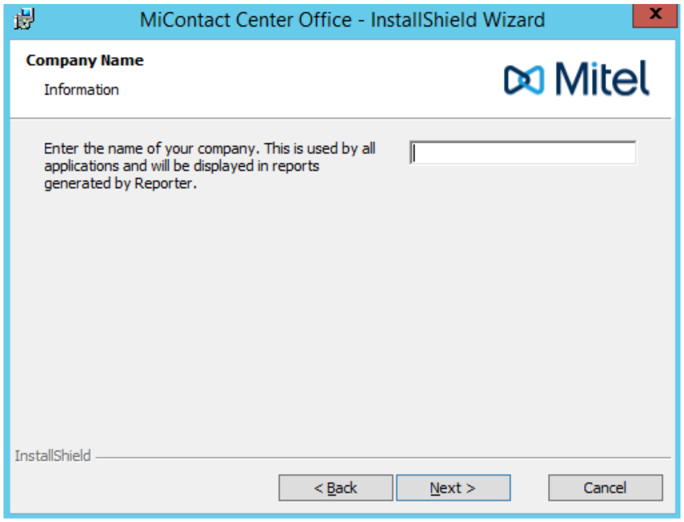
○ **MiContact Center Office Server setup**

This option will install the MiCC Office server and allow you to customise which client applications are installed on this machine.

● **MiContact Center Office Client setup**

This option will allow you to customise which client applications are installed on this machine.

6. (optional) To view the disk space required for a feature, select the feature and click **Space**. Click **OK**. Click **Next**.
7. (new install) The *Company Name* page displays. Enter the company name and click **Next**.



MiContact Center Office - InstallShield Wizard

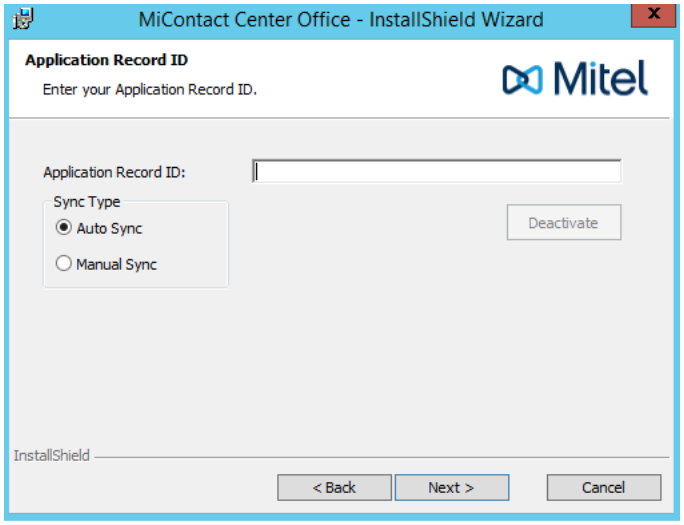
Company Name

Information

Enter the name of your company. This is used by all applications and will be displayed in reports generated by Reporter.

8. (new install) The *Application Record ID* page appears. Enter the Application Record ID (ARID). This number identifies the customer's license and is used to verify that the customer is licensed to run the newer version of the MiCC Office software.

Note: If MiCC Office has already been configured with a valid Application Record ID, then an option to skip the sync is also included.


MiContact Center Office - InstallShield Wizard

Application Record ID

Enter your Application Record ID.

Application Record ID:

Sync Type
● Auto Sync
○ Manual Sync

Select one of the following sync options, and then click **Next**.

a. **Auto Sync** synchronizes the MiCC Office license directly with the AMC using an existing Internet connection.

b. **Manual Sync** allows users to synchronize the MiCC Office license when the server MiCC Office is installed on does not have access to the Internet. You will need to follow these steps first if an Automatic Sync has already been attempted and has failed. Click the deactivate button and re-enter the ARID before you start a manual sync.

Note: You will need to use two PCs to perform a manual sync: a MiCC Office server without Internet access and an alternative PC with Internet access

1.) On the MiCC Office server, perform these steps:

- Start the MiCC Office Install wizard.
- Select **Manual Sync.**
- Choose the location to extract the license files to.
- Click **Next**. A folder labelled ‘AMC’ will appear in the location you chose in the last step.
- Copy the AMC folder to a location on the alternative PC.

2.) On the alternative PC:

- Open the AMC folder you copied from the MiCC Office server.
- Select the file **MiCC Office Manual Sync.exe**, right-click and select **Run as administrator**. You should then see a message indicating the sync was successful.
- Copy and paste the AMC folder back to the MiCC Office server in the location you specified originally.

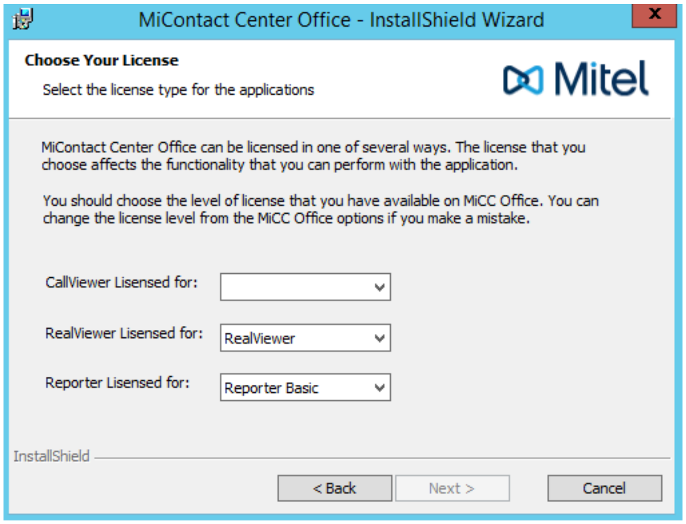
3.) On the MiCC Office server:

- After the folder is copied back onto the MiCC Office server in the correct location click
  Next.
- The MiCC Office server should now be successfully licensed, and allow you to continue through the install\setup wizard.

4.) If you are using a manual sync and the License has been upgraded on the AMC to provide new features, perform the following steps in order to apply those new features to the MiCC Office server. On the MiCC Office server:

- Select Start > All Programs > Mitel MiContact Center Office > MiCC Office Setup Wizard.
- Follow the steps in the Wizard until you get to the ‘Application Record ID’ step.
- Make a note of the ARID you are using.
- Click **Deactivate** and select **Manual Sync**.
- Re-Enter the ARID and click **Next.**
- Follow step 1 to step 3 of the ‘b. Manual Sync’ option.

9. The *Choose Your License* page appears. Select your MiCC Office licenses and click **Next.**



Choose Your License

Select the license type for the applications

MiContact Center Office can be licensed in one of several ways. The license that you choose affects the functionality that you can perform with the application.

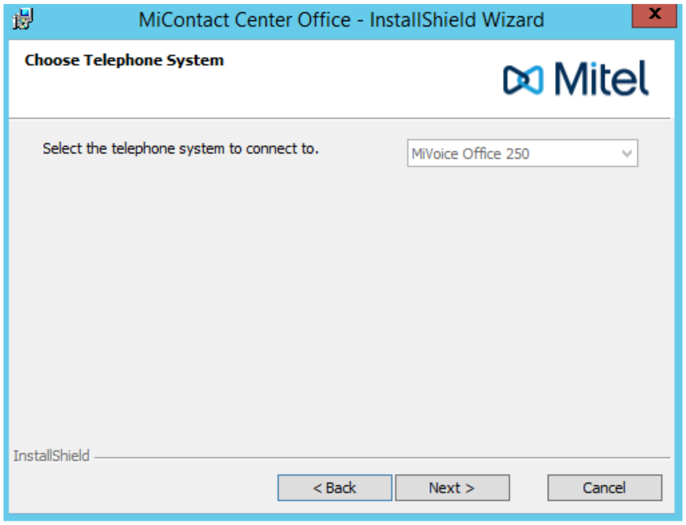
You should choose the level of license that you have available on MiCC Office. You can change the license level from the MiCC Office options if you make a mistake.

CallViewer Lisensed for:

RealViewer Lisensed for: RealViewer

Reporter Lisensed for: Reporter Basic

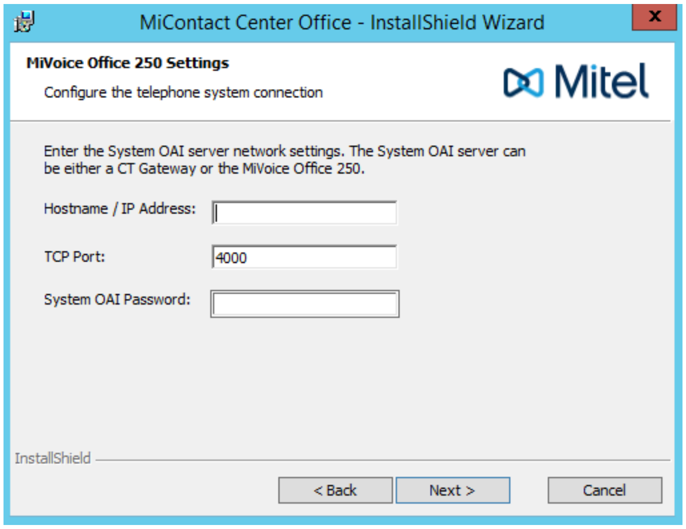
10. The *Choose Telephone System* page appears.
Select which telephone system to connect to, and then click **Next**.



Choose Telephone System

Select the telephone system to connect to. MiVoice Office 250

11. To configure the Mitel MiVoice Office 250 telephone system settings, type in the Hostname/IP Address, TCP Port, and System OAI Password. Click **Next**.



MiVoice Office 250 Settings

Configure the telephone system connection

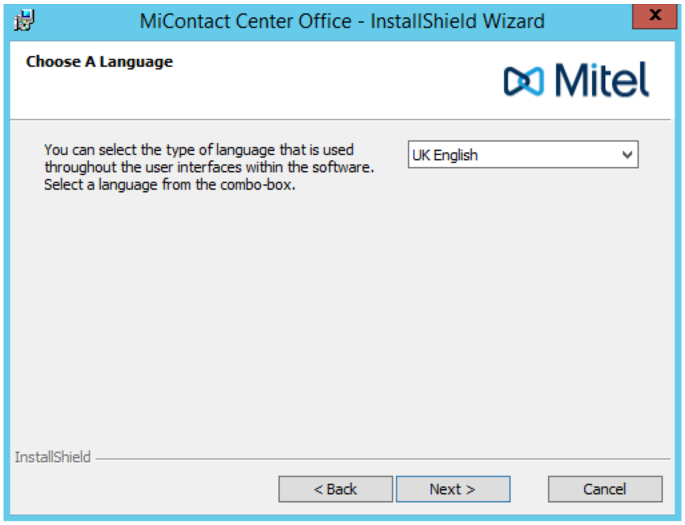
Enter the System OAI server network settings. The System OAI server can be either a CT Gateway or the MiVoice Office 250.

Hostname / IP Address:

TCP Port: 4000

System OAI Password:

12. The *Choose a Language* page appears.



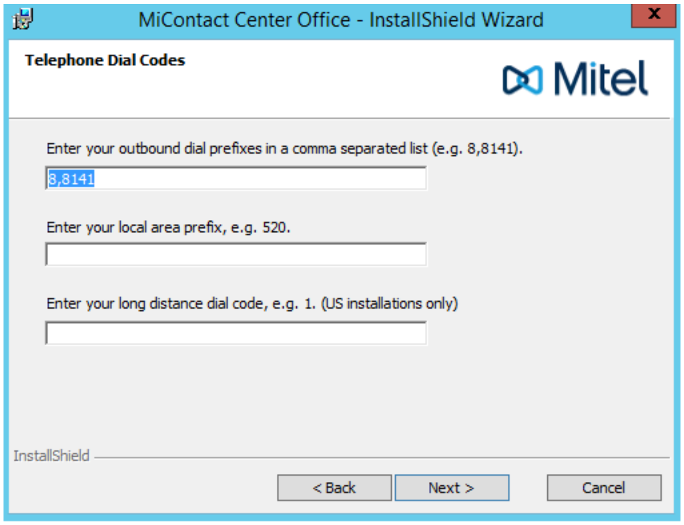
Choose A Language

You can select the type of language that is used throughout the user interfaces within the software. Select a language from the combo-box.

UK English

Select **US English**, **UK English**, or **Australian English** from the drop-down list. Click **Next**.

13. The *Telephone Dialing Codes* page appears.



MiContact Center Office - InstallShield Wizard

Telephone Dial Codes

Enter your outbound dial prefixes in a comma separated list (e.g. 8,8141).

8,8141

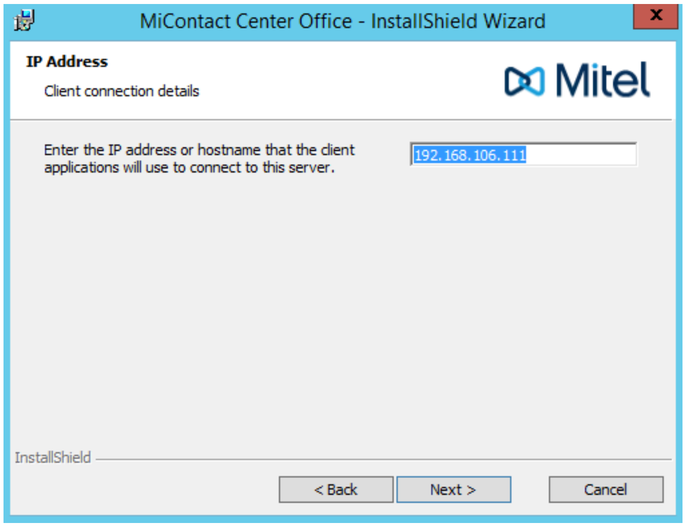
Enter your local area prefix, e.g. 520.

Enter your long distance dial code, e.g. 1. (US installations only)

Depending on which language you selected, perform the following:

- For US Dialing Codes, enter the outbound dialing prefixes, local prefix, and long distance dial code. Click **Next**.
- For UK Dialing Codes, enter the outbound dialing prefixes. Click **Next**.
- For Australian Dialing Codes, enter the outbound dialing prefixes. Click **Next**.

14. The MiCC Office Server *IP Address* page appears.



MiContact Center Office - InstallShield Wizard

IP Address

Client connection details

Enter the IP address or hostname that the client applications will use to connect to this server.

192.168.106.111

15. In the **IP address or hostname** field enter the IP address or hostname that the MiCC Office client applications use to connect to the MiCC Office database. Click **Next**.

16. The Import *Legacy Database* page appears. Perform one of the following actions:

- If you do not have data to import, click **Next**.

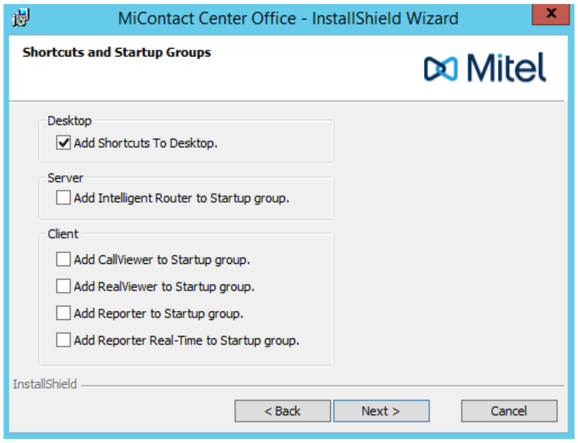
> **Note:** When using the MiCC Office Backup Tool to migrate a MAS environment, DO NOT choose to import a database.
> Click **Next**.

17. Select a database type from the drop-down list. Depending on which database you select, do the following database option and click **Next**. The *Import database settings* page appears.

- If the **'IBM DB2 MICC OFFICE 5.x+'** option is selected, enter the IP address or hostname of the MSL server. To import data from a standalone edition of MiCC Office, enter the Windows IP address or hostname of the MiCC Office Server. Click **Next**. The MiCC Office Setup Wizard tries to connect to a MiCC Office 5.x/6.x DB2 server. Selecting this option will migrate telephone system configuration settings which are stored in the database. The database migration process is completed when the Data Migration wizard runs, which imports historical call and agent data.
  Selecting this option does not migrate Intelligent Router settings or MiCC Office Server settings. The MiCC Office Backup Tool is used to migrate these settings.

18. The *Shortcuts and Startup Groups* page appears.

Select the client, server, and desktop items to add to the startup group and click **Next**.



MiContact Center Office - InstallShield Wizard

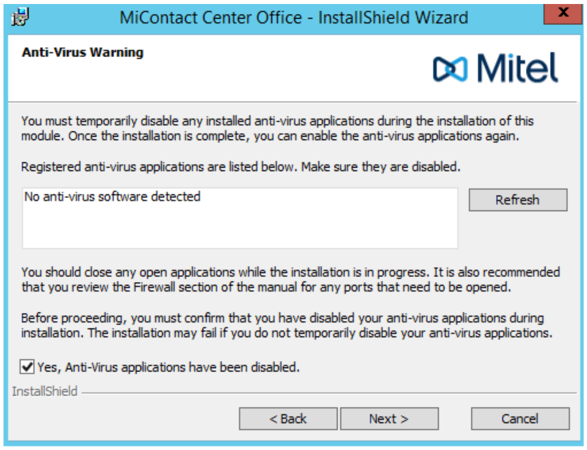
Shortcuts and Startup Groups

Desktop
☑ Add Shortcuts To Desktop.

Server
☐ Add Intelligent Router to Startup group.

Client
☐ Add CallViewer to Startup group.
☐ Add RealViewer to Startup group.
☐ Add Reporter to Startup group.
☐ Add Reporter Real-Time to Startup group.

19. The *Anti-Virus Warning* page appears. Disable all virus programs and click **Refresh**. If you have a virus program that does not appear on the list, disable it. Click **Next**.



MiContact Center Office - InstallShield Wizard

Anti-Virus Warning

You must temporarily disable any installed anti-virus applications during the installation of this module. Once the installation is complete, you can enable the anti-virus applications again.

Registered anti-virus applications are listed below. Make sure they are disabled.

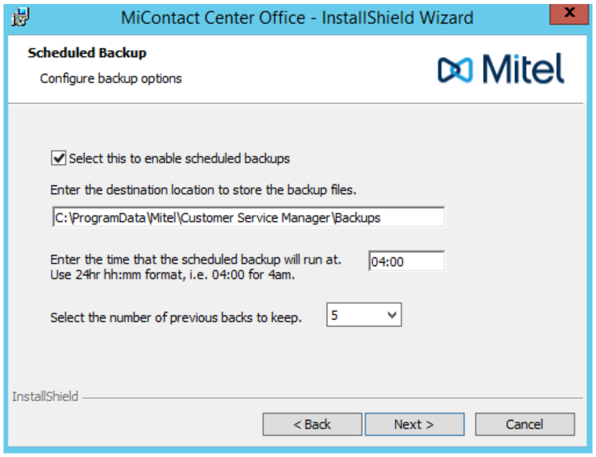
No anti-virus software detected

You should close any open applications while the installation is in progress. It is also recommended that you review the Firewall section of the manual for any ports that need to be opened.

Before proceeding, you must confirm that you have disabled your anti-virus applications during installation. The installation may fail if you do not temporarily disable your anti-virus applications.

☑ Yes, Anti-Virus applications have been disabled.

20. The Scheduled Backup configuration appears. By default the scheduled backup process will be enabled and set to run at 4am. Configure the backup as you require and then click **Next**.



Scheduled Backup

Configure backup options

☑ Select this to enable scheduled backups

Enter the destination location to store the backup files.

C:\ProgramData\Mitel\Customer Service Manager\Backups

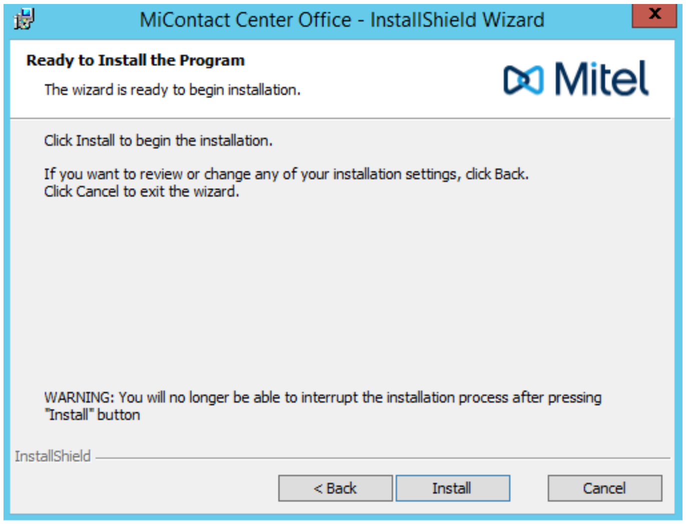
Enter the time that the scheduled backup will run at.
Use 24hr hh:mm format, i.e. 04:00 for 4am.

04:00

Select the number of previous backs to keep. 5

21. The *Ready to Install the Program* page appears. Click **Install** to install the files.

Note: During the upgrade to MiCC Office 6.2, .NET 4.5 is installed. Several Windows Features messages requesting to install .NET 3.5 may appear. Do nothing with these messages to avoid interrupting the installation. MiCC Office 6.2 will be installed and MiCC Office applications will work after reboot.



Ready to Install the Program

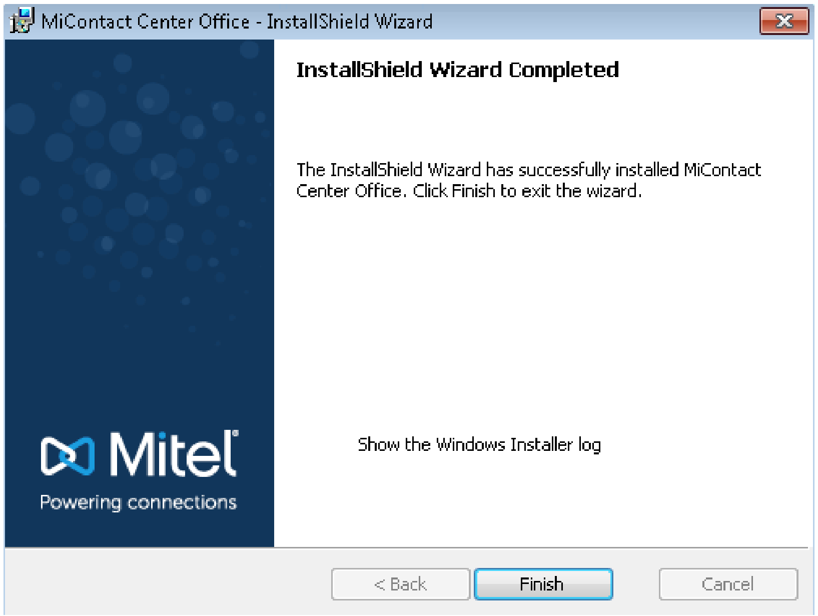
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back.
Click Cancel to exit the wizard.

WARNING: You will no longer be able to interrupt the installation process after pressing "Install" button

The **Installation Complete** page appears.



MiContact Center Office - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed MiContact Center Office. Click Finish to exit the wizard.

Show the Windows Installer log

22. Click **Finish** to exit the Setup Wizard.

MIGRATING FROM A MAS ENVIRONMENT

Beginning with Release 6.x, MICC OFFICE is no longer supported within a MAS environment. To effectively manage the migration from a MAS environment, MiCC Office application records can use new AMC migration licenses, where MiCC Office licenses can be split from MAS and be reused on a new or existing server.

With MiCC Office 6.x an updated backup process uses the MiCC Office Backup Tool, that allows the data and settings from MiCC Office on a MAS server to be backed up and stored on a network drive or local media, and restored into the standalone application.

The migration process is specifically for MiCC Office versions 6.0 and above. The old MiCC Office version is removed before installing the new version.

This section describes the following migration options available for MiCC Office as a standalone application:

- Single application MAS configuration, where MiCC Office is the only application installed on the MAS server
- Multi-application MAS configuration, where MiCC Office is installed among other applications on the MAS server.

The following items are an overview for migrating from a MAS environment, the details of which are described below:

- Backup the MSL server upon which MiCC Office is installed.
- Backup the MiCC Office data using the MiCC Office Backup Tool.
- Re-purpose the MAS server.
- Install standalone MiCC Office.
- Restore the MiCC Office data using the MiCC Office Backup Tool.

CONSIDERATIONS

Migrating to the standalone MiCC Office creates the situation where the existing MAS server can be used for other purposes.

Once the backup is complete (see details below), the MAS server can be dismantled and used for another purpose. There are a number of options available for re-purposing the MAS server, depending on the existing configuration.

RE-PURPOSING A SINGLE APPLICATION MAS SERVER

The following options are available when you want to repurpose a single application MAS server:

- Install a supported Windows operating system for use with standalone MiCC Office. See “System Requirements” on page 9. This is the recommended path when migrating a single application MAS with MiCC Office environment.
- Use the MAS server for another purpose; standalone MiCC Office would need to be installed on another server.

RE-PURPOSING A MULTI-APPLICATION MAS SERVER

When repurposing a multi-application MAS server, continue using the existing MAS server for MAS; upgrade to the latest supported version of MAS, and install standalone MiCC Office on another separate server.
This is the recommended path when migrating a multi-application MAS environment.

MIGRATING MICC OFFICE FROM MAS TO STANDALONE MICC OFFICE

The MiCC Office Backup Tool is used to migrate MiCC Office from
a MAS server.

To use the MiCC Office Backup Tool, the .Net 4.0 Client Profile must be installed within the Windows on the MAS server. The MiCC Office Backup Tool installer will automatically run the .Net setup tool if it is not already installed. If the MAS server does not have access to the Internet, the .Net 4.0 Client Profile will need to be installed prior to installing the MiCC Office Backup Tool.

Note: The date format of the source MiCC Office Server and the new MiCC Office Server must be the same for the backup and restore operation to succeed. For example, DD.MM.YYYY and MM.DD.YYYY would not work but MM.DD.YYYY and MM.DD.YYYY would.

To install the .Net 4.0 Client Profile where the MAS server is not connected to the Internet:

1. From a machine with Internet access, download the .Net 4.0 Client Profile standalone installer from http://www.microsoft.com/download/en/details.aspx?id=24872.
2. Copy the installer to a USB drive.
3. Insert the USB drive into an available USB port on the MAS server.
4. Open the Server Manager for the MAS server using a web browser.
5. Log in as administrator and navigate to the Mitel MiCC Office page.
6. From the USB devices drop down list, select the USB drive containing the .Net 4.0 Client Profile installer.
7. Log in to the MiCC Office Windows virtual machine on the MAS server.
8. Navigate to the USB drive in Windows Explorer and run the .Net 4.0 Client Profile installer.

To begin the migration:

1. Backup the MSL server upon which MAS and MiCC Office are installed. See the *Mitel Standard Linux Installation and Administration Guide* for details.

   Note: Backing up the MSL server is a precautionary measure only, should the migration not proceed as expected.

2. If installed on an MCD platform, upgrade to the latest MCD software release, 4.2 SP2 or 5.0 SP1. See the *Mitel Communications Director Technician's Handbook* for details.
3. Install the MICC OFFICE Backup Tool:
   a. Download the standalone MICC OFFICE zip file from Mitel Online (MOL).
   b. Extract the *MICC OFFICE Backup Tool Setup.exe* file from the zip file.
   c. Copy the *MICC OFFICE Backup Tool Setup.exe* file to the MICC OFFICE Server's Windows virtual ma- chine on the MAS server.
   d. Run the installer.
4. Back up MiCC Office; use the MiCC Office Backup Tool from within the MiCC Office MAS

virtual machine. See “Using the MICC OFFICE Backup Tool” on page 11 for details.

Note: There will need to be sufficient disk space available in order to successfully complete the backup. As a guideline, the available disk space within the virtual machine should be the size of the MICC OFFICE database plus an additional 25%. If the MICC OFFICE Backup Tool runs out of disk space during the backup operation, the backup will be cancelled and any intermediate backup files will be deleted.
Run the MICC OFFICE Backup Tool with the optional `--diskspace` command to display the estimated amount of disk space required for the backup.

5. Apply the appropriate migration part number to the existing MiCC Office MAS ARID. See Product Bulletin PA20110431 for details.

a. To apply the single application MAS migration part number:

i. Go to the AMC.

ii. Assign the part number to the existing MiCC Office MAS ARID.
The AMC will then make the required changes to the ARID to convert it to a standalone or virtual MiCC Office license. Applying the appropriate migration part number to the existing MiCC Office MAS ARID will:

- Convert the ARID to either a standalone or virtual MiCC Office ARID. The existing ARID can be used to license MiCC Office 6.x.
- The MiCC Office 6.1.x base license entitlement will be replaced with the MiCC Office 6.0 base license entitlement. Licenses attached to the original MAS MiCC Office base are lost.
- Licenses over and above those tied to the original base license will remain available for use.
- The MAS service and the MAS MiCC Office service will be removed from the ARID.

iii. Re-purpose or upgrade the MAS server.

iv. Install and configure MiCC Office on the destination server.

v. Use the MiCC Office Backup Tool to restore MiCC Office data to standalone or virtual MiCC Office.

b. To apply the multi-application MAS migration part number:

i. Go to the AMC.

ii. Create a new ARID on the AMC.

iii. Assign the conversion part number to the new ARID.

iv. From the Application Record Information page for the original ARID on the AMC, choose the 'Reassign product' option to transfer all purchased MICC OFFICE licenses over and above the base license entitlement to the new ARID.

v. Once the licenses have been transferred, continue with the MICC OFFICE migration (see Steps vi - viii below).

vi. After the MICC OFFICE migration has been completed, apply the MAS MICC OFFICE removal part number to the original ARID to remove the MICC OFFICE service from that ARID.

vii. Applying the appropriate removal part number to the existing MICC OFFICE MAS ARID will:

- Remove the MAS MICC OFFICE service from the original MAS ARID after which the MAS ARID may optionally be converted to a Virtual MAS ARID. See the *Mitel Applications Suite Installation and Maintenance Guide* for information on converting MAS to Virtual MAS.

viii. Install and configure MICC OFFICE on the destination server.

ix. Use the MICC OFFICE Backup Tool to restore MICC OFFICE data to standalone or virtual MICC OFFICE.

x. Re-purpose or upgrade the MAS server.

CONFIGURING THE SERVER COMPUTER FOR NETWORKING

This section describes the steps needed to configure networking on the MiCC Office Server computer.

NAME RESOLUTION

Other computers must be able to resolve the Server's computer name. Use the following methods to test the name resolution capability of the installation.

CHECKING THE NAME RESOLUTION

The quickest way to verify MiCC Office Server computer name is to use another computer and select **Run** from the Windows Start menu. Then enter the name of the computer you are trying to locate (e.g., to check for MICCOSERVER-01, enter `\\MICCOSERVER-01`). If an Explorer window appears with a MICCO_DISKS folder listed, the name can be resolved.

If you can resolve the computer name, your network configuration should be correct for the other MiContact Center Office products. If you cannot resolve the name, see the following section.

ENABLING NAME RESOLUTION

If you cannot resolve the name of the MiCC Office Server computer from another computer, you must address name resolution issues. How you accomplish this depends on your current network configuration.

Microsoft TCP/IP can resolve names using one of several methods. When attempting to resolve names, the recommended order is as follows:

- HOSTS File
- DNS
- WINS Server
- Broadcast
- LMHOSTS File

Your network administrator should know which of resolution methods should work with your network. If name resolution is failing from one computer to the MiCC Office Server computer, and that computer can see other computers on the network, the Server may be running on a different LAN segment. In this situation, use WINS, DNS, or a HOSTS file to specify the address of the computer to resolve the issue.

Another possible problem is that the computer “sees” the Server, but it does not recognize the name. If you can successfully ping the Server’s IP address (using a command line similar to PING 198.168.128.1), updating WINS, DNS, or the HOSTS file should resolve the issue. Your network administrator should know how to update these settings. If you cannot successfully ping the computer, the error is more severe, and you should ask your network administrator for assistance.

Your network administrator should know which of these resolution methods should work with your network. If name resolution is failing from one computer to the MiCC Office Server computer, and that computer can see other computers on the network, the Server may be running on a different LAN segment. In this situation, use WINS or an LMHOSTS file to specify the address of the computer to resolve the issue.

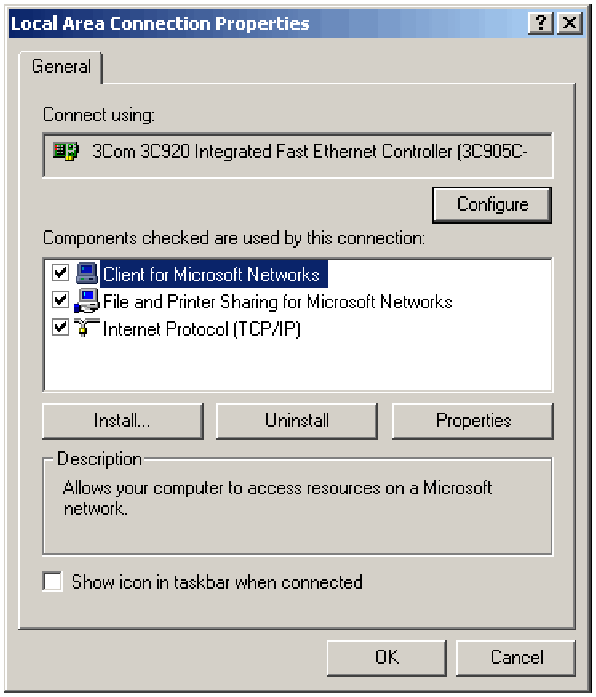
If the Server computer is on the same LAN segment, but the other computer still cannot be seen over the network, check your network settings on both the Server and the computer that is attempting to resolve the name. Ensure they are using the same network protocol and are bound to adapters that are connected to the same part of the LAN. If this does not work, contact your network administrator.

SHARED FOLDERS

After you resolve the computer name, you must verify that the MiCC Office Server's shared folder is accessible. Server configures the share when it is installed.

To ensure that the share is valid:

1. Ensure that **Client for Microsoft Networks** and **File and Print Sharing** are enabled in the Network and Dial-up Connections, Local Area Connection Properties, as shown below.



Local Area Connection Properties

General

Connect using:

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☐ Show icon in taskbar when connected

2. Ensure that the folder where the MiCC Office client installation is located is shared as MICCO_DISKS with access to the necessary users.

If the shared folder is still not available over the network, ensure that the other computers and Server computers are logged on to the network. Also verify that they can "see" other computers on the network. For additional assistance, contact your network administrator.

CONFIGURING MICC OFFICE SERVER

This section describes the options for configuring MiCC Office Server and includes:

- “SmartSync Configuration (MiVoice Office 250 Only)” on page 40.
- “Data Manager Manual Configuration” on page 41.

SMARTSYNC CONFIGURATION (*MIVOICE OFFICE 250 ONLY*)

For Server to work correctly, the telephone system configuration must be entered into the Data Manager within the Agents, Hunt Groups, Extensions, and Trunk Lines views.

When connecting to a Mitel MiVoice Office 250, the SmartSync feature automatically downloads most of this information from the telephone system. The SmartSync functions that are automatically performed for each type of Server device are detailed throughout this section.

SmartSync synchronizes with the telephone system when Server detects that a device has been added, changed, or deleted. SmartSync then queries the telephone system and updates the records stored in Server.

SmartSync does not automatically set up the information listed below. You must manually enter this information using the Data Manager.

- DID/DDI numbers
- Media Blending configuration, including agent and group e-mail addresses
- Call Recording channels, including extensions or trunk lists
- Internal call modeling of extensions

Full automatic download is provided as well as support for immediate live synchronization when extension devices or voice mail applications are added, changed, or deleted on the telephone system. The SmartSync functionality is supported across a single node or an entire networked system when the CT Gateway is employed, regardless of how many nodes there are or whether Server is running in node aware mode or not.

SmartSync will automatically query the phone system for hunt group information. This automatic download and synchronization works for all hunt groups across the entire phone system when Server is operating in either a single-node or multi-node environment (when node aware).

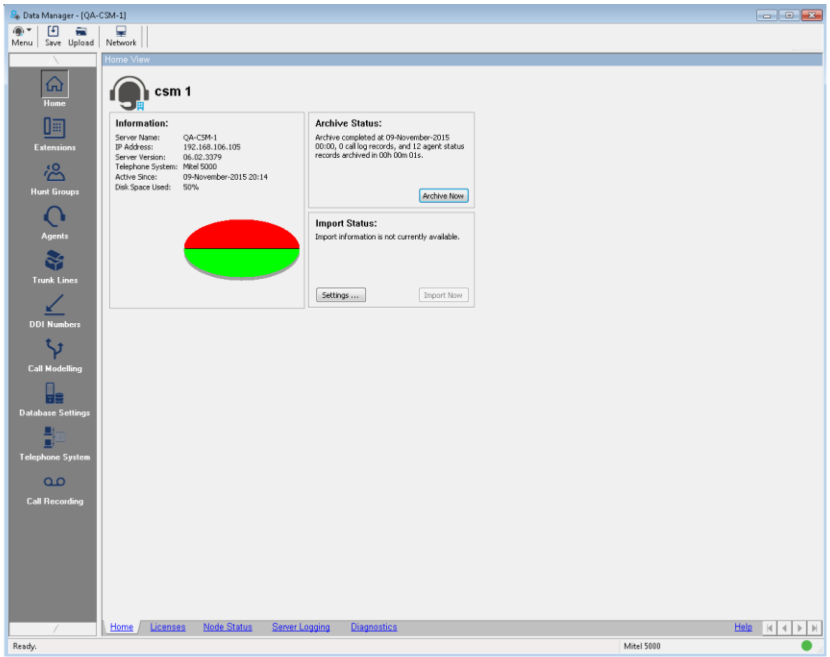
If Server is operating in a multi-node environment but is not node aware, only the hunt groups for one node are downloaded. Although the node for which the hunt groups are downloaded is arbitrarily chosen, it usually corresponds to the lowest active node number.

DATA MANAGER MANUAL CONFIGURATION

To manually configure devices or to access other settings, you must use Data Manager.

To open Data Manager, right-click the MiCC Office Server tray icon (▨), and then select **Data Manager**. The Data Manager Home View appears.

Figure 4: Data Manager Interface



Information:

Server Name: QA-CSM-1
IP Address: 192.168.106.105
Server Version: 06.02.3379
Telephone System: Mitel 5000
Active Since: 09-November-2015 20:14
Disk Space Used: 50%

Archive Status:

Archive completed at 09-November-2015 00:00, 0 call log records, and 12 agent status records archived in 00h 00m 01s.

Import Status:

Import information is not currently available.

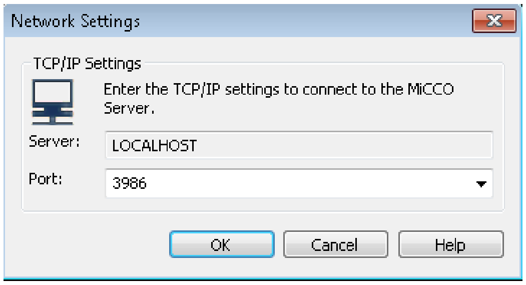
Ready.

Mitel 5000

Access each view in Data Manager by clicking the view buttons on the left panel. Depending on the view you have selected, the main panel may contain links along the bottom to access additional information and/or options. For example, on the Agents View, there are links to Add, Change, Delete, and Delete Range. Before clicking the **Change** or **Delete** options, select an item from the display.

To access network settings for Server, select the **Network Settings** icon (🖳) from the Data Manager Toolbar. The Network Settings screen appears.

Figure 5: Network Settings Dialog Box



Network Settings

TCP/IP Settings

Enter the TCP/IP settings to connect to the MiCCO Server.

Server: LOCALHOST

Port: 3986

The network settings for Server are already configured and cannot be changed from here. The port is set to the default for MiCC Office, click **OK** to return to the Data Manager screen.

Chapter 6

ADMINISTRATION AND MAINTENANCE

INTRODUCTION

This chapter provides administration and maintenance information for MiContact Center Office and the Applications.

SETTING SECURITY LEVELS

MiContact Center Office includes a security feature that limits the information and programming areas that specific users can access. This feature ensures that specific configurations and call information are available only to those with the proper security level.

To accommodate a variety of users, MiContact Center Office allows you to program three different password levels using the Control Panel applet (see “Programming Passwords” on page 110 for details):

- **User**: Provides limited access to certain modules and is designed to provide basic call control and real-time information. Users can configure only specific areas of RealViewer and CallViewer.
- **Supervisor**: Includes limited access to all modules and is designed for individuals who require access to detailed information but who are not responsible for programming the modules. Supervisors can configure specific areas of all modules except Intelligent Router
- **Administrator**: Provides full access to all modules. This level is designed for installers and individuals, such as System Administrators, who program and maintain the modules.

> **Note:** If you set a supervisor password, you must also set an administrator password. If you set a user password, you must also set both supervisor and administrator passwords.

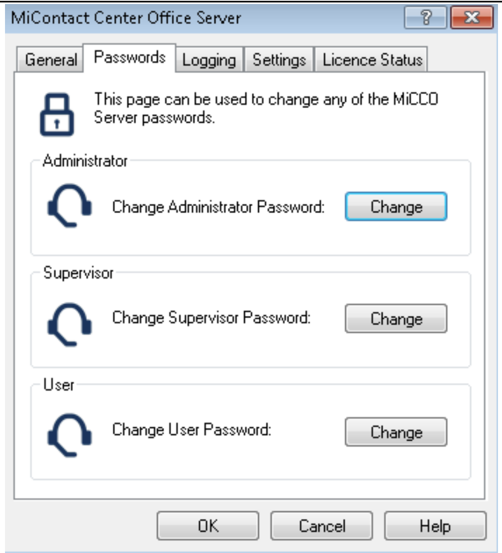
If passwords are not programmed for each level, when you start the application, you are automatically given access to the highest level that does not have a password. For example, if there is no User password, you automatically have user privileges. If there are no User and Supervisor passwords, you automatically have supervisor privileges. If no passwords are programmed, you have full administrator access. For this reason, Mitel recommends that you program the Administrator password at a minimum.

PROGRAMMING PASSWORDS

The password levels are programmed using the MiCC Office Control Panel applet.

To program passwords:

1. Open the MiCC Office Control Panel and click the **Passwords** tab. The Passwords screen appears.



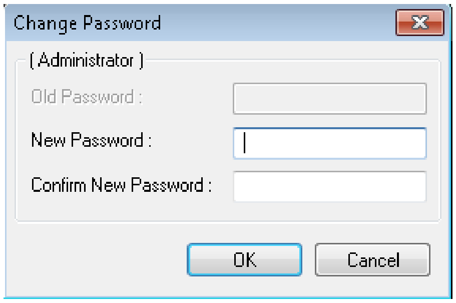
This page can be used to change any of the MiCCO Server passwords.

Change Administrator Password:

Change Supervisor Password:

Change User Password:

2. For all three password levels, click **Change** to change the password. The following dialog box appears.



Old Password :

New Password :

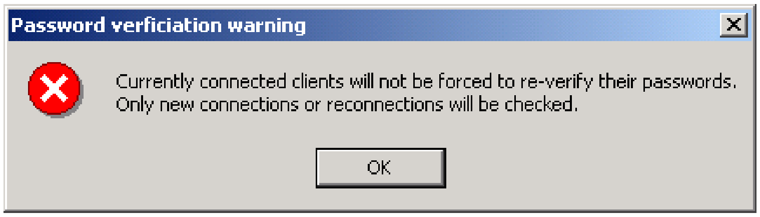
Confirm New Password :

3. Enter the password in the **New Password** and **Confirm New Password** text boxes. The screen displays asterisks (***) in place of the entered characters.

Note: If you are changing an existing password, the **Old Password** text box is enabled. You must enter the existing password in the **Old Password** field to change the password. To be able to change settings in the MiCC Office Server Control Panel, including the passwords, you must have logged into the Server PC with a user name and password that provide Windows Administrative privileges.

4. Click **OK** when finished or click **Cancel** to exit without saving the password. You are returned to the Control Panel Passwords screen.

5. Click **OK** to acknowledge the password verification warning shown below:



Currently connected clients will not be forced to re-verify their passwords. Only new connections or reconnections will be checked.

Note: The new password does not take effect until the user logs off the application, and then logs in again. You need to provide the new password to the user before they can log into the application again.

6. Click **OK** when finished or click **Cancel** to exit without saving any changes.

To clear a password:

1. Access the MiCC Office Control Panel and click the **Passwords** tab. The Passwords screen appears.
2. Click **Change** next to the appropriate level. The Change Passwords dialog appears.
3. Enter the current password in the **Old Password** text box. Leave all other boxes blank.
4. Click **OK** to return to the Control Panel Passwords screen.
5. Click **OK** to save your changes. The password is erased.

USING PASSWORDS TO RUN APPLICATIONS

With the exception of Intelligent Router, all applications require a password on startup when all three password levels (Administrator, Supervisor, and User) have been set up. The password not only allows the module to connect to Server, but it determines the features to which you have access. After you are logged into Server, however, you can change the password level (see “Changing Password Levels” on page 113).

When using Data Manager, you are prompted for a password only if the Supervisor password has been set. If an Administrator password has been set but a Supervisor password has not, you have read-only access until you choose to change the password level.

A password is not required to start Intelligent Router. This is because these applications are crucial to call centers and must be running at all times. After the application is running, however, a password is required to access programming areas (see “Unlocking Configurations” on page 113 for information about the Intelligent Router exception to this).

The Administrator password provides access to all features.

ENTERING PASSWORDS

When you start any application other than Server or Intelligent Router, the Password Required dialog box appears.

Enter the correct password and click **OK**. If the password is valid, the application connects to Server, and you are granted access to the specific areas authorized for your level. If the password is invalid, the application does not connect to Server and an error message appears.

To access a level that does not have an assigned password, click **Cancel** when prompted for the password. You are automatically given access based on the highest level that does not have a password, unless you are changing the password level (see below).

VIEWING PASSWORD LEVELS

If you enter a password, MiContact Center Office grants access to particular features in the application and stores your password information. You can select **About** from the main menu to view the current password level.

The current password level appears in the Current Password Level field. This field displays *[None]* if a password was not entered.

CHANGING PASSWORD LEVELS

If desired, you can change the password level while in any application other than Server.

To change levels:

1. Select **Change Password Level** from the main menu. The Enter Password dialog appears.
2. Enter the password associated with the desired level, and then click **OK**. The new level of access is available until you change the password or close the application.

Note: If you are using the Administrator password to program the application, make sure you change the password level when finished. If you do not change the password level, others will have full access to the application. This is especially important for Data Manager and Intelligent Router.

UNLOCKING CONFIGURATIONS

Intelligent Router prompts you for a password whenever you access a new area of that application. This functionality ensures that anyone can start the application but that all configuration areas remain secure. If, however, you are programming multiple rules and actions, you can unlock the configuration so that you are only prompted once for the password. After you have finished programming the application, you can lock the configuration again so that others are prompted for the password.

Note: The Administrator password is required to unlock the configuration.

To unlock the configuration:

1. Select **Unlock Configuration** from the main menu. The Enter Password dialog appears.
2. Enter the Administrator password and click **OK**.

To lock the configuration, select **Lock Configuration** from the File menu. When prompted, click **OK**.

PASSWORD ACCESS TO FEATURES

The following tables list the features that are available when all three password levels have been set and the User or Supervisor password is entered. The Administrator password has access to all features. In the tables, √ = supported, and X = not supported.

SERVER

Server does not require passwords because it runs as a Windows service. You can however, configure passwords for other applications. See “Programming Passwords” on page 110.

DATA MANAGER

If all three passwords have been set in Control Panel, you need to log in to access Data Manager, where most of the configuration is done. Data Manager will prompt for a password only if a Supervisor password set. If only an Administrator password is set, Data Manager automatically enters read-only mode (effectively obtaining default supervisor access). The Supervisor has only read-only access, which does not allow changes or perform action such as importing or forcing an archive. An Administrator password is needed to make any changes or force imports, etc.

INTELLIGENT ROUTER

Table 1 provides a list of features supported for users and supervisors. Administrators have access to all features.

Table 1: Intelligent Router Password Access

FEATURE	USER	SUPERVISOR
Sizing/Positioning Tiles	√	√
Configuring Network Settings	√	√
Accessing Rule List Properties	√	√
Accessing Event List Properties	√	√
Accessing Contact List Properties	√	√
Accessing Multi-Stat Tile Properties	√	√
Configuring Options (General and Advanced Tabs)	√	√
Configuring Media Blending	X	X
Accessing Filter Manager	X	X
Adding, Editing, and Removing Filters	X	X
Applying All Calls Filter to Contact List	X	X
Accessing Rule Manager	X	X
Adding, Editing, and Removing Rules	X	X
Enabling/Disabling Rules	X	X

Note: If you are programming a lot of rules and actions in Intelligent Router, it is recommended that you unlock the configuration.

CALLVIEWER

Table 2 provides a list of features supported for users and supervisors. Administrators have access to all features.

Table 2: CallViewer Password Access

FEATURE	USER	SUPERVISOR
Adding and Editing Actions	X	√
Adding and Editing Rules	√	√
Adding and Editing Buttons	√	√
Adding and Editing Hot Keys	√	√
Configuring Options (Call Control and Dial Rules)	X	√
Configuring Options (Call List Fields, Call List Buttons, and Call Log Fields)	√	√
Configuring Options (Miscellaneous) * Only an administrator can configure the **Display caller details on DSS tooltips** option.	√*	√*
Configuring Options (Locations)	X	X
Configuring Options (License)	√	√
Configuring Options (Devices) ** Only an administrator can configure the device to which CallViewer is assigned.	√**	√**
Configuring Network Settings	√	√

REALVIEWER

Table 3 provides a list of features supported for users and supervisors. Administrators have access to all features.

Table 3: Realviewer Password Access

FEATURE	USER	SUPERVISOR
Adding and Editing Deskboard Tiles	X	√
Adding and Editing RealViewer Tiles	X	√
Adding, Editing, and Removing Filters	X	X
Applying Filters to Tiles	X	√
Configuring Options (General and Advanced Tabs)	√	√

Table 3: Realviewer Password Access (continued)

FEATURE	USER	SUPERVISOR
Configuring Options (Account Codes, Durations, Licensing, Service Levels, and Tiles Tabs)	X	√
Accessing Network Settings	√	√

REPORTER (HISTORIC)

Table 4 provides a list of features supported for users and supervisors. Administrators have access to all features.

Table 4: Reporter Password Access

FEATURE	USER	SUPERVISOR
Adding, Editing, and Removing Reports	X	√
Applying Filters to Reports	X	√
Applying All Calls Filter to Reports	X	X
Accessing Filter Manager	X	X
Adding, Editing, and Removing Filters	X	X
Adding, Editing, and Removing Tariffs	X	√
Configuring Options	X	√
Changing the License Setting	X	√
Accessing Network Settings	X	√
Importing Filters, Reports, etc.	X	X
Exporting, Publishing, and E-mailing Reports	X	√
Adding, Editing, and Removing Auto Reporter Schedules	X	√
Adding, Editing, and Removing Auto Reporter Sites	X	X

REPORTER REAL-TIME

Table 5 provides a list of features supported for users and supervisors. Administrators have access to all features.

Table 5: Reporter Real-Time Password Access

FEATURE	USER	SUPERVISOR
Adding and Editing Deskboard, Multi-Stat, Graph, Extension List, Agent List, Trunk List, and Contact List Tiles	X	√
Adding and Editing StationViewer, Extension Detail, and Agent Detail Tiles	X	X
Accessing Filter Manager	X	X

Table 5: Reporter Real-Time Password Access (continued)

FEATURE	USER	SUPERVISOR
Adding, Editing, and Removing Filters	X	X
Applying Filters to Tiles	X	√
Applying All Calls Filter to List-Based and Graph By Device Tiles	X	X
Configuring Options (General, Advanced, Account Codes, Durations, Service Levels, and Tiles Tabs)	X	√
Configuring Options (Call Control Tab)	X	X
Accessing Network Settings	X	√
Adding, Editing, and Removing Auto Reporter Schedules	X	√
Adding, Editing, and Removing Auto Reporter Sites	X	X
Enabling Connected Party Flag for StationViewer Tiles	X	X

PERFORMING BACKUP AND RESTORE OPERATIONS

This section provides the required information and procedures for performing backup and restore operations for MiCC Office.

Mitel is not responsible for database backups. It is the responsibility of the customer to routinely back up the MiCC Office server database and Intelligent Router settings. A UPS on the server is recommended for situations such as ungraceful shutdowns that may cause database corruption.

BACKING UP AND RESTORING MICC OFFICE

Use the MiCC Office Backup Tool to routinely backup the MiCC Office Server database and Intelligent Router settings. The MiCC Office Server databases are used to store daily, current month, historic call log, and agent status log information.

The MiCC Office Backup Tool can also be used to restore the MiCC Office Server database and Intelligent Router settings from a previous backup.

When Virtual MiCC Office is running in a VMware vSphere environment, VMware provides the capabilities to back up virtual disks on virtual machines. These virtual machines can be running or not, and the backup is referred to as an image level backup. This type of backup is different from what the MiCC Office Backup Tool provides, which is an application level backup. VMware Data Recovery or a third party backup tool is used to create an image level backup. See Image Level Backup and Restore on page 131 for additional information.

Note: The date format of the source MiCC Office Server and the new MiCC Office Server must be the same for the backup and restore operation to succeed. For example, DD.MM.YYYY and MM.DD.YYYY would not work but MM.DD.YYYY and MM.DD.YYYY would.

The Backup tools are installed at the same time as the MiCC Office Server is installed. There are two types of backup tool provided by MiCC Office:

- Desktop Backup Utility & Service
- Command Line Tool

The command line tool is legacy tool used for making backups. This tool has been kept in the solution for backwards compatibility. The desktop Backup Utility application controls the Backup Utility service. The Backup Utility Service runs manual and automated backups.

USING THE MICC OFFICE BACKUP UTILITY

The Backup Utility is made up of two separate applications:

- Desktop Application
- Windows Service

The windows Service runs all the time and will perform automated backups and manual backup/restore operations requested by the desktop application. The desktop application is used to configure:

- Scheduling of backups
- SMTP notifications
- View backup history and restore backups if necessary

By default, the Backup Utility is configured to created scheduled backups at 4am every morning. The backups are stored in the following location:

C:\ProgramData\Mitel\Customer Service Manager\Backups

By default, the Backup Utility will keep 5 backups, deleting older backups when new ones are created.

The Backup Utility supports storing backups on a share on another server. This is a recommended configuration to minimize the potential for data loss due to hardware failure. If a network share is being used then the target path should be a UNC path. User credentials can be provided for accessing the share.

Note: You need to restore from a local drive not a network share. If you need to restore a backup from a network share copy it locally first and then do the restore

USING THE COMMAND LINE MICC OFFICE BACKUP TOOL

The MiCC Office Backup Tool requires administrative privileges to run, so you must run the backup tool from an administrator command window.

1. Perform one of the following tasks depending on your operating system:
   - To launch an administrator command window on Windows, right click on the command window shortcut and select **Run as administrator**.
   - To launch an administrator command window on earlier versions of Windows. perform one of the following options:
     - Log in as an administrator and open the command window.
     - Right-click the command window shortcut and select **runas**.
2. From the command prompt, navigate to ‘C:\Program Files (x86)\Mitel Customer Service Manager\Backup Tool’ then enter csmbackup.exe followed by a space and then enter one of the options in the table. Alternatively, enter ? for a complete list of options.

The command options tell the MiCC Office Backup Tool what operation to perform. Exactly one command option must be specified for each invocation of the backup tool. The supported command options are described in the table below. Or, enter ? for a complete list of options.

COMMAND OPTION	DESCRIPTION
--backup <full path to backup directory>	Perform a backup operation and place the backup file in the specified directory. The backup location may be a network share specified in Universal Naming Convention (UNC) format
--restore <full path to backup file>	Perform a restore operation using the specified backup file. The backup file may be located on a network share. To use a backup file on a network share, the path must use the UNC format.
--diskspace	Estimate the amount of local disk space required to perform a backup. This provides only an estimate. The actual disk space required may be more or less depending on the contents of the files being backed up. The estimate includes space required for temporary files. The resulting backup file will be smaller than the estimated disk space.
--help	Display usage information.
--dsttemp	If you are backing up to a drive other than 'C:\', this will create the temp files on the same drive as the target path rather than 'C:\'

The MiCC Office Backup Tool shows the progress of the backup or restore operation. For certain operations (such as a normal DB2 backup or restore), progress indication is shown as a spinning character (which is actually a continual output sequence of the characters "|", "/", "-", and "\"). As long as the progress indicator is "spinning", the MiCC Office Backup Tool is still working and should not be cancelled.

IMAGE LEVEL BACKUP AND RESTORE

Image level backup and restore on a virtual machine running in a VMware vSphere environment is different from using the MiCC Office Backup Tool. VMware Data Recovery or a third party backup tool is used to create an image level backup. Refer to the VMware Data Recovery Administration Guide for information on how to perform an image level backup of a virtual machine. Table 1 below provides guidance on the recommended types of backups for virtual MiCC Office.

Table 6: Recommended backup methods for virtual MiCC Office

BACKUP SCENARIO	RECOMMENDED BACKUP METHOD
Day-to-day backup for Application Data Recovery	From most- to least-recommended, only one method to be used: 1 - Application level backup using the MiCC Office Backup Tool 2 - VMware Data Recovery (scheduled) 3 - Third-party backup software using VADP if available 4 - Export/Import OVA
Re-Deploying a new version of virtual MiCC Office 6.0 with a new release	Application level backup using the MiCC Office Backup Tool
Migrating to/from standalone MiCC Office 6.0	Application level backup using the MiCC Office Backup Tool
Migrating from MiCC Office 5.x	Application level backup using the MiCC Office Backup Tool

Image level backups of a running Virtual MiCC Office on Windows Server 2008 R2 are supported. Image level backup software that makes use of VMware's vStorage APIs for Data Protection, including the VMware Date Recovery tools, are supported with Virtual MiCC Office.

To properly perform an image level backup, the backup software (using VMware tools or some other Microsoft Volume Shadow Copy Service (VSS) provider) must be configured to first bring the virtual machine's file system is quiescent (into a quiet or non-busy state). If the file system is not put in such a state, the MiCC Office database and the server applications' settings files may be corrupted and the backup image of the virtual machine may not be able to be restored. If Virtual MiCC Office is under load, then the backup may fail.

Note: Image level backups are not supported for Virtual MiCC Office that is packaged as an OVA file. This is due to a limitation of the VMware's VSS provider on the Windows 7 and Windows 8 platform.

MiCC Office support for Microsoft VSS service is specifically designed for creating consistent image level backups of running virtual machines. Image level backup implementation is supported with the following limitations:

- Microsoft's Backup Utility and other file level backup software that use the VSS service are not supported.
- Virtual MiCC Office's VSS implementation only works with full backup types.
- backup types such as incremental, differential, etc. are not supported.
- The VSS implementation is only installed on virtual MiCC Office on Server 2008 R2.

When an image level backup starts, the Microsoft VSS takes snapshots of each volume on the virtual disk. While these snapshots are being created, the following MiCC Office operations cannot be performed:

- Archiving the MiCC Office database.
- Importing/exporting historical data to/from the MiCC Office database.
- Performing a database warehousing operation.
- Performing a telephone import operation.
- Performing another backup using the MiCC Office Backup Tool.
- Performing a license sync operation with the AMC.
- Performing a backup of the MiCC Office database.
- Modifying the configuration of the MiCC Office Server or Intelligent Router.
- Running historical reports.

Once the snapshots are complete, MiCC Office continues normal operation. During an image level backup, the MiCC Office Server and applications behave the same as if initiated by the MiCC Office Backup Tool.

All MiCC Office data and settings are backed up during an image level backup, including the MiCC Office database as well as Intelligent Router's settings files and registry settings. A manual back up of any MiCC Office components is not necessary when performing an image level backup.

Note: When performing an image level backup of Virtual MiCC Office, the MiCC Office database and Media Blending operations typically come back online quicker than using the MiCC Office Backup Tool. This is because the VSS snapshot usually only take a few seconds to complete which is done before the actual backup. MiCC Office is free to resume normal operations after the snapshot. Using the MiCC Office Backup Tool requires MiCC Office to wait for the entire backup to complete.

BACKING UP AND RESTORING APPLICATIONS

It is recommended that users complete regular data backups to a secondary device, such as a local network drive. This section provides the list of files that should be included in application backups and the backup/restore procedures.

BACKUP FILES

Table 7 provides the settings files that should be included in a routine backup. When completing your backups, include both user-specific *and* default settings in your backup. File locations are as follows:

- User-specific settings are located in the following directories:
  - **Windows 7 onwards:** `C:\Users\<username>\AppData\Roaming\Mitel\Customer Service Manager\<application name>\Settings.`

Table 7: Per-User Settings Files

APPLICATION	FILE NAME
CallViewer	actions.ccd
	buttons.ccd
	features.ccd
	hotkeys.ccd
	rules.ccd
	cvruser.ini
RealViewer	realvwr.cvd
	realviewer.flt
	rvruser.ini

Table 7: Per-User Settings Files (continued)

APPLICATION	FILE NAME
Reporter	default.cvd
	reports.cvd
	wizlink.cvd
	intlrpt.cvd
	callcost.cvd
	netlink.evt
	reporter.flt
	rptuser.ini
Reporter Real-Time	reporterrt.cvd
	rtlink.cvd
	rtlink.evt
	rtalarm.evt
	reporterrt.flt
	rtuser.ini
Auto Reporter	autorptruser.ini
	wizlink.cvd
	rtlink.cvd

If any of the `.ini` files were modified after the clients were installed, include them with your back up. This ensures that the modifications contained in the .ini files are retained when you restore the data.

Table 8 provides the list of default MiCC Office `.ini` files. From CSM 5.1, `.ini` files are split as per-computer and per-user files, and are located in the following directories:

- Per-computer `config` files:
    - *Windows 7 onwards*: `C:\ProgramData\Mitel\Customer Service Manager\<application name>\Settings`

Table 8: Config Files

APPLICATION	FILE NAME
CallViewer	callviewer.ini (per-computer)
	cvruser.ini (per-user)
	cvolkbtn.ini (per-computer)
	cvolkbtnuser.ini (per-user)
	cvlink.ini

Table 8: Config Files (continued)

APPLICATION	FILE NAME
RealViewer	realviewer.ini (per-computer)
	rvruser.ini (per-user)
Reporter	reporter.ini (per-computer)
	rptuser.ini (per-user)
	autorpt.ini (per-computer)[a]
	autorptuser.ini (per-user)[a]
Reporter Real-Time	reporterrt.ini (per-computer)
	rtuser.ini (per-user)
	autorpt.ini (per-computer)[a]
	autorptuser.ini (per-user)[a]
SMTP	smtp.ini (per computer)
BackupTool	setting.xml (per computer)

[a] Auto Reporter .ini files are shared between Reporter and Reporter Real-Time.

BACKUP AND RESTORE PROCEDURES

This section provides the backup and restore procedures for the following applications:

- CallViewer
- RealViewer
- Reporter
- Reporter Real-Time

To perform a backup operation for an application:

1. On the computer where the application resides, close the application.
2. Navigate to the location of the required backup files (see Table 7 and Table 8).
3. Copy the required files for the application backup.
4. Save the files to the backup location (on a secondary storage device or network drive).

To perform a restore operation for an application:

1. On the computer where the application resides, close the application.
2. Navigate to the location where you saved the backup files.
3. Copy the files (see Table 7 and Table 8) from the backup location.
4. Save the files to the appropriate location on the computer where the application resides.

USING CALLVIEWER SIMULATION MODE

Simulation mode allows a macro writer to simulate calls and e-mail without being connected to a MiCC Office Server, or possibly even on site. The simulation window is not available by default.

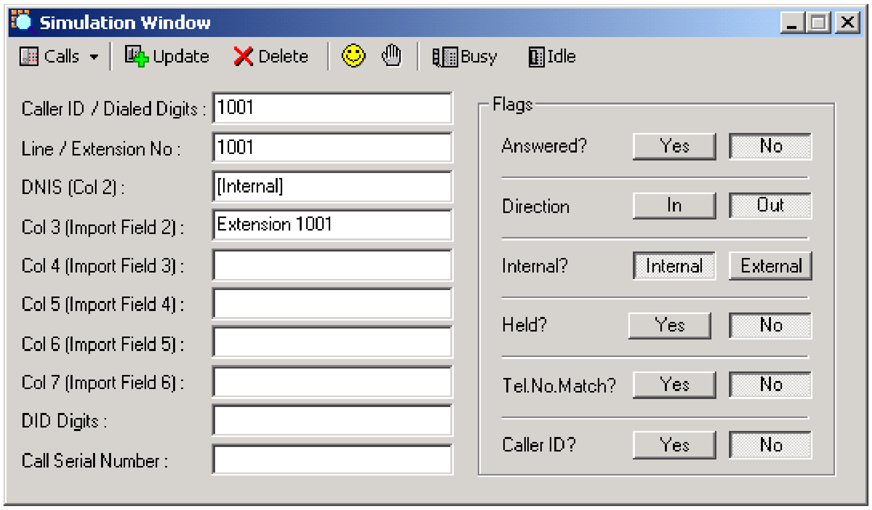
The buttons used to simulate calls are described in the following table.

Table 9: Simulation Mode Buttons

BUTTON	DESCRIPTION
▦ Calls ▾ ✉ E-mails ▾	Event Type
▦✚	Update
✗	Delete
☺	Answer
✋	Hold
▥	Busy
▯	Idle

To set up simulated calls:

1. Open CallViewer.
2. From the **Options Call Control** tab, check the **Enable simulation mode** option.
3. If the simulation window does not appear automatically, click **OK** to access it.
4. If the E-mails window appears, click the ✉ E-mails ▾ drop-down button and choose **Calls.** The simulation window appears, as shown below.



Simulation Window

Caller ID / Dialed Digits : 1001
Line / Extension No : 1001
DNIS (Col 2) : [Internal]
Col 3 (Import Field 2) : Extension 1001
Col 4 (Import Field 3) :
Col 5 (Import Field 4) :
Col 6 (Import Field 5) :
Col 7 (Import Field 6) :
DID Digits :
Call Serial Number :

Flags
Answered? Yes [✓ No]
Direction In [✓ Out]
Internal? [✓ Internal] External
Held? Yes [✓ No]
Tel.No.Match? Yes [✓ No]
Caller ID? Yes [✓ No]

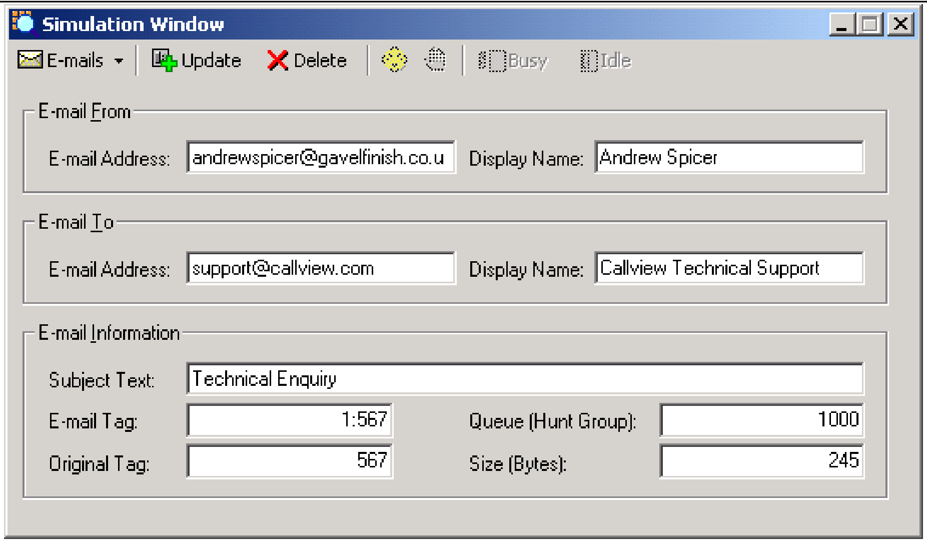
5. Program the following fields for the conditions you want to simulate in a call:
   - Caller ID / Dialed Digits

- Line / Extension No.
- DNIS (Col 2)
- Col 3 (Import Field 2)
- Col 4 (Import Field 3)
- Col 5 (Import Field 4)
- Col 6 (Import Field 5)
- Col 7 (Import Field 6)
- DID Digits
- Call Serial Number
- Answered?
- Direction
- Internal?
- Held?
- Tel.No.Match?
- Caller ID Received?

6. Using the buttons on the toolbar, choose from the following options to simulate call or e-mail activity:
   - **Update**: Takes the options set above and simulates the specified event.
   - **Delete**: Ends the simulated event using the specified information.
   - **Answer**: Toggles the answer flag on the “calls” part of the window, and sends the simulated event at the same time. When the e-mail event is selected, the button will be disabled.
   - **Hold**: This button will toggle the hold flag on the “calls” part of the window, and send the simulated event at the same time. When the e-mail event is selected, the button will be disabled.
   - **Busy**: This will simulate the user picking up the handset. (Not available for simulating e-mail events.)
   - **Idle**: This will simulate the user putting down the handset. (Not available for simulating e-mail events.)

To set up simulated e-mail messages:

1. From the **Options Call Control** tab, check the **Enable simulation mode** option.
2. If the simulation window does not appear automatically, click **OK** to access it.
3. If the Calls window appears, click the Calls ▾ list and choose **E-mails**. The simulation window appears, as shown below.



E-mail From

E-mail Address: andrewspicer@gavelfinish.co.u

Display Name: Andrew Spicer

E-mail To

E-mail Address: support@callview.com

Display Name: Callview Technical Support

E-mail Information

Subject Text: Technical Enquiry

E-mail Tag: 1:567

Queue (Hunt Group): 1000

Original Tag: 567

Size (Bytes): 245

4. Program the following fields for the conditions you want to simulate in an e-mail:

- E-mail From Address
- E-mail From Display Name
- E-mail To Address
- E-mail To Display Name
- Subject Text
- E-mail Tag
- Queue (Hunt Group)
- Original Tag
- Size (Bytes)

Simulate e-mail activity using the toolbar buttons described in step 6 of the previous section.

USING REPORTER DEMONSTRATION MODE

You can use a demonstration mode to view the different features of the Reporter application. In demonstration mode, Reporter does not attempt to connect to a MiCC Office Server, and you can choose the license variant to review.

Note: The demonstration call and agent status data shipped with Reporter for use with the “Demonstration Mode” was artificially created. Company names and telephone numbers that are contained within these files and that are shown in Reporter reports are fictional. Any similarity to a company or person, whether trading, living, or otherwise, is purely coincidental.

The demonstration data consists of three months’ worth of call and agent status activity, covering June 1, 2001 to August 31, 2001. Each specific day in a month has the same call and agent activity for all three months (e.g., the call and agent status activity is the same for the 4th of June as it is for 4th of July and August).

The demonstration data represents a fictitious insurance company with the following attributes:

- There are 11 ACD agents.
- There are 20 DID numbers.
- The system has 69 Extensions, including Voice Mail applications.
- The system is programmed for 12 hunt groups.
- There are 12 analog trunk lines and 42 digital trunk lines.
- There is someone available 24 hours per day.
- The company operates seven days per week (receive and make calls at the weekend).
- The site handles approximately 2200 calls per day.
- The company has approximately 1100 existing customers, which are appropriately depicted within the MiCC Office Server’s telephone number list.
- Approximately 10% of inbound/outbound calls have Account Codes (“111”, “222”, ... , “999”) entered against them.
- Approximately 33% of all external calls are inbound.
- Approximately 95% of inbound calls are received with Caller ID.
- Approximately 85% of inbound calls are identified within the MiCC Office Server’s telephone number list.
- Approximately 90% of outbound calls are identified within the MiCC Office Server’s telephone number list.
- Approximately 65% of inbound calls are abandoned by the caller.
- Most inbound calls ring via DID number 8000, which routes the call to an Automated Attendant. The caller then chooses an option from the Automated Attendant menu so that they are transferred to the appropriate internal department (e.g., Operator, Claims, Quotations, etc.).

Additionally, because the demonstration was artificially created, some differences may exist within reports that are run across the demonstration data. For example, the forecasting statistics may not give meaningful values because they rely on call center traffic appropriate for Erlang B and Erlang C calculations. Reports may show calls being transferred between two devices that do not necessarily make sense (i.e., a call being transferred from the "Quotation" call routing announcement to the "Claims" hunt group). Or, two different company names could be shown as having the same telephone number.

When running reports using Reporter's demo mode, you should consider the following:

- Reporter assumes that the "current date" (e.g., today's date) is the current day-of-month for the month of August 2001. For example, if today's date was the 15th of December 2002, then Demo Mode Reporter would run reports for the 15th of August 2001. The dates and times would still display as the December 15, 2002.
- Because Reporter only has three months of data (June to August 2001), you can only report on three months' worth of data. However, Reporter will run all your reports as if they had been run during the demonstration data's report period, as long as you only run reports within the last three months of the current month. For example, in December 2002, you can reports on dates between October and December 2002; in March 2003, you can report on dates between January and March 2003. Additionally, if you run a report for today at midday, you will get statistics for the entire day.

To access demonstration mode, do one of the following:

- Select the Demo option during the installation process.
- Select the Demo Mode license option on the Options dialog License tab.

After you enter demonstration mode, select the licensed features that you want to view. You can also opt to view Auto Reporter features.

To exit demo mode, select a different license option on the Options dialog License tab.

CHANGING FILTER INITIALIZATION BEHAVIOR

You can change the behavior of RealViewer or Reporter Real Time filters to reduce the time it takes to load modules. By default, filters are initialized when they are called upon.

To initialize filters on start up, add the following filter setting in the application in *.ini file:

```
[Advanced]

AutoInitAllFilters=1
```

=1 to initialize all filters at start-up. Setting to =0 initialize filters when they are used. If the [Advanced] header is not already present add it to the ini file at the bottom of the page.

The *.ini file locations:

Reporter Real-Time

c:\ProgramData\Mitel\Customer Service Manager\Reporter\Settings\reporterrt.ini

Real Viewer

c:\ProgramData\Mitel\Customer Service Manager\RealViewer\Settings\realviewer.ini

Use Notepad or any other text editor to add the filter setting in the *.ini file. Close and restart the application if it was open during the editing of the ini file.

Note: This setting will not affect the recalculation of all tiles when a new filter is created or an existing filter is edited.

CHECKING NODE STATUS IN REPORTER REAL-TIME

The node status dialog provides a continually updated view of the state of all nodes in a multi-node telephone switch environment. Each node appears as a single line consisting of a status icon, node number, node description and status text.

When the telephone system is started, each of the nodes is placed in a list. Server processes these nodes sequentially. Nodes that are waiting to be initialized have a Waiting for initialization status associated with them. As Server processes each node individually, the node being processed is moved to the Initializing state. Once initialized, the node is considered active. If the number of licenses that are available is less than the number of nodes in the system, those nodes that exceed the license limit are marked as “Unlicensed.”

Note: On the MiVoice Office 250 system, the node status dialog is only available when Reporter Real-Time is running in conjunction with the Mitel telephone system and Server is connected through the CT Gateway application to a system of networked telephone system nodes. Additionally, Server also needs to be appropriately licensed for the number of telephone system nodes, as depicted by the “Number of Nodes” license.

To access information on node status, from the main toolbar click the Node Status icon (⁖).

Table 10 provides the status icons available for nodes.

Table 10: Node Status Icons

ICON	DESCRIPTION
●	Disabled. This status appears if the node that the status icon depicts, is disabled.
🕒	Waiting for initialization. This status appears if the node that the status icon depicts is waiting for initialization. The node is in the list of nodes that is to be processed by Server.
🟡	Initializing. This status appears if the node that the status icon depicts is being initialized. Server is currently processing the node.
🟢	Active. This status appears if the node that the status icon depicts is active.
🔴	Unlicensed. This status appears if the node that the status icon depicts is unlicensed. Nodes are only marked as being unlicensed if the number of nodes on the system is greater than the number of node licenses that are available.

.

USING STARTUP SWITCHES ON APPLICATIONS

You can control how CallViewer, RealViewer, Reporter, and Reporter Real-Time start by specifying a startup switch on the command line.

For example, the following command line starts CallViewer using an alternative rules file, my_rules.ccd, and shows the Simulation Window:

```
“C:\Program Files\Mitel Customer Service Manager\CallViewer\Callviewer.exe”
SIMULATION RULES=”C:\Program Files\Mitel Customer Service
Manager\CallViewer\my_rules.ccd”.
```

This section describes how to configure startup switches for MiCC Office applications.

NOTICE

Setting the command line options incorrectly could render your installation unusable. If you are unsure of what you are doing, do not do it. Contact your network administrator for assistance.

To configure startup switches for MiCC Office *applications:*

1. From the Start Menu, go to All Programs – Mitel Customer Service Manager.
2. Right-click the application and select **Properties**. The application’s Properties window appears.
3. Click the **Shortcut** tab. In the Target box, you see the path, with `<application name>.exe”` at the end.
4. At the end of the text string in the Target box, and after the ending quote mark, type the startup switch or switches you want to use. Startup switches are provided in the following tables:
    - CallViewer (see Table 11)
    - RealViewer (see Table 12).
    - Reporter (see Table 13).
    - Reporter Real-Time (see Table 14).

    Remember to include a space between additional switches if you use more than one and be certain that the ending quote mark is at the end.
5. Click **OK**.
6. Open CallViewer to test the options you specified.

Note: You can use startup switches with the **Run** command on the Start Menu. Options specified with the **Run** command are only in effect for the current session.

CALLVIEWER

Table 11 includes the startup switches and commands for CallViewer. In the cases where there are multiple formats, you may use either as a startup option.

Table 11: CallViewer Startup Switches

COMMAND/SWITCH	DESCRIPTION
SERVER=*ctiservername* /**SN**:*ctiservernamee*	Specifies a server name to override the network settings. This option can be specified using either the computer's name (e.g., MICC OFFICESERVER), or the computer's IP address (e.g., 192.168.1.128). **NOTE:** This setting is temporary, and is not written to the registry. However, in the network settings, the overridden server is displayed as the server in use.
EXTN=*ext* **/E:***extno* **/L**	Overrides the Extension Device setting in the Network Settings window. The Extension Device setting is used to associate a specific installation of CallViewer to a physical extension device on the telephone system. If you use a question mark instead of an extension (e.g., EXTN=?), CallViewer prompts for an extension, supplying the current extension setting from the registry as the default. If you append a question mark to the extension (e.g., EXTN=217?), CallViewer prompts for an extension, supplying the given extension in the command line as the default. The switches /E and /L are legacy settings from version 3.x that have been replaced with the new EXTN setting, which supports the “?” option. Effectively, “EXTN=217?” is the same as “/E:217 /L” in version 3.x. If you connect to a secure server and do not set the administrator password, this setting will be ignored.
BUTTONS=”*path”*	Allows you to override the default location where button data is stored. By default, buttons are stored in the `buttons.ccd` file that is located in the default installation folder. **NOTE:** It is easier to edit the path settings using the **Locations** tab in Options, however, the command line settings override the **Locations** tab settings. Using this command line option overrides both the filename and the registry setting, e.g., BUTTONS=”C:\My Options\My Buttons.ccd” would store the button file under a new name and new folder, regardless of registry settings. If you specify no path and only a filename, CallViewer will look for the file in the current working folder, as specified by Windows.
RULES=”*path”*	Allows you to override the default location where rule data is stored. By default, rules are stored in the `rules.ccd` file that is located in the default installation folder. **NOTE:** It is easier to edit the path settings using the **Locations** tab in Options, however, the command line settings override the **Locations** tab settings. Using this command line option overrides both the filename and the registry setting, e.g., RULES=”C:\My Options\My Rules.ccd” would store the button file under a new name and new folder, regardless of registry settings. If you specify no path and only a filename, CallViewer will look for the file in the current working folder, as specified by Windows.

Table 11: CallViewer Startup Switches (continued)

COMMAND/SWITCH	DESCRIPTION
HOTKEYS=*"path"*	Allows you to override the default location where hot key data is stored. By default, hot keys are stored in the `hotkeys.ccd` file that is located in the default installation folder. **NOTE:** It is easier to edit the path settings using the **Locations** tab in Options, however, the command line settings override the **Locations** tab settings. Using this command line option overrides both the filename and the registry setting, e.g., HOTKEYS="C:\My Options\My Hotkeys.ccd" would store the button file under a new name and new folder, regardless of registry settings. If you specify no path and only a filename, CallViewer will look for the file in the current working folder, as specified by Windows.
ACTIONS=*"path"*	Allows you to override the default location where action data is stored. By default, actions are stored in the `actions.ccd` file that is located in the default installation folder. **NOTE: v**It is easier to edit the path settings using the **Locations** tab in Options, however, the command line settings override the **Locations** tab settings. Using this command line option overrides both the filename and the registry setting, e.g., ACTIONS="Z:\Company Data\main.ccd" would store the button file under a new name and new folder, regardless of registry settings. If you specify no path and only a filename, will look for the file in the current working folder, as specified by Windows.
READONLY	Entered as a single word on the command line, this code makes action data files read-only, thus stopping the user from creating or editing actions. To make only certain types of files read-only, use A (actions), B (buttons), F (Features), H (Hotkeys), L (Look and Feel for Skins), N (Network), O (Options), or R (rules) as the setting, without spaces between the options. For example, `READONLY=BRH` would make buttons, rules, and hotkeys read-only, but not actions.
SIMULATION **/D**	Enables the CallViewer Simulation Window (previously called the "Debug" window). This is a window that allows you to simulate calls without connecting to the CTI Server. The Simulation Window is a very useful tool for testing automatic macros. When you use this startup switch, an extra menu item, called Simulation Window, appears on the tray bar menu. This can be used to activate the Simulation Window if it does not have the focus or has been closed. Simulation mode can also be initiated from the **General** tab in the Options settings.
NONETWORK **/N**	Instructs CallViewer not to start network services (connect to the CTI Server) on startup, use mainly with the simulation mode. You can manually start network services by choosing Network Settings from the tray bar menu, and then clicking **OK**.

REALVIEWER

RealViewer supports several command line options that are available if the Windows shortcut is used to launch the application. The available command lines are described in Table 12.

Table 12: RealViewer Startup Switches

COMMAND	FUNCTION	EXAMPLES

LOAD	Allows you to specify a report file for the application to load instead of loading the default report (realvwr.cvd). The parameter for this option is the filename of the report to load. If the name contains any spaces, use quotes to surround the name.	`LOAD=”my tiles.cvd”`
		`LOAD=D:\wizdata\reports.cvd`

FILTERS	Allows you to specify a set of report filters for the application to load instead of loading the default filter (realviewer.flt). The parameter for this option is the filename of the filter to load. If this name contains any spaces, use quotes to surround the name.	`FILTERS=”my filters.flt”`
		`FILTERS=D:\wizrtdata\filters.flt`

SERVER	Allows you to override the CTI Server to which RealViewer connects on start up. The parameter of this option is the name of the server as it would be entered in the Network Settings dialog box.	`SERVER=MICC OFFICESERVER`
NOSAVEONCLOSE	Allows you to top users from making change to their configuration by not saving changes to disk.	`NOSAVEONCLOSE=1` Any other parameters for this option are ignored and will not activate the setting.

REPORTER

Reporter supports several command line options that are available if the Windows shortcut is used to launch the application. The available command lines are described in Table 13.

Table 13: Reporter Startup Switches

COMMAND	FUNCTION	EXAMPLES

LOAD	Allows you to specify a report file for the application to load instead of loading the default report (`reports.cvd`). The parameter for this option is the filename of the report to load. If the name contains any spaces, use quotes to surround the name.	`LOAD=”my reports.cvd”`
		`LOAD=D:\wizdata\reports.cvd`

FILTERS	Allows you to specify a set of report filters for the application to load instead of loading the default filter (reporter.flt). The parameter for this option is the filename of the filter to load. If this name contains any spaces, use quotes to surround the name.	`FILTERS=”my filters.flt”`
		`FILTERS=D:\wizdata\filters.flt`

TARIFF	Allows you to specify the call charge (tariff) for the application to load instead of loading the default call charge (`callcost.cvd`). The parameter for this option is the filename of the filter to load. If this name contains any spaces, use quotes to surround the name.	`TARIFF=”my call costs.cvd”`
		`TARIFF=D:\wizdata\charges.cvd`

SCHEDULES	Allows you to specify the Auto Reporter Schedules for the application to load instead of loading the default call schedules file (`netlink.cvd`). The parameter for this option is the filename of the filter to load. If this name contains any spaces, use quotes to surround the name.	`SCHEDULES=”my schedules.cvd”`
		`SCHEDULES=D:\wizdata\schedules .cvd`

SERVER	Allows you to override the CTI Server to which the Reporter connects on start up. The parameter of this option is the name of the server as it would be entered in the Network Settings dialog box.	`SERVER=MICC`
		`OFFICESERVER`
		`SERVER=192.168.128.2`

NOSAVEONCLOSE	Allows you to provide full access to all features of Reporter (limited by license), but any changes made are not saved to disk. This is useful if multiple users are sharing the same report or filter files, and you do not want one user changing the reports for all users when they close.	`NOSAVEONCLOSE=1` Any other parameters for this option are ignored and will not activate the setting.
READONLY	Places Reporter into read-only mode, allowing no changes to filters, reports, or tariffs. System Administrators may find this mode useful for users who are not very computer literate.	`READONLY` When added to the command line, this activates the setting.

REPORTER REAL-TIME

Reporter Real-Time supports several startup switches that are available if the Windows shortcut is used to launch the application. The available command lines are described in Table 14.

Table 14: Reporter Real-Time Startup Switches

COMMAND	FUNCTION	EXAMPLES

LOAD	Allows you to specify a report file for the application to load instead of loading the default report (reporterrt.cvd). The parameter for this option is the filename of the report to load. If the name contains any spaces, use quotes to surround the name.	`LOAD=”my tiles.cvd”`
		`LOAD=D:\wizdata\intlrt.cvd`

FILTERS	Allows you to specify a set of report filters for the application to load instead of loading the default filter (reporterrt.flt). The parameter for this option is the filename of the filter to load. If this name contains any spaces, use quotes to surround the name.	`FILTERS=”my filters.flt”`
		`FILTERS=D:\wizrtdata\intlrt.flt`

SERVER	Allows you to override the CTI Server to which Reporter Real-Time connects on start up. The parameter of this option is the name of the server as it would be entered in the Network Settings dialog.	`SERVER=MICC OFFICESERVER`
		`SERVER=192.168.128.2`

NOSAVEONCLOSE	Allows you to provide full access to all features of Reporter Real-Time (limited by license), but any changes made are not saved to disk.	`NOSAVEONCLOSE=1` Any other parameters for this option are ignored and will not activate the setting.

SCHEDULES	Allows you to specify the Auto Reporter Schedules for the application to load instead of loading the default call schedules file (`rtlink.cvd`). The parameter for this option is the filename of the filter to load. If this name contains any spaces, use quotes to surround the name.	`SCHEDULES=”my rtlink.cvd”`
		`SCHEDULES=D:\wizdata\rtlink.cvd`

PERFORMING UPGRADES

SERVER AND SOFTWARE UPGRADES

The MiCC Office Backup Tool is a new backup/restore command line utility included with all editions of MiCC Office. The tool was designed to help simplify backing up and restoring the MiCC Office server applications. This utility automates backing up and restoring all MiCC Office server applications' per- computer and per-user settings files and registry settings. For standalone and Virtual MiCC Office editions of MICC OFFICE/CCS, the tool backs up and restores the MiCC Office database automatically.

The MiCC Office Backup Tool can only be used to restore a backup to MiCC Office 6.0 or later. It cannot be used to restore a backup to an older version of MiCC Office regardless of which version of MiCC Office the backup was taken from. The contents of the backup file, however, can be extracted and manually restored to a different version of MiCC Office if required.

In order to perform backups of older CSM 5.x systems, the MiCC Office Backup Tool must first be installed on the machine to be backed up. The MiCC Office Backup Tool Setup.exe can either be accessed from the MICCO_DISKS share of an installed version of MiCC Office 6.0 or it can be extracted from the standalone zip file.

TO INSTALL THE MICC OFFICE BACKUP TOOL:

1. Launch the MiCC Office Backup Tool Setup.exe. The Setup Wizard begins and the Welcome page displays.
   Click **Next**. The License Agreement screen displays.
2. Accept the License Agreement.
   Click **Next**. The *Destination Location* screen displays.
3. Accept the default installation location or click **Browse** to select a new location. Once the installation location has been chosen, click **Next**. The *Start Installation* screen displays.
4. Click **Next**. The installation begins.

The MICC OFFICE Backup Tool requires Microsoft. NET framework v4.0 to be installed. If the .NET Framework is not already installed, a dialog box displays below appears to install the .NET Framework. Install if necessary.

To use the MICC OFFICE Backup Tool, see "Using the MICC OFFICE Backup Tool" on page 119.

UPGRADE AND MIGRATION

In order to upgrade a MICC OFFICE 6.0 or 6.1 installation, the server setup kit requires you to close all running MICC OFFICE applications except for the MICC OFFICE Server (which is stopped automatically). If any MICC OFFICE applications are running once you complete the server setup wizard, an error dialog box displays.

Registry records and product folders created by MICC OFFICE applications may be removed during the Uninstall/Modify or Repair procedure. Critical server settings are deleted during the Uninstall only.

It is mandatory for the date format of the source MiCC Office Server and the new MiCC Office Server to have the same date format. For example, DD.MM.YYYY and MM.DD.YYYY would not work but MM.DD.YYYY and MM.DD.YYYY would.

Note: It may take 30 minutes or more to upgrade your database depending on its size. With very large databases, an upgrade may take 1 to 2 hours or more and appear that the upgrade has failed. Do not reboot the MiCC Office server. Instead, view the DB2 progress bar to see the status of the upgrade.

To upgrade an already-installed MiCC Office 6.0 standalone edition to an updated MiCC Office 6.1 or 6.2 release

1. Stop the MiCC Office Server service and server applications.
2. Download the MiCC Office standalone zip file from Mitel Online (MOL).
3. Run the Server_Setup.exe file.

MICC OFFICE AND WINDOWS COMBINED UPGRADES

It is important to back up user settings files and modified .ini files before upgrading the user's Windows operating system.

1. It is recommended to follow Microsoft's recommend upgrade path when upgrading from one versions of Windows to the next or more current version of Windows.
2. Performing a MiCC Office backup for either the MiCC Office or server prior to upgrading to the next supported Windows version is recommended.
3. Upgrading from 32 bit Windows to 64 bit Windows of any version will require a full install of the newer Windows versions. This is a Microsoft OS requirement. The MiCC Office data for either the client or server will have to be saved and restored for this type of Windows upgrade.

USER SETTINGS FILES

Table 15 provides the user settings files that should be backed up before performing a combined upgrade to Windows 7/Windows 8 and MiCC Office v6.x. Default directory locations are provided below:

- For v6.1+, user-specific settings are located in the following directories:
  - **Windows 8**: `C:\Users\<username>\AppData\Roaming\Mitel\Customer Service Manager\<application name>\Settings`.
- For v5.1 to v6.0+, user-specific settings are located in the following directories:
  - **Windows 7**: `C:\Users\<username>\AppData\Roaming\Mitel\Customer Service Manager\<application name>\Settings`.

- For CSM 5.0 and CCS/Callview 4.11/4.2, user settings files are located in the application installation directory. Default installation directories include:
  - **Mitel CSM 5.0**: `C:\Program Files\Mitel Customer Service Manager`
  - **Inter-Tel CCS 4.11/4.2**: `C:\Program Files\Inter-Tel Contact Center Suite`
  - **Swan CallView 4.11/4.2**: `C:\Program Files\Callview`

Table 15: User Settings Files

APPLICATION	FILE NAME		
	CSM 5.0/5.1/6.x	CCS 4.11/4.2	CALLVIEW 4.11/4.2
CallViewer	Actions.ccd	Actions.ccd	Actions.ccd
	Buttons.ccd	Buttons.ccd	Buttons.ccd
	Features.ccd	Features.ccd	Features.ccd
	Hotkeys.ccd	Hotkeys.ccd	Hotkeys.ccd
	Rules.ccd	Rules.ccd	Rules.ccd
	*.chf	*.chf	*.chf
RealViewer	Realvwr.cvd	Intlrvr.cvd	Wallbrd.cvd
	Realviewer.flt	Intlrvr.flt	Wallbrd.flt
Reporter and Reporter Real-Time	Callcost.cvd	Callcost.cvd	Callcost.cvd
	Reporterrt.cvd	Intlrt.cvd	Cvwizrt.cvd
	Reports.cvd	Reports.cvd	Reports.cvd
	Rtlink.cvd	Rtlink.cvd	Rtlink.cvd
	Wizlink.cvd	Wizlink.cvd	Wizlink.cvd
	Rtalarm.evt	Rtalarm.evt	Rtalarm.evt
	Rtlink.evt	Rtlink.evt	Rtlink.evt
	Netlink.evt	Netlink.evt	Netlink.evt
	Reporterrt.flt	Intlrt.flt	Cvwizrt.flt
	Reporter.flt	Reporter.flt	Reporter.flt
	netlink.ini (autorptruser.ini)	netlink.ini	netlink.ini
	*.xdt	*.xdt	*.xdt
SMTP*	Smtp.ini		
BackupTool*	Setting.xml		

(* only from MiCC-O 6.2 onwards)

To perform a restore operation for an application see: #Backup_and_Restore_Procedures

If you are going from an older version you may need to rename the config files as per Table 15 above

Chapter 7

IMPLEMENTING MEDIA BLENDING

INTRODUCTION

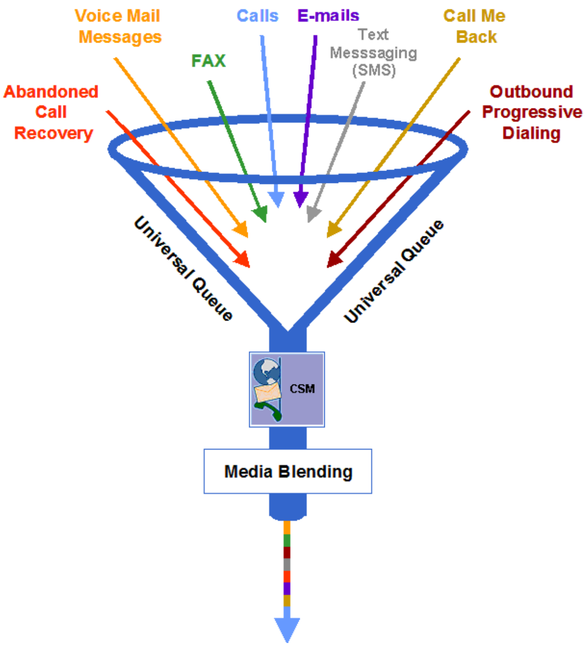
This section explains how to configure MiCC Office to handle different media types, including what third party configuration requirements are necessary. It provides information necessary to create and compile macros for use with MiContact Center Office (MiCC Office).

What is Media Blending?

Media blending enables contact centers to intelligently blend and distribute calls, e-mail messages, and other forms of media to available agents within the contact center by using MiCC Office Server and Intelligent Router. You can configure Intelligent Router so that other forms of media, such as faxes or call backs, can be routed alongside customer e-mail messages and calls.

As more customers turn to the Internet for sales, support, and service, call centers are getting more e-mail messages, faxes, and other forms of contact other than the usual phone call. In turn, call centers must make the migration to become contact centers, being able to deal with a variety of media in a similar way to how calls are handled.

To accomplish this, Intelligent Router provides media blending functionality that allows it to route calls, e-mail messages and other media to available agents, so that customers get the most efficient and effective response available, while still maximizing agent productivity



Examples of media that can be routed, and additional applications that Intelligent Router can provide, include:

- Calls
- E-mail messages
- Faxes

-

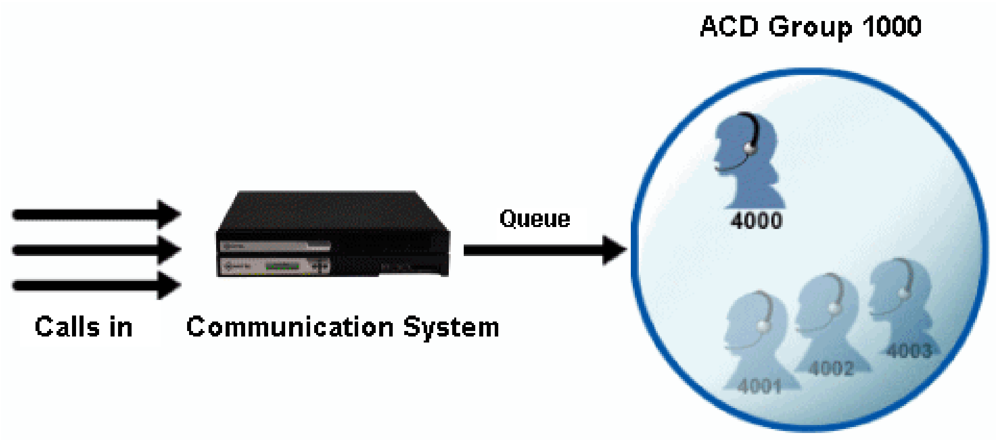
- Voice mail messages
- Mobile text messages (SMS)
- Call back requests from a Web page
- Abandoned call automated call backs
- Progressive dialing

HOW MEDIA BLENDING WORKS

This section explains the concepts behind the media blending functionality provided by MiCC Office Server and Intelligent Router.

WITHOUT MEDIA BLENDING

To fully understand the differences between a site with media blending and a site without, it is necessary to first consider the topological overview of a call center without media blending.



Customers call one or more DID numbers that route their calls to a particular ACD group containing several ACD agents. The telephone system queues these calls in the order that they arrive, and offers the calls to the available ACD agents. If one agent does not answer the call, it is advanced to the next available agent, until an agent answers the call. Agents can log in and out of the ACD group to indicate whether they are available to take calls for it or not. While an agent is busy on a call that arrived via an ACD group, that agent will not be offered any more calls from the same group.

In this environment, the telephone system is configured with a list of DID numbers, ACD groups, and agents. The telephone system engineer configures the telephone system to define where individual DID numbers are routed to, and which ACD groups the calls originating via those DID numbers actually queue at, as well as which ACD agents can log in to which ACD groups.

Without media blending, agents will work on calls all the time. To be able to process other forms of media they have several alternatives:

- Everyone checks a central media store when they have a spare moment, e.g., a common mailbox for e-mail messages, or a central fax machine.

- The group supervisor checks the group mailbox or fax machine, and manually passes the received media to agents, regardless of whether they are able to deal with the item immediately or not.

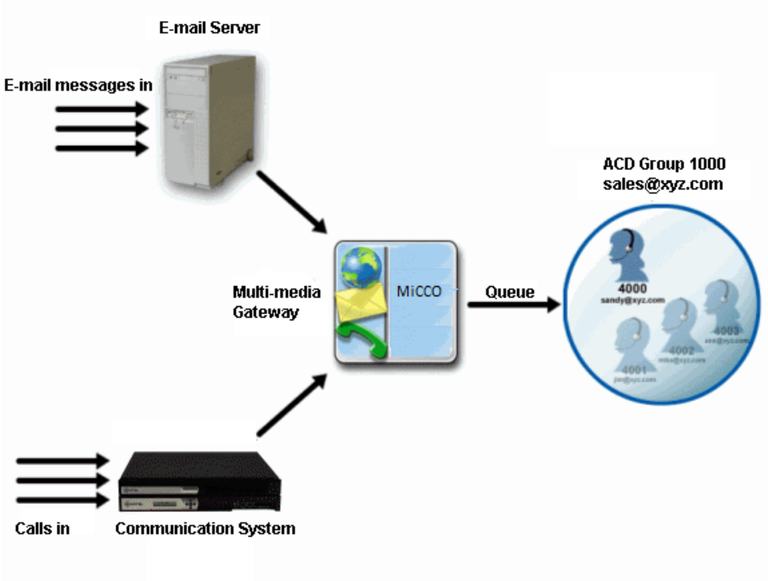
- Given agents only ever deal with queries for certain media types, e.g., some agents only deal with calls, some only with e-mail messages, some with faxes, etc.

None of these options are ideal, since they do not optimize the group's productivity, and can cause customers sending non-call based requests, such as e-mail messages or faxes, to wait a considerable period of time for a response

WITH MEDIA BLENDING

When a call center chooses to implement media blending with MiCC Office and Intelligent Router, the topology changes slightly, enabling them to intelligently blend and distribute a variety of media to available agents on MiCC Office.

Similarly to an environment without media blending, the telephone system engineer configures the telephone system with a list of DID numbers, ACD groups, and ACD agents. Additionally though, the MiCC Office Server is configured with a list of e-mail addresses. It is told which e-mail addresses map to the ACD groups, e.g., ACD group 1000 can receive e-mail messages at sales@xyz.com, and which e-mail addresses map to the ACD agents, e.g., ACD agent 4000 receives e-mail messages in the sandy@xyz.com inbox.



This simple configuration step allows Intelligent Router to know which ACD agents it can route e-mail messages to; if the agent is logged in to ACD group 1000 they can either be offered calls arriving via ACD group 1000, or be routed e-mail messages sent to “sales@xyz.com.”

Once an agent has been routed a call or an e-mail, they will not be routed further calls or e-mail messages for the corresponding ACD group until they have finished their current work.

The MiCC Office Server decides which agent receives the next call or the next e-mail, and ensures that customers wait the least amount of time before being dealt with by an agent. It also means that agents are more productive.

Other forms of media, such as faxes or voice mails, are converted into e-mail messages, such that an agent can expect any media to either be received via their handset, or via their e-mail client. This also means that once the installer has configured the system to route calls and e-mail messages accordingly, then the only work required to support another form of media is to configure the system to convert such media into an e-mail; the existing configuration to route calls and e-mail messages will then take care of the rest.

WHAT IS REQUIRED

The media blending features of Intelligent Router require the following:

- **An Installation of MiCC Office Server**: Server can provide Media Blending only if the Media Blending Module option is purchased (part number 550.6244). Without this option, Server will process only calls. When the Media Blending Module option is included in the license, MiCC Office Server can process calls, e-mail messages and other media.
- **An Installation of Intelligent Router**: The media blending configuration is provided by Intelligent Router, so Intelligent Router (part number 550.6243) must be purchased along with the Media Blending Module option to achieve media blending. Intelligent Router provides call routing as standard.
- **A POP3/SMTP Enabled E-mail Server:** The e-mail messages processed by media blending are retrieved using POP3 and sent via SMTP. These are standard Internet protocols that most e-mail servers support. Your company e-mail server must support POP3 and SMTP to be able to support media blending with Intelligent Router. Examples of e-mail servers that support POP3 / SMTP include Microsoft Exchange Server (with Internet Mail Connector, or the Small Business Server POP3 Connector), Lotus Domino / Notes, and most UNIX mail servers, etc.
- **Secure SSL/TLS connection for Media Blending:** The “Use secure SSL/TLS connection” setting is required for secure Inbox (POP3) and Outbox (SMTP) authorization and e-mail data transfer. Your mail server administrator configures e-mail security settings.
- **An E-mail Client**: Your e-mail server will either use standard POP3 / SMTP e-mail clients, or have a preferred e-mail designed to work with it, e.g., Microsoft Exchange Server can work with any POP3 / SMTP e-mail client, but integrates best with Microsoft Outlook. Each employee that will deal with routed media will need an e-mail configured to connect to your e-mail server.
- **ACD Working on the Communication System**: Media blending requires that you have ACD agents configured and/or licensed on your Mitel communication system. ACD is a purchasable license on the Mitel MiVoice Office 250. Additional MiCC Office ACD Reporting licenses may be required.
- **CallViewer or Connection Assistant**: Some of the scenarios described in this document must have CallViewer or Connection Assistant installed on the agents’ desktops. For those scenarios where it is not specifically mentioned as a requirement, agents may find media

blending much easier to use if it is installed anyway. Certainly the benefits of a CallViewer or Connection Assistant installation will be of great use to a contact or call center agent, regardless of whether media blending is being used or not.

Note: Configuring the system to route e-mail messages is the most involved element of this configuration, and this should be undertaken before attempting to support other media types. For this reason, configuration to handle routing e-mail messages is dealt with first.

ROUTING E-MAIL MESSAGES

This section explains how to configure your e-mail server, the MiCC Office Server, and Intelligent Router to successfully start media blending. This should be used in conjunction with the product help files and manual to correctly configure the media blending rules required by a particular site.

TESTING YOUR E-MAIL SERVER

Regardless of which e-mail server you are using, you should test the server as described in this section to ensure that MiCC Office Server will work successfully with it. The examples given were performed against an Exchange Server, so your own results may be different.

TELNETTING TO NON-STANDARD PORTS

To be able to test your e-mail server you will need to be able to use the “TELNET” application to connect to non-standard ports.

Note: By default, Telnet is not installed on Windows 7 and above or Windows Server 2008 and above. For more information, see the Microsoft Telnet Operations Guide.

- On Windows:
- Click **Start**, and then **Run**. Enter `TELNET.EXE` and press **Enter**. A command prompt window will open.
- For the connections we will be making, we need to turn on local echo. Type **`SET LOCAL_ECHO`** and then press **Enter**. (You can undo this setting by typing **`UNSET LOCAL_ECHO`**).

To make a connection, type **`OPEN [IP Address] [Port]`**

For example, to connect to port 25 on IP address 192.168.254.1 you would type:

```
OPEN 192.168.254.1 25
```

To test your e-mail server for functionality with MiCC Office Server, the following tests need to be performed. You will need to know the IP address or hostname of your e-mail server’s POP3 and SMTP services. Your system administrator should be able to tell you these.

CHECKING FOR AN SMTP SERVER

MiCC Office Server uses SMTP to send e-mail messages. SMTP accepts connections on port 25 by default. To test connectivity to your SMTP service you should TELNET to the IP address or hostname of the computer running the SMTP service, on port 25, as described above.

The following shows an example output of a successful connection to an SMTP server; items in bold indicate what is typed by the user:

```
220 xyzsvr.xyz.com ESMTP Server (Microsoft Exchange Internet Mail Service
5.5.2653.13) ready

QUIT

221 closing connection
```

```
Connection to host lost.
```

CHECKING FOR A POP3 SERVER

MiCC Office Server uses POP3 to receive e-mail messages. POP3 accepts connections on port 110 by default. To test connectivity to your POP3 service you should TELNET to the IP address or hostname of the computer running the POP3 service, on port 110, as described above.

The following shows an example output of a successful connection to a POP3 server; items in bold indicate what is typed by the user:

```
+OK Microsoft Exchange POP3 server version 5.5.2653.23 ready

QUIT

+OK Microsoft Exchange POP3 server version 5.5.2653.23 signing off

Connection to host lost.
```

IF YOU CANNOT CONNECT TO YOUR POP3/SMTP SERVER

If you are having problems performing the tests and the TELNET application fails to connect as documented on “Telnetting to Non-standard Ports” on page 7, there are several possible reasons:

- Can you connect to the computer using the given IP address at all? Try PINGing the IP address to see if the computer is running.
- `PING 192.168.1.1`
- `Pinging 192.168.1.1 with 32 bytes of data:`
- `Reply from 192.168.1.1: bytes=32 time=41ms TTL=240`
- `Reply from 192.168.1.1: bytes=32 time=68ms TTL=240`
- `Reply from 192.168.1.1: bytes=32 time=40ms TTL=240`
- `Reply from 192.168.1.1: bytes=32 time=82ms TTL=240`
- Replies indicate a successful connection to the IP address. If you see “Request timed out” instead of valid replies as indicated above, then you should check that the computer you are trying to connect to is active on the network, or that the computer you are trying to connect from can see other computers on the network. If you are trying to connect using a hostname, try again using an IP address, as you may be experiencing problems with hostname resolution.
- The computer you are trying to connect to may not be an SMTP or POP3 server. If this is the case then the TELNET connection to the given port will fail. You should check with your system administrator to ensure that the computer you are trying to connect to is a valid SMTP or POP3 server. Alternatively, it could be that the computer is a valid SMTP or POP3 server, but that the appropriate service is not running, e.g., if the Internet Mail Service is not running in Exchange Server, then you will not be able to connect to the SMTP server of the Exchange Server.
- The system administrator may have changed the SMTP/POP3 service port number on the server from the default of 25 (SMTP) or 110 (POP3). You may need to change the port for SSL/TLS. Your system administrator should be able to notify you of the required port.

If you are still having problems trying to connect to your POP3/SMTP server, there are two options:

- You do not have a POP3/SMTP-compliant e-mail server, and so cannot use the media blending options in MiCC Office Server.
- Ask your system administrator to read this document and appropriately configure the e-mail server.

CONFIGURING MICC OFFICE SERVER

Having set-up the e-mail server, you are now ready to configure the MiCC Office Server. The configuration of the Server for connection to the telephone system will not be considered, since it is required irrespective of whether media blending is to be used. This section will only consider the configuration elements that will affect media blending.

CONFIGURING ACD GROUPS

The MiCC Office Server needs to know which groups map to which e-mail addresses, e.g., the Sales ACD group 1000 maps to “sales@xyz.com.” This means that customers can contact sales either by ringing a DID number that queues calls at ACD group 1000, or by e-mailing “sales@xyz.com.”

It is not necessary to map an e-mail address to each ACD group; certain ACD groups may not have an associated e-mail address, or some may have so little e-mail traffic that it would not be worthwhile to map them for media blending purposes.

Another point to note is that the Server is licensed by number of queues, and number of agents. A queue license is consumed for each ACD group that is mapped to an e-mail address. If you have purchased only a single queue license, then you can only map one ACD group to an e-mail address.

Mappings are performed in the Hunt Groups view of Data Manager.

1. Select a group from the list and click **Change** to display the following dialog box.
2. To map the ACD group to the e-mail address, type the e-mail address in the E-mail Address field and then click **OK**.

CONFIGURING AGENTS

The Server needs to know the e-mail addresses of agents it can route messages to. You can enter e-mail addresses for each of your agents in the Data Manager, but Intelligent Router will only use the first logged in agents that you have licenses for. For example, if you have five agent licenses, and enter 10 agents with e-mail addresses, the first five agents who are logged in when Intelligent Router starts will be considered licensed and therefore able to receive routed e-mail messages. If one of the agents logs out, the next available logged in agent will be considered licensed.

You should only enter in e-mail addresses against agents that you want to receive routed media, otherwise Intelligent Router may license agents who you do not want to receive the routed media.

1. To enter an e-mail address for each of your agents, open the Agents View of Data Manager.

2. Select an agent from the list and then click **Change**.
3. Enter the agent's e-mail address in the E-mail Address field, and then click **OK**. The agent ID and e-mail address are now mapped together. When the agent logs in to an ACD group, they can be routed non-call based media intended for that ACD group.

CONFIGURING INTELLIGENT ROUTER

Intelligent Router's configuration is composed of two parts. First, it is necessary to configure how Intelligent Router will send and receive e-mail messages, so that it can queue e-mail messages along with calls. Second, Intelligent Router must be told which rules to apply in order to define how different types of media are routed and distributed together.

CONNECTING TO AN E-MAIL SERVER

After Intelligent Router has successfully connected to the MiCC Office Server, the **Media Blending** toolbar button is enabled. This button displays a dialog box which allows you to configure how e-mail is sent and received for each queue, as well as options global to Intelligent Router's Media Blending functionality.

The list shows all ACD groups that have an e-mail address mapped to them. Any other ACD groups configured in MiCC Office Server will not be displayed, as they have no mapped e-mail address.

Intelligent Router will process only the queues that are enabled. When you first launch Intelligent Router all queues are disabled; you will first need to configure a queue before enabling it.

Select a group that you want to enable, and click **Edit…** to display settings for that group.

GENERAL SETTINGS FOR CONNECTIVITY

First, it is necessary to configure some general settings for connectivity, before Intelligent Router is configured to send and receive messages for this queue.

- **Enabling the Queue**: When you first configure a queue, you should enable it by checking the **Enable message processing for this queue** option. Intelligent Router does not process a queue until it is enabled.
- **Administrator Address**: The administrator receives messages that expire because they have queued for too long without being routed or forwarded from the queue. You should always enter an administrator e-mail address for a group, preferably the supervisor of the particular ACD group.
- **Root Folder**: The root folder defines the location where Intelligent Router will store its data while e-mail messages are being queued. This defaults to a subfolder in the Intelligent Router installation folder. You should ensure that the drive where this folder resides has enough space to accommodate the maximum size of e-mail that the queue is likely to receive, taking into account the greatest number of messages that will be handled at any one time.

For example, if a group generally receives quite small messages of about 2 KB, that will queue for around 5 minutes, but take about 2 minutes to respond to, and 500 new messages arrive every hour, then:

```
E-mails Received / Second
= 500 e-mails / 3600 seconds (1 hour)
= 0.14 e-mails / second

Time One E-mail Is In System
= 300 second queue time + 120 second respond time
= 420 seconds

Average E-mails Queued At Any One Time
= Time One E-mail Is In System * E-mails Received / Second
= 420 * 0.14
= ~58

Average Disk Space Used
= Average E-mails Queued * Max. Message Size
= 58 * 2 KB
= 116 KB
```

However if we consider a group that generally gets larger messages with attachments of about 5 MB that queue for around 30 minutes, but take about 2 hours to respond to, with a new message arriving every 30 minutes, then:

```
Emails Received / Minute
= 1 e-mail / 30 minutes
= 0.0333 e-mails / minute

Time One E-mail Is In System
= 30 minute queue time + 120 minute respond time
= 150 minutes

Average E-mails Queued At Any One Time
= Time One E-mail Is In System * E-mails Received / Minute
= 150 * 0.0333
= ~5

Average Disk Space Used
= Average E-mails Queued * Max. Message Size
= 5 * 5 MB
= 25 MB
```

Generally speaking, with hard drives currently available at very large sizes, the amount of space should not be a problem, but you should be wary of storing your e-mail messages on a drive with very little space.

> **Note:** It should be assumed that media size is much greater when routing messages that contain attachments, such as faxes or voice mail messages.

SETTINGS FOR DEALING WITH AGENT RESPONSES

On the Agent Responses tab you can configure what e-mail address and display name the customer will receive messages from. This allows e-mail messages to appear to be from the agent who responded to the message, but customer replies go to the queue's e-mail address for suitable distribution.

- **Display Name:** This setting allows you to select a display name when a customer receives a reply. You can choose either the agent's display name, the queue's display name, or specify your own text. The agent or queue display name is configured in the e-mail or server, depending on your configuration. For example, using Microsoft Outlook with Exchange Server, the display names are configured in Exchange Server, but if using Outlook Express, the display name is configured in the Account settings of Outlook Express.

  > **Note:** On Exchange Server, the server always defaults the display name to that of the queue's mailbox. However, the display name of the address where a reply is sent to will match what is entered for this setting.

- **E-mail Address**: This setting allows you to select an e-mail address that the message will appear to be from when a customer receives a reply. You can choose either the agent's e-mail address, the queue's e-mail address, or specify an alternative e-mail address. You can use this setting to enable customer replies to a routed message to go straight back to the agent, or to an alternative queue that does not send an auto reply.

  > **Note:** On Exchange Server, the server always defaults the e-mail address to that of the queue's mailbox. However, the e-mail address where a reply is sent to will match what is entered for this setting. This setting will usually have an effect when replying to actual e-mail media, as opposed to faxes or other media forms where the e-mail is purely a means to get the media to the agent.

- **Responses**: This setting allows you to choose what happens when an agent manually leaves the Busy (E-mail) state having been routed a message. The default is for the agent to effectively refuse the message, causing it to be routed to another agent as per. the routing rule configuration. However, you can change this setting to leave the agent with the message, but no longer be in Busy (E-mail) or to consider the routed message as not needing a reply. These options allow the agent to manually leave the Busy (E-mail) state without necessarily having to reply to the routed e-mail, or to reply to it later, if the contact center suddenly becomes busy.

SETTINGS FOR TIMER CONFIGURATION

On the Timers tab you can configure how frequently Intelligent Router processes messages, and after what duration a message expires.

- **The Poll Interval**: Intelligent Router will check for new messages every 5 seconds by default. Under most circumstances there is no need to change this value.
- If you have a large number of non-call based media being received every hour, you may want to consider reducing this interval so that you connect more frequently, but this is not strictly necessary.
- Sites may want to increase this interval if they have a WAN based e-mail server, as opposed to a local e-mail server, and pay for their Internet connection charges.

  - **Expiry Time**: Customer media that is not routed after the “expiry time” is considered as expired. This can occur if rules have been configured incorrectly (thus causing no rules to fire against the inbound e-mail), or if no agents are available to process the e-mail, and so the message cannot be routed. By default, expired e-mail messages are routed to the queue administrator.
  - You can choose the expiry time that is suitable for your environment, although the default is for five days to allow for long weekend national holidays where no staff are available. If a site is running 24 hours a day, 365 days a year, this setting could be significantly reduced. Bear in mind, however, that e-mail messages tend not to need to be processed as quickly as calls, and so the expiry timer should normally be at least 4 or 5 hours.

SETTINGS FOR DOWNLOADING E-MAIL MESSAGES

On the Inbox tab you configure the settings for how Intelligent Router will download media for the current queue.

The Incoming Mail (POP3) setting is the IP address or hostname of your e-mail server. Your system administrator should be able to tell you this setting.

The Port and Timeout settings are set to default values, and you would not normally have a reason to change these.

For most POP3 servers, the authentication mechanism will be **Plain text password (USER/PASS)**, and you should enter a username and password that has authorization to download messages for the e-mail address mapped to this queue.

EXCHANGE SERVER USERNAMES

With Microsoft Exchange Server, the username you enter is usually of the form:

```
[Domain] \ [User] \ [Mailbox Alias]
```

For example, if `sandy@xyz.com` logs on to the domain “XYZ” as user “sw” with mailbox alias “sandyw,” then the username would be “XYZ\sw\sandyw.” The mailbox alias can be configured within Exchange Server, but is usually the first name and initial of the surname of the user who has access to the mailbox.

It is also possible to use just the mailbox alias, e.g., “sandyw” from the example above.

SETTINGS FOR SENDING E-MAIL MESSAGES

On the Outbox tab you configure the settings for how Intelligent Router will send messages for the current queue, e.g., when an inbound message needs to be routed to an agent, or an agent’s response sent to the customer.

The Outgoing Mail (SMTP) setting is the IP address or hostname of your e-mail server. Your system administrator should be able to tell you this setting. Generally speaking, your LAN-based e-mail server will have the same IP address for both the Inbound and Outgoing Mail settings.

The Port and Timeout settings are set to default values, and you would not normally have a reason to change these.

Whether your SMTP server requires authentication depends largely on your SMTP server. Most LAN-based SMTP servers do not require authentication by default. However, your system administrator may have changed this, due to the increase of unsolicited e-mail being sent through unprotected SMTP servers. If your server does require you to log in, choose the **Encoded password (AUTH LOGIN)** option, and enter the username and password that has the authorization to send messages for the given mailbox.

RULES AND ACTIONS

After configuring Intelligent Router to process messages that are routed to the available queues, it is necessary to create various rules to route these messages accordingly. This section briefly covers the rules and actions that are available, and outlines the order that media blending rules are processed. The Intelligent Router online help provides further detail on the functionality of the rules and actions mentioned.

- **Rules**: Several rules are available in Intelligent Router to facilitate media blending, such as the following:
  - *Media Routing*: This rule is used to instigate the routing of an inbound message. When a non-call based media object arrives in the queue from a customer, this rule will fire. Typically this rule would then fire the Route Media action, to route the message between available agents. When a message is routed in this way, it is tagged by Intelligent Router, so that when the agent replies to the routed message, Intelligent Router knows how to handle the response. Additionally, this rule will be checked while messages are queuing to ensure that a rule has not become valid while a message has been queuing. This enables you to have different rules for routing messages while outside of office hours, or at busy periods.
  - *Media Received*: This rule is fired the first time that a non-call based media object is received in the queue, including messages from customers and from internal agents. This rule is mainly used for sending automatic responses, or to stop messages from being sent that contain inappropriate responses. The main difference between this rule and the Media Routing rule is that the Media Routing rule fires only for external

customers, because it is principally such messages that would need routing.

- *Expired Media***.** Each queue configured in Intelligent Router has an expiry time that defines how long a message queues before it is assumed that no rule will fire against the message. This can occur because conditions against the available rules preclude this message from being processed, or because no agents have been available for this message to be routed. By default, any message that expires is automatically forwarded to the queue administrator. However, this rule allows you to override such functionality.

- **Actions**: Intelligent Router provides several actions to handle media blending, as follows:
  - *Route Media***:** This action distributes a received message to an available agent. The agent is chosen based on one of several distribution criteria, such as number of contacts handled, time spent idle, least amount of time spent busy, etc. (described below). If no agent is available to be routed the message, the message is postponed for a short time, and the agents checked for availability later.

    - When an agent is successfully routed a message they enter the Busy (E-mail) state. While in this state they will not be routed telephone calls or other e-mail messages via the ACD group. The agent will, however, be able to make outbound calls to assist them in processing the e-mail. When the agent replies to the message, they are taken out of the “Busy (E-mail)” state so that subsequent e-mail messages or calls can be processed. After the agent replies, and the response is sent to the customer, both the original inbound message from the customer and the agent’s response are removed from the queue.
    - The “Route Media” action provides the following distribution mechanisms:
      - Cyclic (Linear): This mechanism routes non-call based media objects to the agents in the order that they have been entered in the action. It always starts routing from the first agent in the list.
      - Cyclic (Distributed): This mechanism routes non-call based media objects to the agents in the order that they have been entered in the action, starting from the next agent after the last agent to be routed a media object by this action. For example, when routing between agents 4000, 4001, and 4002, the first message is routed to agent 4000, the second message to 4001, the third to 4002, and so on. If agent 4000 is busy when the fourth message arrives, it is routed to agent 4001 instead.

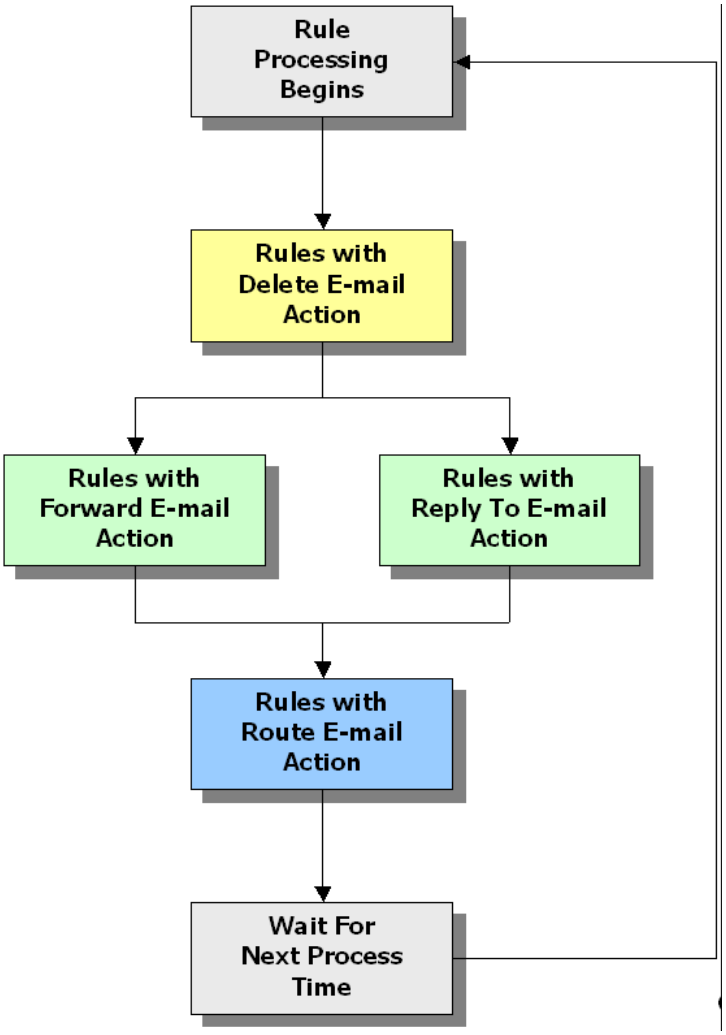
  - – Balanced (Contacts Handled): This mechanism routes non-call based media objects to the agent with the lowest number of contacts (e-mail messages and calls) handled so far today. If that agent is busy, then the next agent with the lowest number of contacts handled today is routed the media object, and so on.
  - – Balanced (E-mails Handled): This mechanism routes non-call based media objects to the agent with the lowest number of e-mail messages handled so far today. If that agent is busy, the next agent with the lowest number of e-mail messages handled today is routed the e-mail, and so on.
  - – Balanced (Longest Idle): This mechanism routes non-call based media objects to the agent with the longest time spent since they last ended a call, or entered the Free or Free (E-mail) agent states. If that agent is busy, the next agent with the longest idle time is routed the media object, and so on.
  - – Balanced (Longest ACD Free): This mechanism routes non-call based media objects to the agent with the longest time spent in the Free and Free (E-mail) agent states so far today. If that agent is busy, the next agent with the longest free time is routed the media object, and so on.
  - – Balanced (Least ACD Busy): This mechanism routes non-call based media objects to the agent with the least time spent in the Busy (Call) and Busy (E-mail) agent states so far today. If that agent is busy, the next agent with the least busy time is routed the media object, and so on.
  - – Random: This mechanism routes non-call based media objects to agents at random.

- o *Forward E-mail:* This action forwards a copy of the e-mail to another e-mail address. It can also be used to optionally delete the message after it is forwarded, to ensure that no further rules process the message. This action is useful for having an archive of received messages, or to send inappropriate messages to the administrator for processing.
- o *Reply To E-mail:* This action replies to the received e-mail, sending the response to the message originator. It can also be used to optionally delete the message after it is forwarded to ensure that no further rules process the message. This action can be used to send message receipt confirmation to received e-mail messages, e.g., “Thank you for your e-mail. It will be processed shortly,” or even to send complete automated responses based on keywords in the original message. This action is more suited to handling actual e-mail media objects, rather than other forms of media that have been converted to an e-mail to facilitate routing, such as faxes or voice mail messages.
- o *Delete E-mail:* This action deletes the received message, causing it to not be processed by any another rules. For example, if unsolicited e-mail messages were persistently being received from users in the “spam.com” domain, this action could be used to automatically delete such messages, reducing the number of inappropriate e-mail messages that agents had to process.

RULE PROCESSING ORDER

Most Intelligent Router rules are processed in the order in which they are created. However, this is not feasible with media blending rules, because a rule that will delete a media object should be fired before a routing rule, otherwise one rule would attempt to route the message, and then the next rule would delete the routed media!

Rules are therefore processed in the following hierarchy:


Rule Processing Begins
Rules with Delete E-mail Action
Rules with Forward E-mail Action
Rules with Reply To E-mail Action
Rules with Route E-mail Action
Wait For Next Process Time

Rules with Delete E-mail actions are always fired first to ensure that no other rules get chance to process the media object, should it be deleted. Both Reply and Forward actions are then processed, because both of these actions can delete a media object, and so, again, it is important that we delete an item before it is processed by subsequent, lower level actions. Finally, Route E-mail actions have a chance to process rules, before the message is postponed where it will be checked against all rules again in a short while.

If you have several rules of the same action type, they are processed in the order in which they are created. You can change the order in which rules are processed using the Rule Manager dialog box. This dialog box allows you to move rules up and down in the rule list, thus altering the order in which they are processed.

Media Received type rules fire only once and before Media Route type rules regardless of the order they appear in the Rule Manager dialog box.

Typical Media Received actions are to trap or forward out of the queue any messages not appropriate for the agents i.e., Spam, Calendar Invitations, Out of Office Advisories. It is important for this step to occur before an auto-response steps to avoid an endless loop of auto-responses.

A separate rule must be configured to trap each “type” (i.e., Spam, Calendar Invitation, Out of Office, etc.). The most common method for trapping is to search for keywords in the subject of the e-mail message.

The order in which rules should be processed depends on the conditions that are applied to the rule. The rule with the most restrictive set of conditions should be placed higher than rules with the least restrictive conditions, or with no conditions at all.

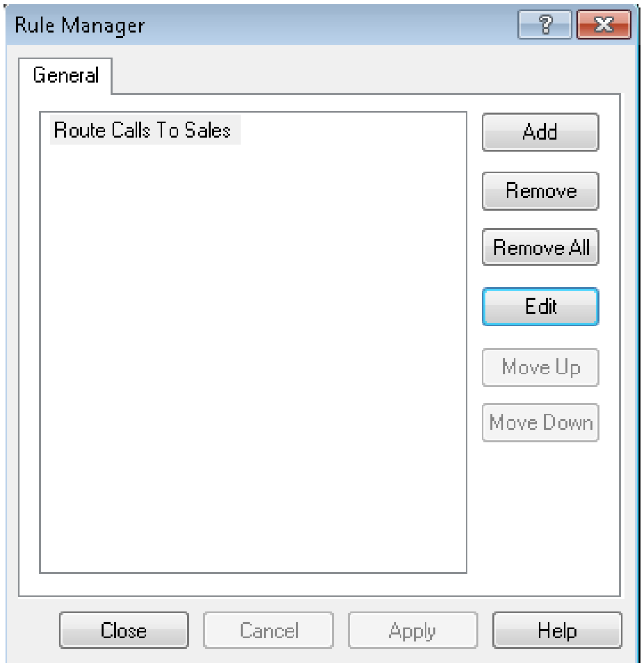
For example, let's consider a system where we want to route e-mail messages between agents 4000 and 4003 with three different scenarios:

- E-mail messages from `sam@abc.com` should be routed to agent 4000.
- E-mail messages with the words "PRODUCT" or "SOFTWARE" should be routed to agents 4000 to 4005.
- All e-mail messages should be routed to agents 4000 to 4015.

The first scenario will apply only to a small number of e-mail messages, and so should be the first routing rule to be processed. The second scenario could apply to any e-mail originator, but only with certain keywords, so will apply to a greater number of e-mail messages, and so should be the second routing rule to be processed. The last scenario, which deals with all e-mail messages, should be the last routing rule to be processed.

In this example, consider an e-mail sent from `sam@abc.com` containing a subject of "Tell me about your product." Both rules 1 and 2 could fire against this e-mail, because the message is from `sam@abc.com`, but the subject also contains the word "PRODUCT." However, because rule 1 is the first in the list, it is this rule that will fire against the message, and so the message will be routed to agent 4000 when they are available.

In this example, the **Route E-mails After Delay When Busy** rule is the first rule to be processed. It is necessary to move other e-mail routing rules that use conditions to be processed first, so that the conditions can take effect.


Rule Manager

Route Calls To Sales

For example, the **Route E-mails After Delay When Busy** rule is configured to make e-mail messages queue for longer when the number of calls waiting is high (so that calls are given a higher priority than e-mail messages). This rule should therefore be processed before the **Route E-mails** rule. The **Auto Reply** rule can be placed anywhere in the list because the rule processing order will force a **Reply Media** rule to be processed sooner.

By using the **Move Up** and **Move Down** buttons, we can alter the order that rules are processed. Rules near the top of the list are processed before rules near the bottom of the list.

ROUTING E-MAIL MESSAGES EXAMPLE

This section shows how to create a very basic rule that will route incoming e-mail messages to available agents. This is the most basic configuration of media blending, where Intelligent Router is taking into account the agent state when deciding where to route an e-mail, but no other factors affect the routing decision. This rule and action will either be re-used for all other types of media routing, or will be the basis of the rules and actions for other types of media routing.

CREATE THE RULE TYPE

Right-click the “Rule List,” and choose Add Rule from the menu to create a new rule. For media blending, where you need to manage e-mail -based media between agents, choose the Media Routing rule type, followed by a queue for which you want to route media.

For example, if ACD group 1000 receives messages at mailbox `sales@xyz.com`, we would choose queue 1000 to route the messages in `sales@xyz.com`.

Because this is basic media blending, we will choose to always route messages, regardless of the number of calls queuing at the ACD group or the current service level

DEFINE THE ACTION

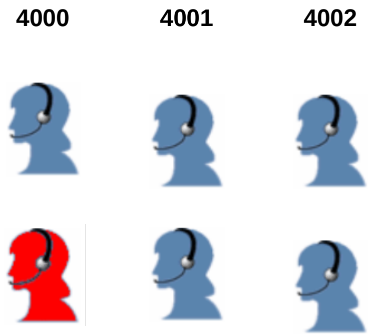
After defining when the rule will fire, we must now tell Intelligent Router what to do with the messages received by customers. On the Action tab, the **Route Media** action will have already been selected for you.

Enter a comma-separated list of agents to whom you want to route messages. This can be all the media blending agents in your contact center if you want, since Intelligent Router will only route messages to agents based on certain criteria; for an agent to be routed a message for this queue, the agent must be:

- Logged in.
- Not in the Busy N/A or Wrapup (Call/E-mail) agent states.
- Not in Do-Not-Disturb state (DND).
- If you choose the **Calls take priority over e-mails** option, the agent must be in the Free or Free (E-mail) agent states, without a call alerting or being offered at their extension. When the **Calls take priority over e-mails** option is chosen, agents are not considered as being available for e-mail processing when they are being offered a call.
- If you choose the **E-mails take priority over calls** option, then the agent must be in the Free or Free (E-mail) agent states although calls may alert or be offered to that agent at the same time. When the **E-mails take priority over calls** option is chosen, agents are always considered as being available for e-mail processing if they are also being offered a call.
- If the agent is busy on a call or e-mail, they will not be routed a message.

Next, you should choose the type of distribution that you want to perform on messages. This defines how messages are allocated to available agents. At the simplest level, the **Cyclic (Distributed** option routes available messages to each agent in turn, in the order that they are entered. When the next message needs to be routed, it is offered to the next agent.

For example, if we are routing messages among agents 4000, 4001, and 4002:



Initially, all agents are free.

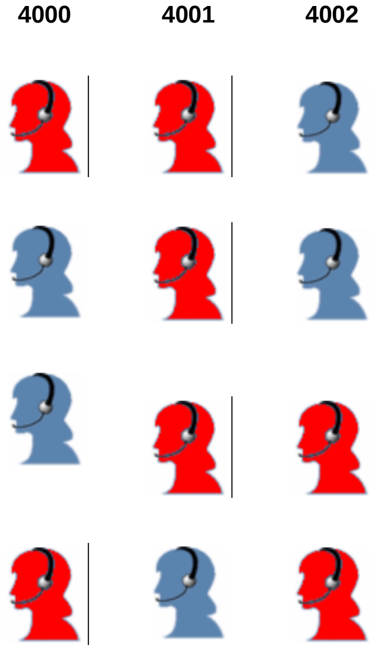
A message arrives at the queue, and is routed to agent 4000.

A call alerts the queue, and is answered by agent 4001.

Agent 4000 completes the message routed to them.

A second message arrives, and because agent 4001 is busy, the next agent that can receive the message is agent 4002.

Agent 4001 completes the call, and when the third message arrives, the next agent to route it to is agent 4000 again.

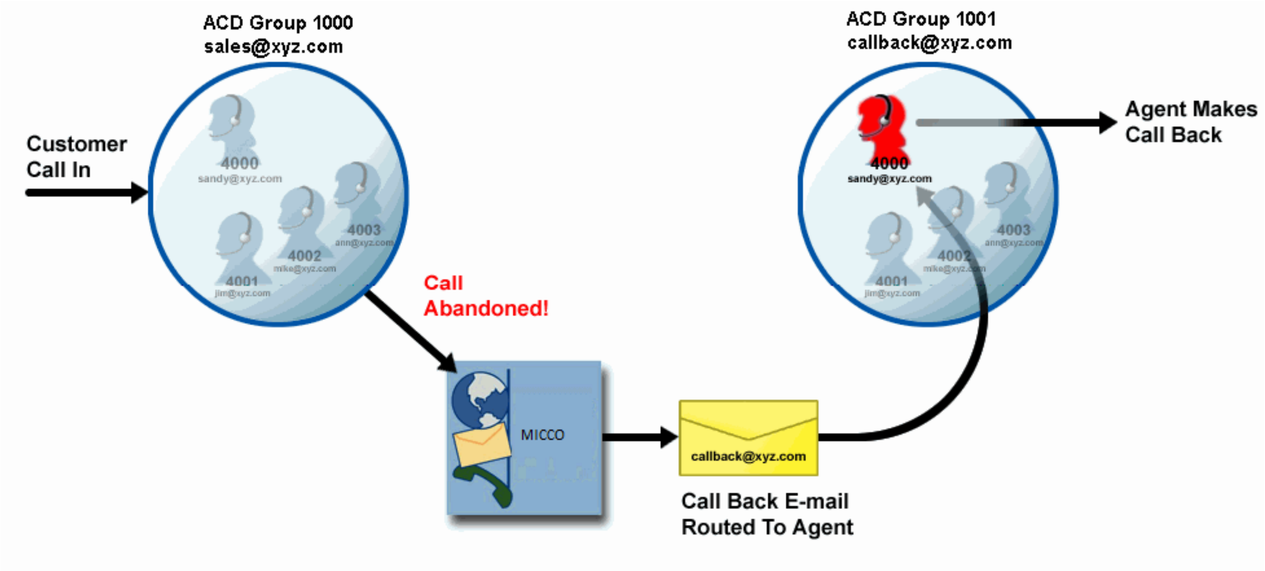


Click **OK** on the rule dialog, and the simplest media routing rule has been created. Calls to ACD group 1000 will be offered to agents logged in to ACD group 1000 using the telephone system programming logic, while other media sent to `sales@xyz.com` will be offered to the agents listed in the rule’s action who are logged in. You could configure a call routing rule using the **Call Routing** rule to override the telephone system programming logic for routing calls.

ROUTING ABANDONED CALLS

There can be occasions when the contact center is busy, and agents are not available to take calls. A busy customer can get frustrated, and choose to abandon the call, in search of a competitor. In such a scenario the ability to return the customer's call as quickly as possible is imperative. This can be achieved using media blending, and if a basic media blending rule has been configured as shown in the previous section, it is a very simple process to configure.

The principle behind this type of application is that Intelligent Router has a rule that creates a new e-mail when a call is abandoned. This e-mail contains the telephone number of the abandoned caller, and it is sent to a media blending queue's e-mail address. A media blending routing rule is then used to route the e-mail to an agent when one is available, and the agent's CallViewer or Connection Assistant interprets the e-mail to make the return call.



Note: Although the example diagram shows the call back ACD group as being a different group (1001), it could easily be the same ACD group (1000), so that the call back request is blended with existing media that is still queuing.

REQUIREMENTS

To achieve this solution, the following items are needed, in addition to the items outlined in "How Media Blending Works" on page 143:

- **Microsoft Outlook or MAPI-compliant e-mail application**: The MAPI compliant e-mail application will be installed on the same computer as Intelligent Router, and configured to use a spare mailbox to send e-mail messages to the media blending queue, i.e., the ACD group that agents log in to when they want to process blended e-mail messages.
- **CallViewer or Connection Assistant**: Any agent who wants to make automatic call backs to abandoned callers needs to have either CallViewer or Connection Assistant installed on their computer. They also need to be licensed accordingly, i.e., if the site only has five Connection Assistant licenses, but eight agents need the ability to make

automatic call backs, then an additional three Connection Assistant licenses (or three CallViewer licenses) will be required.

- **AutoDial Ready To Go**: Each CallViewer or Connection Assistant application needs an instance of the AutoDial Ready To Go to be configured. This Ready To Go is included as standard when CallViewer or Connection Assistant is installed, but an instance of the Ready To Go will need to be configured accordingly.
- **Call Back E-mail Address (optional)**: If you want to use a separate queue for call back requests, you need another e-mail address for such requests. This can be an alias of an existing mailbox which is already a media blending queue. By making the address a separate mailbox, it can be assigned to a separate media blending queue, allowing for a different group of agents to perform call backs. For simplicity, it is easier to have call back requests routed to the main media blending queue.

CONFIGURING MICROSOFT OUTLOOK

Note: Outlook is not required if using the Send Email (Via SMTP) option. **Consider using this option instead of Send Email (via MAPI)**

Microsoft Outlook, or a MAPI-compliant e-mail application, needs to be installed and configured on the Intelligent Router computer. It is beyond the scope of this document to explain how to configure such an application. However, one important thing that will greatly simplify the installation, is that the mailbox that Outlook is configured to use should be the default mailbox for the user that is logged in to the computer that is running Intelligent Router. Usually Intelligent Router should be running using its own user account on the system (e.g., a “router” account, rather than another user’s actual account), in which case, just ensure that the given user account has a mailbox associated with it.

CONFIGURING INTELLIGENT ROUTER

To process call backs for abandoned calls via Intelligent Router, you need a basic media routing rule as described in “Routing E-mail Messages Example” on page 159, as well as a new rule that fires when a call is abandoned. It will be assumed that the routing rule described in “Routing E-mail Messages Example” on page 159 has already been created.

CREATE THE ABANDONED CALL RULE

To create a new rule, right-click the Rule List tile, and choose **Add Rule** from the menu. Choose the **Call Abandoned** rule type, which fires when a call is abandoned, and then enter the ACD group(s) that you want to monitor for abandoned calls in the **Extension(s) / Group(s) Alerted** field.

For example, if sales calls alert at ACD group 1000, and you want to place call backs to abandoned sales callers, `1000` would be entered in this field.

There are no other parameters to configure for this rule type.

CONFIGURE THE SEND E-MAIL VIA MAPI ACTION

After defining when the rule will fire, we must now tell Intelligent Router what to do when the rule does fire. On the Action tab, the **Send E-mail (Via MAPI)** action will have already been selected for you.

Note: The same result can be achieved using the Send E-mail (Via SMTP) action

In the **To** field, type the e-mail address of a media blending queue to which you want to route the call back requests. For example, if you have a media blending queue 1000 that routes email messages for `sales@xyz.com`, you would enter **`sales@xyz.com`** as the “To” address for this rule. This will cause the action to send an e-mail message to the media blending queue that will then be routed to an available agent using a standard media blending routing rule.

For this type of action to work correctly, the Caller ID needs to be included in the subject line of the e-mail that is sent so that the AutoDial Ready To Go knows the number to dial. So that AutoDial can detect where the Caller ID appears in the subject, it should be prefixed with “--> CALLBACK” followed by the **Caller ID / Dialed Digits** placeholder, which you can select from the **Call / E-mail Details** menu that is accessed by clicking the placeholder button (**[...]**) next to the Subject field.

You can also specify a message body for the e-mail. This could contain something useful to the agent who will receive the e-mail when it is routed to them. It is not necessary to enter a message for the rule to work correctly.

DEFINE THE CONDITIONS

The rule that has been defined so far can fire whenever an inbound call is abandoned. However, if a call is received without Caller ID, there is no need for a call back attempt to be made because there is no known number to call back. This can be avoided using the Conditions tab of the rule.

From the Conditions tab, choose **Caller ID Received?** from the Call / E-mail Details submenu of the condition menu. In the drop-down box that appears, ensure that **Yes** is selected, and then click **Add**.

The rule is now configured such that it will be evaluated only for calls that have been received with Caller ID.

CREATE A MEDIA BLENDING RULE

A media blending rule is also required to route the e-mail generated in Step 2. The creation of such a rule is described on “Routing E-mail Messages Example” on page 159. Ensure that the queue that the blending rule is monitoring is assigned to the e-mail address to which the **Send E-mail (Via MAPI)/ Send E-mail (Via SMTP)** action is sending the e-mail.

CONFIGURE OPTIONAL SETTINGS

Because this application routes a “call back” e-mail to an agent, the agent is placed in the Busy (E-mail) state when they receive the call back e-mail, and will need to manually change state after the call back is made. This can be made simple for the agent using the Agent Responses tab for the given media blending queue.

By default, if an agent manually leaves the Busy (E-mail) agent state, Intelligent Router assumes that they are refusing the e-mail. However, each queue can be configured with its own setting, such that if an agent manually left the Busy (E-mail) agent state, the e-mail can be considered as being ARMed, NRNed, or left with the agent even though they are still free.

If you are using a single media blending queue for both call backs and also other media routing, you will need to leave the Agent Responses option as something sensible, based on the types of media that the queue will be routing. However, if you have a separate queue/e-mail address for call backs, the most sensible option for the Agent Responses setting would be **Treat message as being ARM’ed**. This means that when an agent has finished a call back, they put themselves into the Free state, and the call back e-mail will automatically be ARM’ed.

CONFIGURING CALLVIEWER

With the configuration created so far, agents would be routed call back e-mail messages, but they would need to dial the telephone number manually. To overcome this, each agent handling call backs should have the AutoDial Ready To Go solution installed on their installation of CallViewer or Connection Assistant, as follows.

To install the AutoDial Ready To Go solution:

1. From the Install A Ready To Go Solution page in the Setup Wizard, select **AutoDial**, and then click **Next**.

2. Complete the settings that affect how the AutoDial Ready To Go will work:
   - **E-mail Subject Prefix**: This is the text that precedes the telephone number in the subject line of routed call back e-mail messages. In the scenario previously described, this was `--> CALLBACK`. You can use any text, but it should be something that would not be expected in a typical user's e-mail subject.
   - **Display message to user...?**: This option causes the AutoDial action to display a message warning the user that they are processing a call back. Typically, it is a good idea to enable this setting.
   - **Make the call when message is closed:** This option controls when the message is closed while the agent handles the call back. If the option is off, the call back will be placed before a warning message is displayed. Enable or disable this option based on your preference.
   - **Close message automatically after...:** Setting this option causes the warning message to be automatically closed after a number of seconds. If the **Make call when message is closed** option is enabled, the call back will be placed when the warning message is either closed by the user, or automatically closed by the timer.
3. Click **Next**.
4. Click **Finish**.

This will create a new rule called **Handle AutoDial E-mails** that checks routed e-mails for specific text in the subject line. If the text is found, the rule searches the subject line for a telephone number, and then dials the telephone number.

Using the settings displayed in the previous example screen, the call back would be placed as soon as the e-mail arrived, although the user would see an explanatory message indicating that the call back was being placed, which would disappear after 10 seconds.

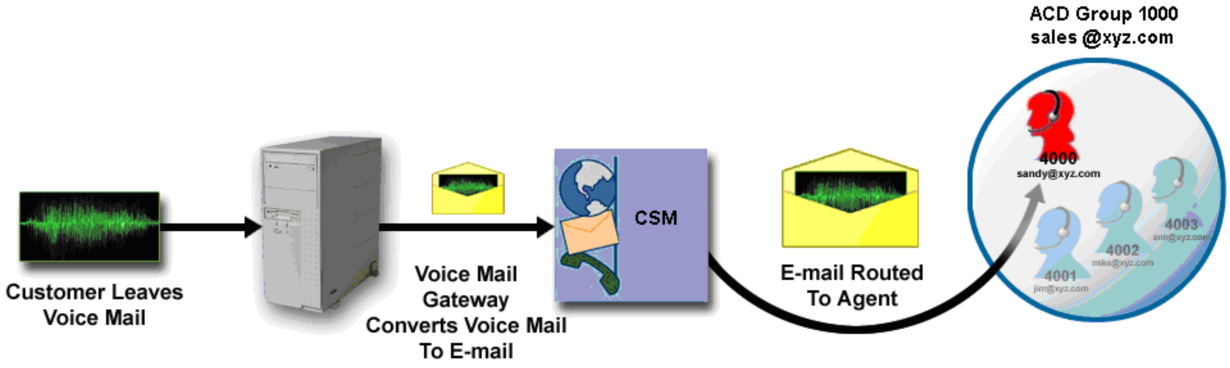
The **Agent Responses** setting in Intelligent Router affect what the agent needs to do when they have completed the call back:

- If the Agent Responses setting is set to **Refuse message and route to different agent** or **Leave message with agent**, the agent will need to manually NRN or ARM the routed call back message, possibly using the Outlook Integration buttons.

- If the Agent Responses setting is set to **Treat message as being NRNed** or **Treat message as being ARMed**, the agent could manually NRN or ARM the routed call back message. However, it is easier if they just return themselves to the Free state, either via their handset, or using an appropriate button on CallViewer or Connection Assistant.

ROUTING VOICE MAIL MESSAGES

If you are using a system that can present voice mail messages as e-mail messages in your e-mail client, you can use this system to enable voice mails left at a group's voice mailbox to be routed to agents for processing, as illustrated below.



When using such a system, you would configure the voice mail software so that it can relate a voice mailbox to an e-mail address, such that when a voice mail is left, it can be stored in the user's e-mail mailbox as well. By configuring the ACD group's voice mailbox to similarly pass the voice mail to an e-mail address, the voice mail can subsequently be routed to an agent, if the e-mail address used is that of a media blending queue.

REQUIREMENTS

To achieve this solution, the voice mail system can typically be configured to pass voice mail messages to the e-mail system as e-mail messages with audio file attachments. This functionality is provided by a voice mail to e-mail gateway, commonly referred to as unified messaging. The voice mail gateway will need to be able to provide the e-mail message in such a form that it can be downloaded via POP3 without requiring proprietary software to be installed on the machines to play the voice mail audio file attached to the e-mail.

For additional requirements, see "How Media Blending Works" on page 143.

CONFIGURING THE VOICE MAIL GATEWAY

How you configure the Voice Mail Gateway will depend on the Voice Mail Gateway being used. This section explains how to configure the voice mail gateway for the Mitel MiVoice Office 250 so that a given voice mailbox forwards voice mails to a particular media blending queue.

To configure the voice mail gateway on the Mitel MiVoice Office 250 CP:

1. Open Mitel DB Programming and connect to the telephone system.
2. Select System – **E-mail Gateway**.
3. Configure the following settings:
   - Configure the **E-mail System** to **SMTP/POP3.**
   - Configure the **E-mail SMTP Server** and **E-mail POP Server** to the IP address or host name of your e-mail server. (This will probably be the same as the SMTP/POP3

addresses that Intelligent Router have been configured with for media blending).

- Configure the **E-mail Username** and **Gateway Password** with the user name and password for a mailbox that the Voice Mail Gateway will send e-mail as.
- The remaining settings should be self-explanatory.

4. Configure ACD group mailboxes to associate them with the e-mail address of the media blending queue:
   - Select Voice Processor – Devices – Mailboxes –<***ACD Group Mailbox***>.
   - Select one of the following for the **Unified Messaging Level** option:
     - **Forward & Copy** Forwards the voice mail to the given e-mail address, leaving a copy in the voice mail box.
     - **Forward Only**: Forwards the voice mail to the given e-mail address, *removing* it from the voice mail box.
   - Specify the e-mail address for the **E-mail Address for Voice Messages** option. For example, if ACD sales group 1000 has a related e-mail address for media blending of "**sales@xyz.com**," type `sales@xyz.com` for the **E-mail Address for Voice Messages** setting for mailbox 1000.
5. Repeat step 4 for all ACD groups where you want to route voice mails to available agents.

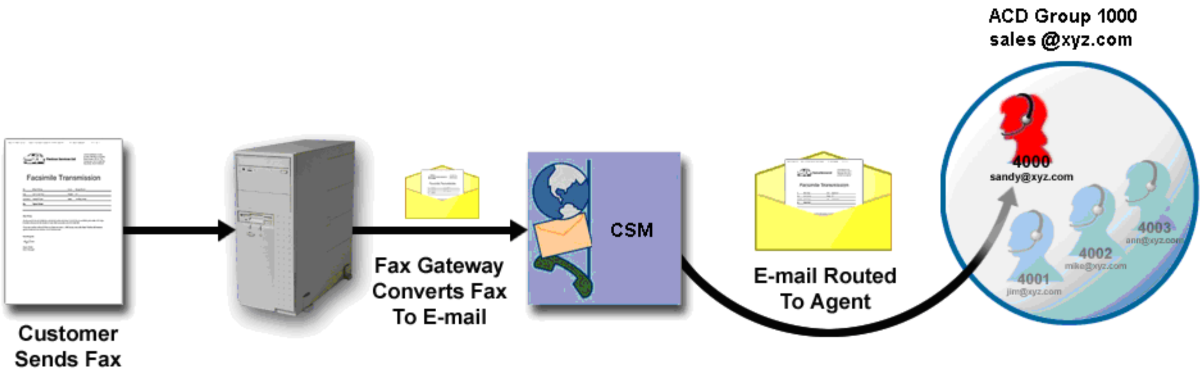
For further information on configuring the telephone system for this functionality, please consult the *Mitel DB Programming Help File*.

CONFIGURING INTELLIGENT ROUTER

A standard media routing rule, as defined in "Routing E-mail Messages Example" on page 159, is all that is required for this scenario to work.

ROUTING FAXES

Media Blending can be used to route faxes to available agents when used with a fax to e-mail gateway. The basic principle is that the fax to e-mail gateway converts faxes received at a specific fax number into an e-mail which is sent to the media blending queue. Intelligent Router then routes the e-mail to an available agent, whereby the agent can review the fax contained within, and act accordingly.



REQUIREMENTS

To achieve this solution, in addition to the items outlined in “How Media Blending Works” on page 143, a fax to e-mail gateway is needed. The fax to e-mail gateway is server-side software that uses a fax card or modem to send and receive faxes. Received faxes are converted into e-mails and subsequently arrive in a given mailbox. This can allow individual users to have their own fax number without the need for an associated fax machine. Such software often allows users to send faxes from common applications such as their e-mail or Microsoft Office application.

A list of some fax to e-mail gateway applications is available at http://www.msexchange.org/software/Fax-Connectors/.

CONFIGURING THE FAX GATEWAY

Configuration of the fax gateway is dependent on the fax gateway software that is being used, and as such is beyond the scope of this document. However, as an example, the steps below show how to configure GFI FAXmaker to route faxes for a given DID number to a media blending queue. GFI FAXmaker is available from the GFI Web site (http://www.gfi.com). This section will assume that the software has been installed on a Windows 2000 Server or later, using Microsoft Exchange Server 2013 or later.

CREATE A LICENSED USER

Run the GFI FAXmaker Configuration Wizard, and click the **Licensed Users** option on the left pane. The right pane will then display a list of users from the Windows Active Directory that are licensed to use the fax capabilities.

Click **New licensed user / group** and then select the group that owns the mailbox that is mapped to the media blending queue. For example, if `sales@xyz.com` is to be routed faxes and has been configured as a media blending queue, you would select the Active Directory Group or User that owns the mailbox with the e-mail address `sales@xyz.com`.

The user or group will then appear in the list of licensed users on the right side of the window.

CONFIGURE A DID NUMBER FOR ROUTING

Next, you need to configure the software for the DID number that faxes are received on, so that received faxes can be passed to the appropriate e-mail address.

On the left side of the window, select **DTMF/DID** under the Routing option. The right side of the window will display a list of configured DID numbers. If you have not configured any DID numbers in GFI FAXmaker yet, click **New...** to add a DID number, otherwise double-click an existing DID entry in the list.

After adding a DID number or editing an existing entry, the properties for that DID number will appear. If no user is configured to receive the faxes for this DID number, the list of users on the Users tab will be empty.

Click **Add** and choose a licensed user that should receive such faxes via e-mail, and then click **OK**.

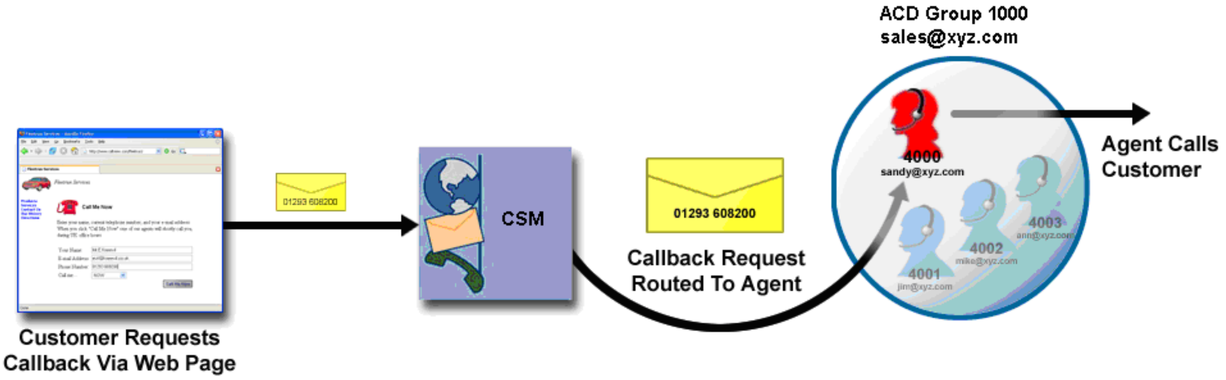
> You do not necessarily need to route faxes by DID number. You can route them via trunk line, e.g., if using analog lines, or one of several other ways, depending on the software that you are using. If you are using a BRI Fax card, and connecting it to the PBX, ensure that the PBX supports S0 Bus / BRI extensions. The Mitel MiVoice Office 250 does not support S0 Bus / BRI extensions.

CONFIGURING INTELLIGENT ROUTER

A standard media routing rule, as defined in “Routing E-mail Messages Example” on page 159 is all that is required for this scenario to work.

ROUTING WEB-BASED CALL BACKS

Media Blending can also be used to route Web-based call requests to an available agent. The basic principle is that the customer fills out a form on the company Web site. This generates an e-mail containing the customer contact details, which is sent to a media blending queue. Intelligent Router then routes the e-mail to an available agent, and the AutoDial Ready To Go in CallViewer or Connection Assistant automatically places the call.



REQUIREMENTS

To achieve this solution, the following items are needed, in addition to the items outlined in section “How Media Blending Works” on page 143:

- **Company Web Site**: You will need access to a Web site to which you can upload new files. The Web server must have the ability to send e-mail messages, using software such as Microsoft Internet Information Server on Windows 2000 and later. The folder that contains the files must have execute permissions.
- **CallViewer or Connection Assistant**: Any agent who wants to respond to Web-based call backs needs to have either CallViewer or Connection Assistant installed on their computer. They also need to be licensed accordingly, i.e., if the site only has five Connection Assistant licenses, but eight agents need the ability to make automatic call backs, an additional three Connection Assistant licenses (or three CallViewer licenses) will be required.
- **AutoDial Ready To Go**: Each CallViewer or Connection Assistant application needs an instance of the AutoDial Ready To Go to be configured. This Ready To Go is included as standard when CallViewer or Connection Assistant is installed, but an instance of the Ready To Go needs to be configured accordingly.

CONFIGURING THE WEB SITE

The Web site should need no special configuration, although it must be able to programmatically send e-mail messages. Such a consideration is beyond the scope of this document for all Web servers. Microsoft Internet Information Server has the ability to send e-mail messages from a default installation. Sample Web pages for IIS are available in subsequent sections.

The basic principle is that the customer completes information on a form on the Web site and submits it, which generates an e-mail that is sent to a media blending queue. The important point to note is that the customer-provided telephone number must be available in the subject of the sent e-mail with some specific text, e.g., “**--> CALLBACK**” followed by the phone number. The text that is used in the message subject must also be configured in the AutoDial Ready To Go that is installed with CallViewer and Connection Assistant.

SAMPLE WEB PAGES

Two Web pages are required on the Web server. The first asks the user for the information, and the second sends the necessary e-mail to the media blending queue.

CALLME.HTML

This is the main file that creates the form the user would navigate to before placing a call request. The example below is deliberately very plain; there are no logos or other visual elements that might normally be used on a live Web page.

```
<!DOCTYPE HTML PUBLIC “-//W3C//DTD HTML 3.2 Final//EN”>

<html>

<head>

<title>Web Based Call back Sample</title>

</head>

<body>

<p>

Enter your name, current telephone number, and your e-mail address. When
you click &quot;Call Me&quot; one of our agents will call you shortly,
during normal office hours.

</p>

<p>

<form id=EmailForm method=POST action=”callme2.asp”>

<table border=0>

<tr><td width=100>Your Name:</td><td><input type=”TEXT”
name=”MyName” size=”48” maxlength=”64”></td></tr>

<tr><td width=100>E-mail Address:</td><td><input type=”TEXT”
name=”MyEmail” size=”48” maxlength=”64”></td></tr>

<tr><td width=100>Phone Number:</td><td><input type=”TEXT”
name=”MyPhone” size=”48” maxlength=”64”></td></tr>

<tr><td colspan=2 align=right><input type=”SUBMIT” value=”Call
Me”></td></tr>

</table>

</form>
```

```
</td>

</tr>

</table>

</BODY>

</HTML>
```

CALLME2.ASP

This file processes the form data provided by the previous page and generates the e-mail, before displaying a confirmation to the user. This file uses Active Server Pages (ASP) to interpret the form data, and generate the e-mail.

Note that the line that reads `objMail.To=’callback@xyz.com’` needs to be updated to use the appropriate e-mail address for the media blending queue that will route such messages.

```
<%

Dim objMail Dim

bOK

Dim szText

  ' Create a new instance of the Mail object

  Set objMail = Server.CreateObject(“CDONTS.NewMail”) '

  Set up the e-mail

  objMail.From = Request.Form(“MyEmail”)

 objMail.Subject = “--> CALLBACK “ & Request.Form(“MyPhone”) & “ <--” '

 Change the next line to the address you want to send the message
to objMail.To = “callback@xyz.com”

szText = Request.Form(“MyName”) & “ has requested a callback on the
number above. If you have the AutoDial Ready To Go installed in
CallViewer, the call will be made automatically. “

szText = szText & “Please reply to this message with an ARM response
when the call is complete.”

  objMail.Body = szText '

  Send the message

  objMail.Send

  'You must always do this with CDONTS. Set

  objMail = Nothing

%>
```

```
<!DOCTYPE HTML PUBLIC “-//W3C//DTD HTML 3.2 Final//EN”>
```

```
<html>

<head>

<title>Web-Based Call Back Sample</title>

</head>

<body>

<p>

You request has been placed in a queue. You will be called shortly
when one of our agents is available.

</p>

</body>

</html>
```

CONFIGURING INTELLIGENT ROUTER

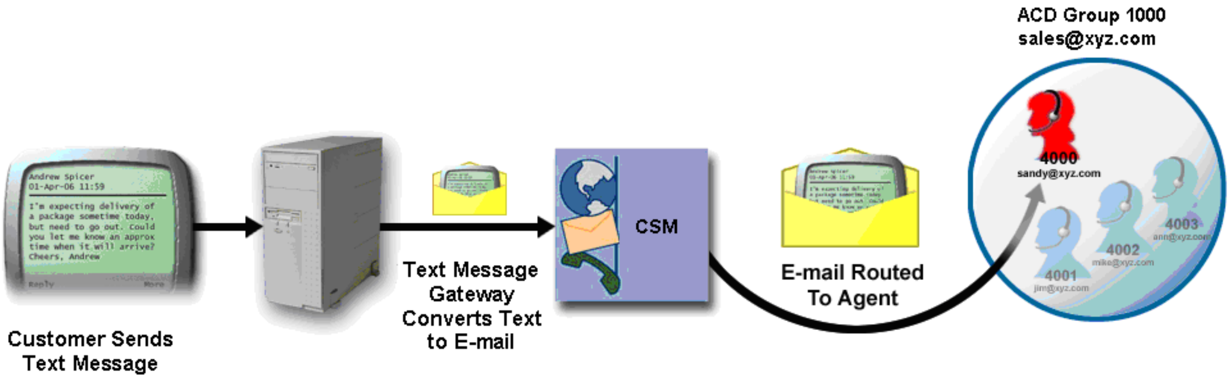
A standard media routing rule, as defined in “Routing E-mail Messages Example” on page 19, is all that is required for this scenario to work.

CONFIGURING CALLVIEWER

CallViewer or Connection Assistant need to be configured for each agent as described in “Configuring CallViewer” on page 165.

ROUTING MOBILE TEXT MESSAGES

Media Blending can be used to route mobile text messages to available agents when used with a mobile text to e-mail gateway. The basic principle is that the mobile text to e-mail gateway converts text messages received at a specific mobile number into an e-mail that is sent to the media blending queue. Intelligent Router then routes the e-mail to an available agent, whereby the agent can review the text message contained within, and act accordingly.



Andrew Spicer
01-Apr-06 11:59

I'm expecting delivery of a package sometime today, but need to go out. Could you let me know an approx time when it will arrive? Cheers, Andrew

REQUIREMENTS

To achieve this solution, in addition to the items outlined in “How Media Blending Works” on page 143, a mobile text to e-mail gateway is needed. The mobile text to e-mail gateway is software that converts text messages into e-mail messages and vice versa. Received mobile text messages are converted into e-mail messages and subsequently arrive in a given mailbox. It also allows a user to send an e-mail in some form such that it is sent to a given mobile number as a text message. There are two possible implementations for mobile text conversion and creation of an e-mail message:

- **Using a software application**: In this instance the customer site would run a piece of software on a server. Typically, the server would be connected to a GSM modem or mobile phone, which would be used to send and receive mobile text messages. The cost of sending such messages is dependent on the carrier and tariff used on the related GSM modem or mobile phone.
- **Using a third-party service**: In this instance the customer site uses a third-party service to act as the mobile text to e-mail gateway. The third-party service will provide the mobile number, and when mobile text messages are received on this number, they are forwarded to a given e-mail address in the customer’s domain. This option requires no additional infrastructure at the customer’s site, and can lead to reduced costs because the third-party provider can get discounted mobile text prices from bulk buying.

CONFIGURING THE MOBILE TEXT GATEWAY

Configuration of the mobile text gateway is dependent on the mobile text gateway software or service being used, and as such is beyond the scope of this document. Generally speaking, however, a third-party service requires little or no configuration, because they will provide a mobile phone number to send and receive the mobile text messages, and the customer provides an e-mail address to receive such messages. The e-mail address provided to the service would be one that is used as a media blending queue.

CONFIGURING INTELLIGENT ROUTER

A standard media routing rule, as defined in "Routing E-mail Messages Example" on page 159, is all that is required for this scenario to work.

SUMMARY

As can be seen from this document, the media blending functionality of Intelligent Router allows for more than just simple routing of e-mail messages. It permits several types of media to be presented to agents in a consistent form. It also enables the contact center to maximize the workload of agents by delaying non-call based media when call traffic is high, while processing non-call based media when call traffic is low.

This document details only a few ways that the media blending functionality can be used beyond just basic e-mail routing. Anything that can be converted into an e-mail can ultimately be routed to agents to process, and not necessarily in a contact center environment. For example, job assignment to on-site engineers, where jobs needing to be assigned are e-mailed to a media blending queue, which routes them to agents – the associated e-mail address is the external address of an engineer, who ARMs the routed e-mail when the assignment is complete.

Media blending performs *workload packet distribution* – whatever work can be encapsulated inside a packet, or e-mail, can be distributed.

Chapter 8

TROUBLESHOOTING

ACCESSING THE MICC OFFICE SERVER DIRECTLY

Accessing and modifying the MiCC Office database directly (and reports produced) is out of the scope of Mitel support. Reporter used in conjunction with the Auto Reporter module is often a better method of extracting statistical report data from Server for use in third-party applications.

LOG FILES

For MiCC Office v5.1 and later, application logs (including CallViewer logs generated by RTG macros) are located in the current user's application data directory as follows:

- **Windows 7 and higher** `C:\Users\<username>\AppData\Roaming\Mitel\Customer Service Manager\<application name>\Logs`

The Backup Utility logs are found here:

- **Windows 7 and higher** `C:\ProgramData\Mitel\Customer Service Manager\Backup Utility`

Table 1 provides the application log file names.

Table 1: Application Log Files

Application	File Name
CallViewer	Cvmain.log
	cvpkt.log
	cvnet.log
	cvrmt.log
	<*macro name*>.log
	<*action name*>.log
	cvrupgrade.ini
RealViewer	Wbmain.log
	wbnet.log
	wbrmt.log
	wbsystem.log
	wbsystem.log
	rvrupgrade.ini
Reporter	Wzmain.log
	wznet.log
	wzrmt.log
	wzsystem.log
	rptupgrade.ini
	smtp_<ID>.log
Reporter Real-Time	Rtmain.log
	rtnet.log
	rtrmt.log
	rtsystem.log
	rtupgrade.ini

Table 1: Application Log Files (continued)

Application	File Name
Backup Utility	DebugLog.Log
	Desktop_<yyyy_mm_dd>.log
	ProgressLog.Log
	ServiceLog_<yyyy_mm_dd>.log
	ServiceStateLog_<yyyy_mm_dd>.log
	ProcessState.xml
	ProgressFile.xml
	ProgressInfoFile.xml
	ServiceState.xml
	Setting.xml
	State.xml

FILE SENDER

MiCC Office v5.1 and later includes a tool (File Sender) designed to collect and send configuration and log files to Mitel Technical Support for troubleshooting purposes. File Sender should only be used by Mitel certified technicians when troubleshooting an issue with a MiCC Office application.

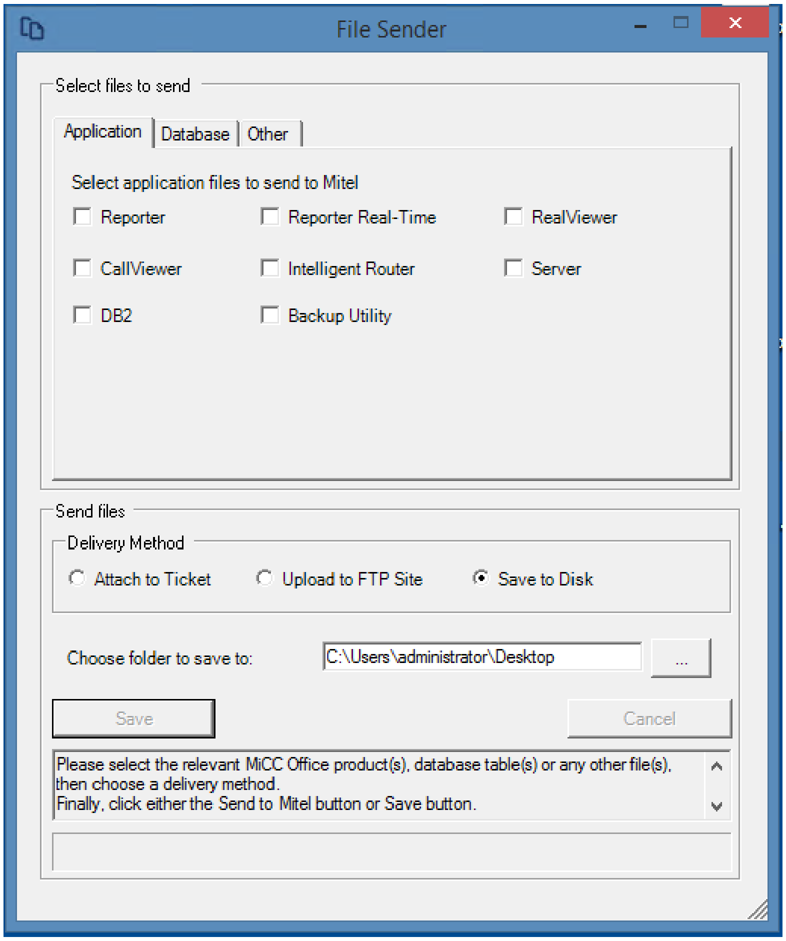
File Sender is a Windows application that is included in the and server installation package. This tool gathers and compresses the required files into a single zipped file so that the data can be quickly sent to Mitel Technical Support. File Sender requires a six-digit problem ticket number to properly route the zipped file it creates. Before using File Sender, you must open a problem ticket with Mitel Technical Support.

Before launching File Sender, close the MiCC Office application you are troubleshooting. This ensures that the latest changes to the configuration files are included in the File Sender zipped file.

To launch the File Sender tool, do one of the following:

- Locate and double-click the executable (for example, `C:\Program Files\Mitel Customer Service Manager\File Sender`).
- Launch the tool from the Windows Start menu (for example, Start – All Programs – Mitel Customer Service Manager – **File Sender**.

Figure 1: File Sender Tool



Delivery Method: ○ Attach to Ticket ○ Upload to FTP Site ● Save to Disk

Choose folder to save to: C:\Users\administrator\Desktop

Please select the relevant MiCC Office product(s), database table(s) or any other file(s), then choose a delivery method.
Finally, click either the Send to Mitel button or Save button.

NETWORKING-RELATED PROBLEMS

Table 2 includes networking-related problems for MiCC Office.

Table 2: Networking-Related Problems

Symptom	Possible Cause	Corrective Action
A module remains in the “Waiting For Connection” state and never connects.	The computer is configured incorrectly for networking.	If only one computer is experiencing this problem, then it is most likely that computer that is at fault. See Table 3 on page 181 for the network configuration you are using. If several computers are experiencing this problem, then it is more likely that the Server computer is at fault. See Table 3 on page 181 or the network configuration you are using. If network configuration for the above computers appears valid, then there is an underlying problem on the computer network and you should consult your IT department.
	Server is not running.	If the Server computer is not powered on, power it on. If the PC is powered on, check the tray bar for Server to see if there is a flashing question mark. If there is, the service is not running, go to the Server Control Panel and click **Start**.
	The Computer Identification name is correct but the Server name is incorrect.	The network settings for **every** MiContact Center Office application should have the same name or the server's IP address in the Server Name field. However, some versions of Windows show the short computer name while others show the full computer name in the Properties of My Computer. Any dashes/hyphens that are in the computer name MUST be present when that name is entered in the settings.
	Networking protocol is not installed or working properly.	See if you can connect to another network resource (e-mail, internet, etc.). If you cannot connect to other network resources, contact the your IT/MIS department for assistance.
The software connects but displays an error that the database is not available.	Permissions on the CTI_DATABASE folder are not properly configured.	Anyone who runs MiContact Center Office applications needs to have Read and Write access to the CTI_DATABASE share without being prompted for a password. You can test this access from the PC by selecting Start and then **Run**, typing **`\\<servername>\cti_database`**, and then click **OK**. If you see a list of files, then you have Read access. To test the write access, open the `Archive.log` file in Notepad, make a change to the file, and then save the file (do not use Save As). If you receive an error or Notepad displays the **Save As…** dialog box, then you do not have Write access. If you either never see the contents of the folder or cannot save the file, contact your IT/MIS department to ensure that these permissions are configured in a manner that will not conflict with your security policies.

NETWORK CONFIGURATION PROBLEMS

Table 3 includes network configuration problems for MICC OFFICE.

Table 3: Network Configuration Problems

Symptom	Possible Cause	Corrective Action
Network problems	Incorrect TCP/IP configuration	**TO TROUBLESHOOT NETWORK PROBLEMS:** 1. From PC, “ping” the Server's *computer* name (e.g., PING MICCOSERVER). If this works, both computers are on the network and your problem is unlikely to be network-related. 2. From PC, “ping” the Server's *IP address* (e.g., PING 172.16.14.71). If this works, TCP/IP is working on both PCs, but not necessarily name resolution; go to “Name Resolution” on page 104. 3. From the PC, “ping” any other IP address on your network. If this works, then the Server is most likely not powered on. Turn on the Server. 4. If you cannot “ping” other computers on your network, consult your IT department. 5. If name resolution does not appear to be working, “ping” your WINS and/or DNS IP addresses. If either of the “ping” operations fail, check with your IT department that those servers are running and that your computer is correctly configured to use them.
	File and print sharing	From the PC, click Start, then **Run** and type **`\\<Server computer name>`** (e.g., \\MICCOSERVER) and press **Enter**. • If, after 30 seconds or more, you get no response, file and print sharing is probably not installed on the Server. • If you are prompted for a username and password, refer to “Shared Folders” on page 105. • If an Explorer window opens, but you do not see an item labeled CTI_database, you should reinstall Server. • If you can see the CTI_database share, open it and try to create a blank text file. If you cannot, refer to “Shared Folders” on page 105.
	Miscellaneous	Check the following: • **Network card**: Some network cards are sub-standard. The use of 3COM and Intel network cards is recommended. Problems may be resolved by putting known-working NICs in the machines. • **Latest network card drivers**: Again, some drivers will have bugs in them, and a few site issues have been resolved by installing the latest NIC drivers. • **Main server configuration**: If PCs (including Server) use WINS or DHCP, their successful operation is likely to be affected by successful installation of the main network server. Check to see if DHCP or WINS is working correctly. Also check to see if the name has been registered with WINS by looking at the WINS Manager on the NT Server and searching for the name in the list of mappings. • **Firewall***:* If there is a firewall between the PC and the Server computer, then the firewall should be configured to allow the relevant ports. See Firewall Ports Table8 on Page 28

VOICE RECORDING PROBLEMS

Table 4 includes voice recording problems for MICC OFFICE.

Table 4: Voice Recording Problems

Problem	Probable Cause	Solution
I cannot play back voice recordings.	The computer running Reporter does not have the appropriate software installed.	Install the call recording integration software on the computer running Reporter. Refer to the CRE original equipment manufacturer's documentation.
	There is no available license on the Server key.	You will see an error when launching Reporter if call recording is not licensed on the Server.
	Server cannot communicate with the CRE.	Make sure the voice recording server name programmed in Server matches the name programmed in the voice recording server. If necessary, update the information in Server.
	The voice recording server is not on the network.	Make sure the voice recording server is connected to the LAN. If it is, try to ping the server. If the ping fails, verify that the server is on the same subnet as the MiCC Office Server.
The voice recording server does not recognize the T1 trunks.	The CRE equipment is not programmed properly.	Make sure you have the correct digital network information programmed in the voice recording server. The information programmed in the **Digital Network** tab (for example, line build-out, framing scheme, etc.) for the T1 Tap card must match the information programmed for the T1/PRI card in the system Database Programming.
Calls are not being recorded.	The connection between MiCC Office Server and the CRE equipment server is down or incorrectly configured.	Make sure MiCC Office Server is configured with the correct CRE name and that both servers can connect to the network. Make sure the channel settings for trunks and/or extensions in MiCC Office Server match those assigned in the CRE. Also, make sure the trunks and/or extensions are mapped to channels. If a channel is not mapped, that channel is not recorded. Make sure the CRE server is turned on.

INVALID STATISTICS-RELATED PROBLEMS

Table 5 includes statistics-related problems for MiCC Office.

Table 5: Invalid Statistics-Related Problems

Symptom	Possible Cause	Corrective Action
Invalid statistics	User error	
	• Misinterpretation of statistic/data – User does not have sufficient knowledge of the product, statistics, etc.	Attend technical training at Mitel University or contact Mitel Technical Support
	• Incorrect report “filter” – User selects/creates filter that is not what they think it is.	
	Incorrect installation, setup, and configuration	
	• Duplicate trunk or device IDs (i.e., networked system does not conform to the Universal Numbering Plan) for multi-node sites only.	Program the system to conform to Universal Numbering Plan.
	• The system node(s) database programming is incorrect.	Fix errors in the system database programming.
	Lost OAI data between the system and Server could be due to:	
	• Server was “down” due to:	
	• Intentional shut down by technician for maintenance, upgrades, and AMC (Adds, Moves, Changes).	Restart Server.
	• Unintentional shut down (power glitch, PC glitch, network glitch, software glitch, etc.).	
	• The system node was “down.” If one node goes down in a multi-node site, Server loses data from *all* nodes.	Bring node back up.
	Communication lost between CT Gateway and/or Call Processing Server with MiCC Office Server due to lost Server data (packets) between Server and applications over LAN/WAN due to a networking problem.	
	Software Bugs in:	
	• MiCC Office Software	Update to the latest version of software.
	• The MiVo 250 switch with System OAI	
	• CT Gateway - for multi-node networked system sites only	

SECURITY-RELATED PROBLEMS

Table 6 includes security-related problems for MICC OFFICE.

Table 6: Security-Related Problems

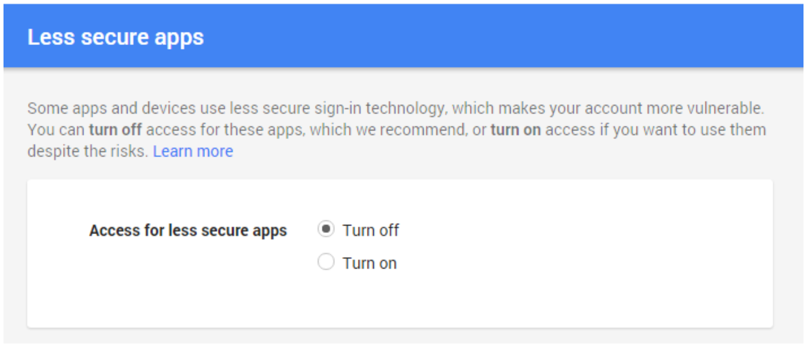
Problem	Probable Cause	Solution
Certain options are not available when I try to access them.	Your password level does not allow access to that option.	Change the password level, if necessary (see "Setting Security Levels" on page 110). Otherwise, contact the System Administrator to change your password level.
I periodically have to re-enter my password.	Server has gone down or has reset.	This is a security feature to ensure that no one has unauthorized access to the Server database. You must re-enter your password to re-establish a connection with Server.
When I upgrade the software, I am not given the option to start Server with a blank database. I don't want to convert my old database because it is corrupt.	The upgrade does not allow you to clear out the database. This helps to prevent loss of data.	Attempt to upgrade the existing database. If the upgrade fails, you may have to uninstall and re-install Server.
When I enter an agent, trunk line, hunt group, or extension description, the information automatically changes whenever I access the database again.	Server is retrieving information from the MiVo 250 database.	This is how SmartSync works. With SmartSync, you do not have to manually enter agent, trunk line, hunt group, or extension information in the Server database. If you do, Server automatically overwrites the information with the data from the MiVo 250 whenever the two systems synchronize. If you want to change the description, you must do so in Database Programming, not in Server.

GMail Security Configuration

If using Gmail for your SMTP connection, 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

Screenshot of setting:



Less secure apps

Some apps and devices use less secure sign-in technology, which makes your account more vulnerable. You can **turn off** access for these apps, which we recommend, or **turn on** access if you want to use them despite the risks. Learn more

Access for less secure apps ● Turn off ○ Turn on

MISCELLANEOUS PROBLEMS

Table 7 includes miscellaneous problems for MiCC Office.

Table 7: Miscellaneous Problems

Problem	Probable Cause	Solution
CallViewer displays the wrong DND message.	During initialization, MiCC Office downloads the DND messages for the first node it initializes with, and therefore the DND messages can be different from those displayed on the phone.	Program the same DND messages in the same order on all nodes to which MiCC Office Server is connected.

Appendix A

STATISTICS

INTRODUCTION

Every piece of data that can be displayed in MiContact Center Office is a statistic. Some of these relate to information about a particular call, but the majority of statistics are calculated values. How you choose to create your tiles and filters affects how the statistics are calculated.

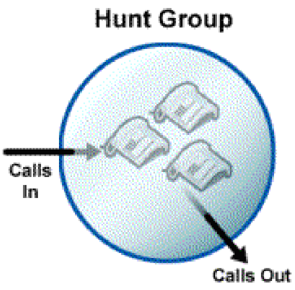
CALCULATE STATISTICS

On the **General** tab of the Add/Edit Filter dialog box ("General" on page 44) you can choose to calculate statistics by device or by trunk line. In Reporter the **By Device / By Trunk** option is selected on the **Filter** tab of report properties, and is defaulted depending on how the report is grouped. In Reporter Real-Time and RealViewer the choice is made in the filter options and this setting is defaulted for you when you create the filter, so you should not need to change it. How this setting is defined affects how statistics are calculated, because it affects how calls are modeled.

CALCULATING STATISTICS BY DEVICE

In this method, statistics are calculated by modeling calls on devices (extensions, agents, and hunt groups) that the trunk call was active on. This means that transferred calls are included when calculating the statistics.

Figure 2: Statistics by Device



For example, a call that rang at group 1000, was answered at 210, but then transferred to group 1001, would be considered as two calls; one that initially rings 1000, and one that rings at 1001.

For the majority of reports, this setting is the most appropriate.

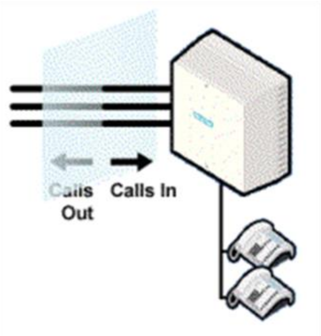
The best way of visualizing this is to imagine a sphere of glass surrounding internal devices in the PBX. Statistics are calculated by considering the trunk line call traffic that has passed through the sphere's external surface.

✓ You would choose to calculate call statistics by device when you were measuring the number of calls that alerted a particular, hunt group or extension device.

CALCULATING STATISTICS BY TRUNK

In this method, statistics are calculated by modeling calls on the trunk line that the call was active on. This means that transferred calls are ignored when calculating statistics.

Figure 3: Statistics by Trunk



For example, a call that rang at group 1000, was answered at extension 210, but then transferred to group 1001, would be considered as one call.

The best way of visualizing this is to imagine a piece of glass cutting through the trunk lines that connect the PBX and the Network Provider. Statistics are calculated by considering the calls that have passed through the glass.

However, there are instances when calculating statistics by trunk does not necessarily make sense when done in the context of certain types of filters. This is because “by trunk” call count statistics are calculated by considering only the last call segment record of an entire call chain.

For example, consider an inbound trunk line call that was answered by a hunt group member, and then subsequently transferred to a different extension device on the telephone system, where the call was then ended.

In this case, only the last call record corresponding to the final device that the call was transferred to is considered when working out how many calls have been received from the network provider. “By trunk”-orientated call count statistics are calculated this way to optimize the speed at which statistics can be calculated from a large number of call records.

Filtering options that are appropriate to use for by-trunk orientated statistics are the “longitudinal” filtering options that will not exclude any particular record in a complete call segment chain. Such filtering options are the trunk line device, DID number, and telephone number filtering parameters.

Most other filtering options, such as the other device, agent ID, and call duration options, can be considered more “sectional” filtering parameters, which may include only individual record “fragments” of the entire underlying call segment chain. These tend to translate “by-trunk”-calculated statistics into unsuitable results because the filter might not include the final call record of some call segment chains. This means that the corresponding call count for those matching call chains may or may not have been necessarily incriminated, depending on whether the call segment chain ended “inside” the applied filter.

When using “sectional” filtering options, these are often instances where it is more appropriate to use the “by device” statistics calculation option because one would ordinarily want to count calls from the perspective of an internal telephone system device entity (i.e., how many calls have been presented to a particular hunt group).

✓ You would choose to calculate call statistics by trunk line when you wanted to know the actual call traffic entering the telephone system from the network provider. For example, you might want to measure how many calls have originated via different DID numbers or from different sets of trunk lines.

The default All Calls filter calculates call statistics this way.

GROUP STATISTICS

In Reporter, statistic reports are grouped by a particular value. For example, a report grouped by telephone number collates all calls with the same telephone number, and calculates statistics for those calls; a report grouped by 30 minute intervals collates all calls within the same 30 minute interval, and calculates statistics for those calls.

When you group by device or by agent, more than one device or agent could easily have handled the call. For example, a call that rings 1000 and is answered at 210; statistics at both 1000 and 210 are updated.

This will mean that if you run a report grouped by device, you are likely to see a greater number of total calls than for a report grouped by telephone number. This is because the device report is taking into account calls that have been handled by multiple devices. A device grouped report will be exactly the same as if calculate statistics by device had been chosen.

CALL SUMMARY STATISTICS

Call Summary Statistics are usually a single number or piece of information that summarizes the calls for a particular group or filter. Such statistics can be displayed on Deskboard or multi stat tiles or graphed on the graph tiles. Examples include Total Inbound Calls, Calls Refused, and Agents Logged In.

Call Summary statistics include the following categories:

- Call Details: Call statistics that show specific details for each call.
- **Call Totals**: Call statistics that increment after call termination, for example, Calls In Completed.
- **Active Call Statistics**: Real-time call statistics, for example, Calls Queuing.
- **% Call Totals**: Percentages of call statistics that increment after call termination, for example, % Answered <= 5, 15, 30, 60, 90, or 120s. Service level statistics are included in this category.
- **Call Times**: Various times of call and e-mail statistics, for example, Avg Ans Time (E-mail).
- **Agent Statistics**: All agent statuses, for example, Logged In, Idle, and Busy (Call).
- **DND Statistics:** DND statistics for extensions.
- **Network Statistics**: Tools for testing traffic over the network between the application and the MiCC Office Server, for example, Packets Sent / Minute.
- **Miscellaneous**: Time and date options.

Detailed information about each individual statistic and the license required to use it are available in the Reporter Help File. This is available where the application is installed or from Mitel Online

Part No. 835.3272
Release 6.2 SP1
January 2017

Powering connections