A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise
System Engineering Guide

Release 9.8
Document Version 1.0

October 2025

Mitel
Powering connections

Notices

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.

®,™ Trademark of Mitel Networks Corporation

Contents

About This Guide

The *MiContact Center Enterprise System Engineering Guide* is a reference guide used by planners and implementation specialists to determine the system requirements for MiContact Center Enterprise, as validated by the quality assurance department at Mitel Networks. The following topics are included:

• **MiContact Center Enterprise deployment models**
  This section discusses different contact center topologies based on type of call manager integration, contact (traffic) volumes, overall network topology and chosen resilience method.

• **System requirements**
  This section specifies the hardware required to run the servers based on their role and implementation details. In addition, software applications that are supported and have been verified as compatible with the current release are listed here. Requirements for virtual applications are also described in this section.

• **Server virtualization and client virtualization**
  This section includes the supported virtualization software for servers and clients.

• **Performance and scalability**
  This section describes capacity limits, based on verification testing, for all media types, including voice, email, chat, open media, and SMS. IVR Routing scalability and port sizing are also discussed here.

• **Bandwidth and storage requirements**
  This section provides an estimate of how long a server's disk space will last based on the volume of information being collected. It also includes recommendations for disk space, network connectivity requirements, and bandwidth requirements.

• **Additional considerations, including:**
  – Translated language support
  – Synchronized time settings
  – Backing up data

• **Licensing**
  Refer to this section for all licensing details.

• **Statements of support**
  This section contains information on various supported features and applications, as well as a brief discussion on software assurance.
  To report an issue with this document, please email to techpubs@mitel.com.

Searching for key words and topics

You can search for content in this PDF by using the search function built into Adobe Acrobat or Reader. Consult your Adobe documentation for other search options.

To search for a key word or topic

- In the open PDF, press Ctrl+F.
- Alternatively, right-click in the document and select Find.
- Type the key word or topic for which you want to search.
- Press Enter.
- Navigate the results by clicking the Next or Previous buttons.

Printing this guide

We have designed this guide as a double-sided flipchart. Although printing options are specific to each printer, you must select the following printing options to print a double-sided flip-chart guide:

- Double-sided
- Landscape
- Flip pages up (on the long side)

Locating the Latest Version of Our Guides

The MiContact Center Enterprise documentation library is included in the downloadable Media Kit at the Mitel SW download site, accessible via Mitel MiAccess. It can also be found at the Mitel Document Center also accessible via Mitel MiAccess.

MiContact Center Enterprise Deployment Models

You can determine the number of servers you will require based on the following:

- **Type of Call Manager integration**: TAS together with MX-ONE, Cisco or Telepo, or OAS together with MX-ONE.
- **Contact volume:** The number of contacts being handled during peak hours affects the number of servers required.
- **Network requirements:** Additional servers may be required based on the network topology.
- **Availability:** Servers will be required depending on the level of resiliency, redundancy, and availability that is required. Whether it is warm or cold standby status, N+1 redundancy or high availability via VMware or Neverfail.

Deployment models based on Volume and concurrent agents

Refer to the figure below to determine your server deployment model based on volume and concurrently logged on agents. Your deployment should fit into one of the server configurations described in this section (Tier 1, 2 or 3).

The volume of interactions per hour and active agent count directly dictates the chosen deployment model.

Regarding server resource specifications, see section *"Server hardware requirements"* below.

Recommended deployment model based on the volume of interactions during busy hours combined with number of concurrent agents:
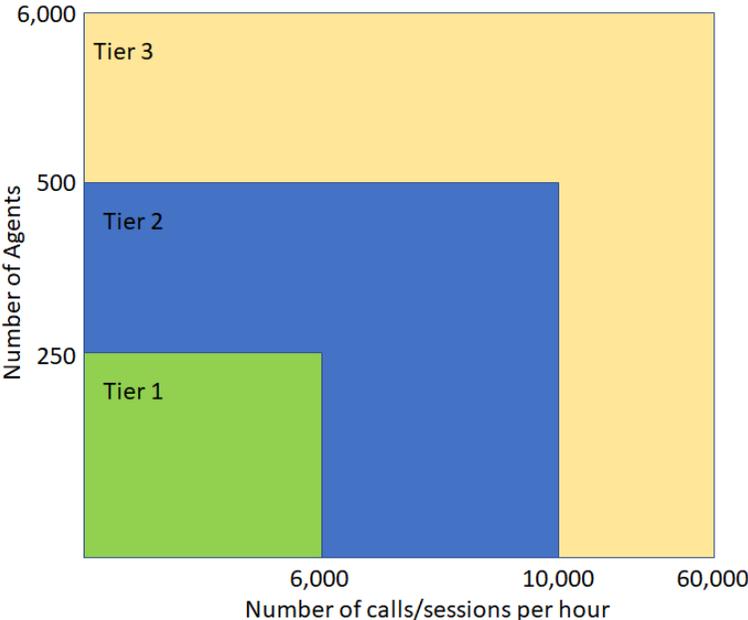
Tier 1

In this model the contact center is deployed on a single server. Up to 250 concurrently logged on agents and up to 6,000 busy hour customer contacts (voice, E-Mail, SMS, Chat and/or Open Media) are supported in this model. The SQL database can be running locally or on a separate server. The CTI and media services can support up to 6,000 calls per hour in this model.

Single server

Up to:
250 concurrent agents
60 IVR ports
6,000 calls/hour

Tier 2

Tier 2 is used for systems with between 250 and 500 concurrently logged on agents and a call volume of less than 10,000 calls per hour. In this tier, two servers are used where the CC services (plus optionally the SQL database) are deployed on one server and the CTI, Media and IVR services are deployed on a separate server.

MiCC-E + database

OAS/TAS, IVR and Media Ports

Between 250 and
500 concurrent agents

Up to:
60 IVR ports
10,000 calls/hour

Tier 3

Tier 3 is used for systems where the number of concurrently logged on agents exceeds 500 and/or the peak hour call volume exceeds 10,000. In this model the recommendation is to split the CC services between two servers, one handling all traffic related services and separate out the data processing intensive services (archiving and reporting plus SQL database) to a server of its own.

The following services should be installed on the data processing server:
- SQL database (if not installed on external server)
- Report Service
- Archive Service
- Event Service (should also be installed on MiCC-E traffic server)

MiCC Enterprise traffic handling Services

Up to 6,000 concurrent agents

MiCC Enterprise data processing Services + SQL DB

OAS/TAS and IVR

Up to 10,000 calls per hour

Up to 6 of these IVR and Media Server combos:
60,000 calls/hour
3,000 IVR ports

Media Servers (up to 5)

Up to 100 IVR ports each
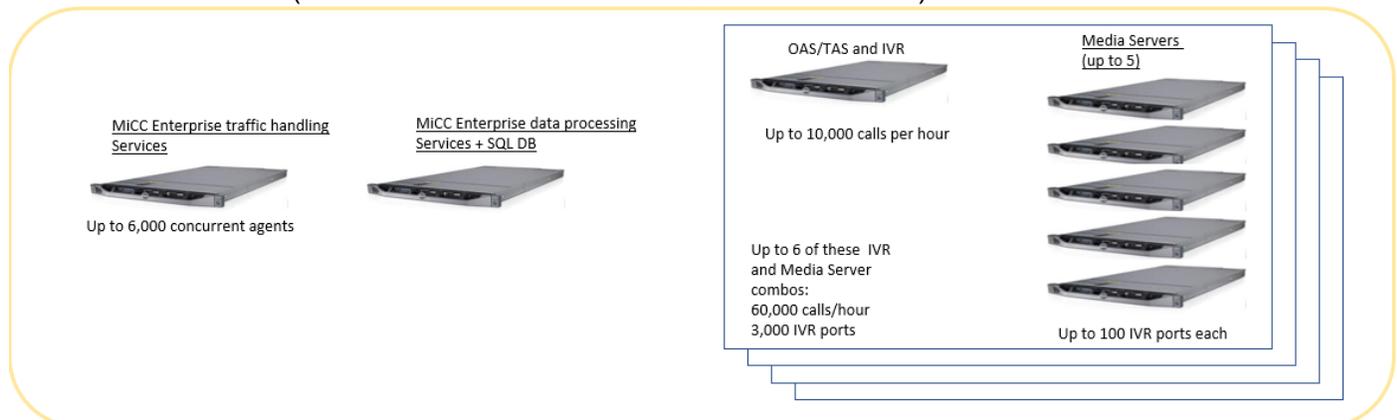
Number of Media Servers

The number of Media Servers needed is calculated differently depending on whether OAS or TAS is used as the CTI and Media Server platform. For OAS based systems the number of concurrently used media ports is the determining factor, and for TAS based systems the deciding factor is the number of concurrently voice connected agents together with the maximum number of queuing calls during peak traffic.

OAS based systems

For Tier 1 based systems, where the whole contact center resides on a single server, the Media Server is capable of handling up to 60 media channels. These media channels are used both for IVR and delivery of queue messages. To calculate the number of Media Channels needed the SecCalc tool can be used. It is available in the Tools folder on the MiCC-E Media Kit. If more than 60 media channels are needed a second server with a second instance of the OAS Media Server component is required. Each stand-alone OAS Media Server supports up to 100 media channels/IVR ports.

TAS based systems

The deciding factor to determine the number of Media Servers required for TAS based systems is the Media Server's maximum limit of handling 500 concurrent connection points. A connection point is the termination of one media stream. Each ongoing agent conversation requires 2 connection points: one for the agant and one for the customer. Queued calls and ongoing IVR sessions require one connection point each. An example: a contact center has 200 agents, expects 200 calls in queue and 75 concurrent IVR sessions. The number of connection points to handle will be (200*2)+200+75=675. Two Media Servers will be needed.

Recommendations for Co-locating Server Applications

MiContact Center Enterprise is a highly distributed system where various components can be distributed to run on different server hosts. Based on the deployment model Mitel recommends the following distribution.

Tier 1 deployment

In this model all services (MiCC-E, TAS/OAS and optionally SQL database are installed on one single server host.

Tier 2 deployment

In this model the MiCC Enterprise components plus optionally the SQL database are installed on one server and the CTI and Media Services (OAS or TAS based) are installed on a separate host. If heavy IVR use is expected, then the IVR (Script Manager) services could also be installed on the OAS/TAS server in order to reduce network signaling.

Tier 3 deployment

In this model the single MiCC Enterprise Server is split into two separate servers as described above:

1. Traffic handling server
2. Data handling server

For information on database usage and projected database growth statistics, see *Bandwidth and Storage Requirements* below.

Microsoft SQL Server Recommendations

A Microsoft SQL database is required for each MiCC Enterprise system. The SQL server can be installed on one of the MiCC Enterprise servers or be hosted on an external server. Microsoft SQL Standard, Enterprise or Data Center versions are supported for production systems. For lab, reference, staging or demo systems MS SQL Express can also be used. The amount of disk space can be calculated using the formulas specified in the User Guide "*Estimating Database Size*" available in the documentation library and available on the Doc Center accessible via the MiAccess portal.

Factors like archiving interval (the shorter the interval the more disk space is needed), retention period, call volume (call detail record storage) and configuration data (number of queues, agents etc.) will impact the amount of disk space needed.

Note that Azure SQL Database (serverless) is **not** supported by MiCC Enterprise. It lacks certain features needed by the MiCC Enterprise system. SQL Server running on an Azure hosted Windows Server instance is supported.

Choice of Call Manager integration

There are two options for call manager integration towards MiVoice MX-ONE: OAS and TAS.

OAS

The original integration uses the Open Application Server (OAS) as the CTI and Media Services platform for the contact center and IVR. This integration uses CTI-Groups in the MX-ONE as the landing point for the contact center calls. The pilot numbers for one or more CTI Groups form a BVD (Basic Virtual Device) which is monitored using CSTA via OAS to the MX-ONE, and incoming calls trigger Queued events to the contact center. The entry points into the contact center are Service Accesses which either trigger an IVR application to be executed or use the Auto Attendant feature to provide Welcome and menu selection messages to the caller.

When media services are requested to play messages and to listen to input from the caller then the call is temporarily connected to a media channel, SIP or extension in MX-ONE, and the media server of OAS performs the required media service.

When media services are no longer required the call goes back to the CTI Group queue and Music On Hold services are provided by MX-ONE. The call is at all times under the control of MX-ONE and can thereby utilize the availability and redundancy features of the call manager.

The obvious advantage of OAS is that calls stay under control of the call manager and backup solutions to fall back to PBX ACD or Hunt groups are easily achieved.

Among the drawbacks is the complexity of setting up load balancing and redundancy solutions in larger systems with multiple OAS servers.
Other limitations compared to TAS include:

- TLS 1.3 is not supported
- SRTP voice encryption not supported
- TLS not supported on the CSTA III interface
- No user authentication possible on the CSTA III interface

Figure: Sample diagram of OAS based system
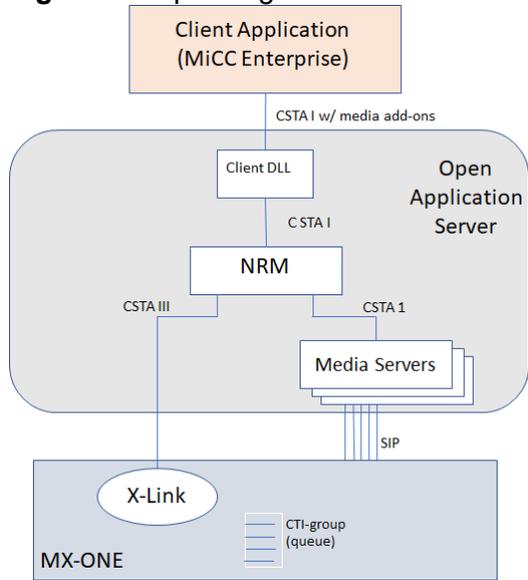
TAS

The alternative call manager integration to use is the Telephony Application Server (TAS), which was initially developed in order to be able to connect MiCC Enterprise to call managers other than MX-ONE. It uses a SIP trunk connection from TAS to the call manager, and TAS and its Media Server(s) terminate each contact center call (inbound as well as outbound). TAS also acts as a SIP registrar for the agents using the MiCC Agent application in soft phone mode. It is now also available to customers using MX-ONE as a call manager and support for CSTA is included to give full CTI capability to agents using MX-ONE connected phone sets (desk or remote/mobile extensions).

Figure: Sample diagram of TAS based system connected to Cisco or Telepo
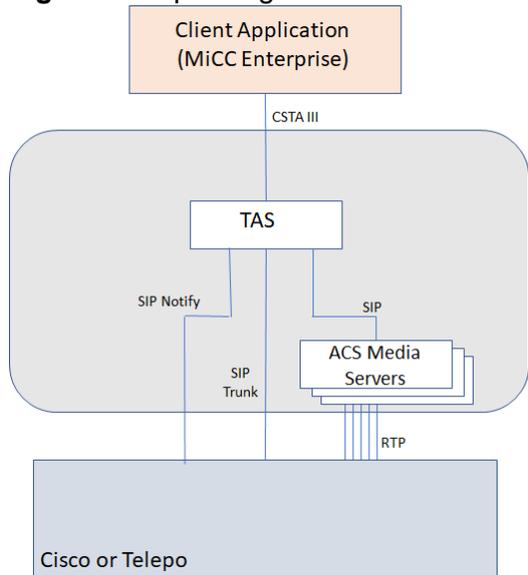
Figure: Sample diagram of TAS based system connected to MX-ONE
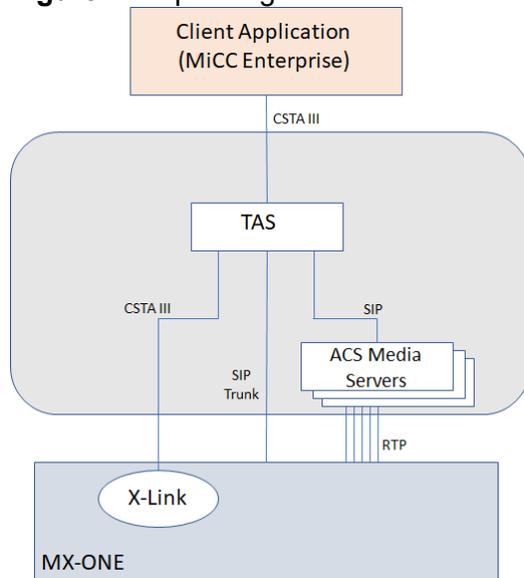
When using TAS, automatic load balancing is enabled when agents log on to a system with multiple TAS servers. The MiCC Enterprise system will automatically distribute agent logons over multiple TAS servers, and in case of failure of a TAS server all agents using the failing TAS server will automatically be moved over to a working TAS without having to log off and back on again. This enables easy setup of systems using N+1 type redundancy for the TAS server(s).

Another advantage of TAS based systems is that the termination of the calls on the server enables better control of the calls and call features. For example, when agents serve as Attendant Agent the features for sending callers directly to the wanted party's voice mail box, and the capability to call through an active diversion are only available when TAS is used. Also, voice encryptions for calls between the call manager and the media server are only possible when TAS is used. TAS also supports TLS 1.3 and to enable TLS and user authentication on the CSTA III i/f towards MX-ONE.

Resilience and Redundancy options

There are several different options when it comes to resiliency and redundancy including various variations of cold, warm, or hot standby systems, N+1 redundancy (applies to OAS and TAS plus their Media Servers), VMware HA and Neverfail Continuity Engine.

Stand-by system

This type of redundancy is provided by having a second, stand-by system installed. The stand-by system could be in different stages of readiness such as cold, warm, or hot.

Cold stand-by

Cold stand-by typically refers to a stand-by system that is shutdown when not in use and in case of severe failure on the active system the server is booted up and made ready for service. Depending on how incoming service calls are routed to the system, it might be necessary to manually redirect the incoming traffic to the backup server.

Warm stand-by

Warm stand-by typically refers to a backup system that is booted up, but the contact center services need to be manually started up on the backup server(s) in case of failure of the active system. Again, depending on how incoming service calls are routed to the system, it might be necessary to manually redirect the incoming traffic to the backup server.

Hot stand-by

Hot stand-by refers to a backup server that is booted up and fully ready to handle incoming service calls. In this scenario (as well as for cold and warm stand-by) agents need to logoff and back on again specifying the backup server as the MiCC Enterprise server location.

A way to avoid this is to manually update the DNS server record for the server hosting the MiCC Enterprise Broker service, which in the case of multiple MiCC Enterprise servers would be on the server hosting the traffic handling services. In the hot stand-by case the passive server needs its own unique set of access numbers so that the standby system does not interfere with the active system. Depending on how incoming service calls are routed to the system, it might be necessary to manually redirect the incoming traffic to the backup server. There are techniques that could be used to configure a fallback destination for incoming calls should failures be detected.

In case of active OAS server failure, backup CTI-Groups in MX-ONE can be configured so that calls would overflow to the backup groups in case of loss of monitor on the MiCC-E group. These backup groups are then monitored and used by a stand-by OAS server.

In the TAS case, an alternative SIP route can be configured in the call manager so that if an Active TAS server fails, calls can re-route to a stand-by TAS server in case of congestion.

N+1 redundancy

This type of redundancy is the recommended way to provide redundancy to any type of Media Server (OAS or TAS based) and to TAS servers. It can be used also for OAS servers but due to the complexity of having to "manually" load-balance agent utilization between OAS servers, and agents having to logoff and back on again in case of OAS server failure, it is recommended that either VMware HA or Neverfail provided redundancy is used for OAS.

For multi-TAS systems this is the recommended redundancy solution. As an example, the traffic level calculation concludes that 2 TAS servers and 4 Media Servers would be needed to manage the traffic load. To provide a redundant system install 3 TAS servers (2+1) and 5 Media Servers (4+1). Each TAS server should be configured to use all 5 Media Servers. Round Robin load balancing built into TAS ensures that all 5 Media Servers will be utilized evenly. Should one Media Server fail or manually be taken out of service for maintenance, the remaining 4 will be able to carry the full load until the failed server is recovered. TAS will detect that the server is back online, and it will automatically start to be used again.

Similarly, should one of the 3 TAS servers fail or be taken out of service for maintenance then agents using this server will automatically be distributed evenly on the 2 remaining TAS servers. The agents will be forced to Not Ready state during this process but are not required to log off and back on again. They will be notified when the move is completed and can then be put back to Ready (manually or automatically if so configured) and resume handling calls.

VMware High Availability

VMware High Availability (HA) provides failover protection against hardware and operating system outages and allows you to:

- Monitor VMware vSphere hosts and virtual machines to detect hardware and guest operating system failures
- Restart virtual machines on other vSphere hosts in the cluster without manual intervention when a server outage is detected
- Reduce application downtime by automatically restarting virtual machines upon detection of an operating system failure

Mitel requires that the partner's and/or customer's IT personnel setting up VMware HA on any MiCC Enterprise server are fully trained and certified on VMware. Please refer to the "*Virtualization Description*" in the documentation library and available on the Doc Center accessible via the MiAccess portal.

Neverfail Continuity Engine

This solution typically works hand in hand with VMware HA and adds application monitoring on top of the failover criteria provided by VMware. Neverfail can also be used on physical servers.
With application monitoring the Neverfail Continuity Engine is configured to failover to the backup server if a failure is detected on one of the monitored MiCC Enterprise services. Please see https://neverfail.com/product/continuity-engine/ for additional information.
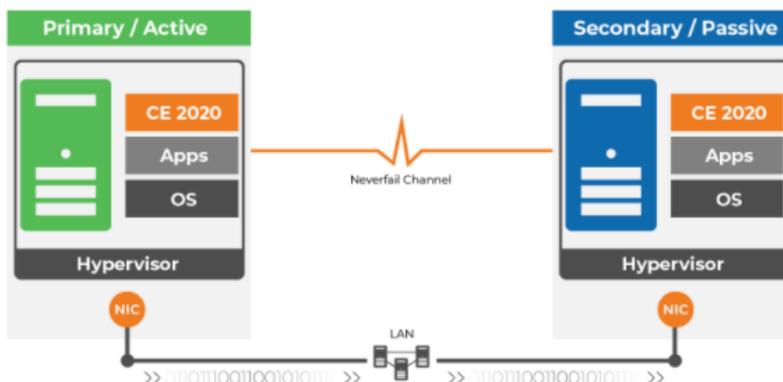
Mitel and Neverfail strongly recommend that the partner's and/or end customer's IT personnel take the Neverfail Admin training eLearning class. This self-paced, Web-based Administrator training is bundled with each Neverfail order and is provided through Neverfail University. Instructions to access training are provided on fulfillment of the Neverfail product.

Mitel has an OEM agreement with Neverfail and server licenses for the Neverfail Continuity Engine are sold by Mitel, which also provides support. Remote installation and configuration support is included in each purchase of a Neverfail license. See the document "*MiCC Enterprise Neverfail HA Quoting, Ordering, Fulfillment, Services and Support Process*" available on Content Hub for more details.

System Requirements

The following section outlines the hardware and software requirements for server and client systems within MiContact Center Enterprise. To ensure successful deployment in both lab and production environments, you must meet or exceed the system specifications outlined here. It is important when planning the deployment infrastructure to not only consider what the traffic rates will be when initially implementing MiContact Center Enterprise but also to consider the amount of growth over the lifetime of the system.

The system specifications outlined here provide the resources required to run the MiContact Center Enterprise applications and services under load and allow for an approximate 20% overhead for potential performance spikes during peak periods.

You must consider all applications and services running on the server when determining your server needs. The specifications described here include baseline operating system overheads but do not include additional applications, such as productivity software, management and backup solutions. You must allow for these additional applications when determining your system requirements to ensure adequate resourcing for MiContact Center Enterprise applications and services.

Server Hardware Requirements

The following minimum requirements apply for a full MiCC Enterprise 9.8 installation (all components installed on single server):

CPU Performance	Dual Intel Xeon 3.0 GHz CPUs (8 vCPUs) [1]	Or equal or better performance on other architecture
Memory	8GB[2]	In addition to OS memory needs
Disk, MiCC-E SW	16 GB	
Disk, MiCC-E logs	50 GB	The more the better
Disk, SQL Database		See the User Guide "*Estimating Database Size*" available in the documentation library

The complexity of the configuration, the system size, and the load on the system determine whether higher performance and/or additional servers are required. Please refer to the section "*Deployment models based on Volume and concurrent agents*" for details.

VMWare, Hyper/V, Proxmox and Nutanix Requirements

When determining the allocation of resources (e.g., RAM, vCPUs, and disk space) to a virtual instance the same equivalent resources as for a physical server should be allocated. Please note that the hypervisor typically adds a ~10% overhead compared to equivalent resources on a physical server.

Lab measurements during high volume traffic shows that number of I/O operations per second (IOPS) is ~15/s.

---

[1] Standalone OAS, TAS or ACS Media Server can run on Single Xeon CPU or 4 vCPUs

[2] Standalone MiCC-E, OAS, TAS or ACS Media Server can run on server with 4GB RAM

Server Software Requirements

The following table defines which software technologies are supported or required by MiContact Center Enterprise. In accordance with Microsoft best practices, we advise you to update your Windows operating system with the recommended security patches, hotfixes, and service packs. For more information, consult your Microsoft documentation.

NOTE:
- If there is a technology that is not included in this guide and you are unsure whether it is supported, please contact your approved Mitel Account Team. For information on support requirements for Microsoft technologies, see http://www.support.microsoft.com.
- Install the appropriate antivirus software with the latest virus definitions and data backup software on the MiCC Enterprise Server. Ensure antivirus software is disabled before installing MiContact Center Enterprise.
- Depending on the antivirus software being used it may require disabling and re-enabling the software to add/edit exclusions.
- During testing, it was observed that running Windows Defender full scan can consume 80 to 90% of CPU usage, which will have negative performance impact on the MiContact Center Enterprise Server operations. We recommend running full scans only during off-peak business hours.
- To ensure your MiContact Center Enterprise applications can write to files without error, you must configure your antivirus software to exclude the installation folders of MiCC Enterprise, TAS/OAS and the Media Server. Typically, they are located under <installation_drive>:\Program Files (x86)\Mitel\

Software	Notes
Operating Systems	
Windows Server 2025 Standard and Datacenter	
Windows Server 2022 Standard and Datacenter	
Windows Server 2019 Standard and Datacenter	
Windows Server 2016 Standard and Datacenter	**NOTE:** Microsoft Windows Server 2016 Essentials is not supported.
Microsoft SQL Server	

SQL Server 2016, 2017, 2019 and 2022	SQL Server comes in different editions: Express, Standard, Enterprise, and Datacenter. They are all supported by MiCC Enterprise, but for MiCC Enterprise Multimedia systems, a non-Express edition of SQL Server is recommended due to the limitations of database size and number of connections.
	Azure SQL Database (serverless) is **not** supported by MiCC-E. It lacks certain features needed by the MiCC-E system. SQL Server running on an Azure hosted Windows Server instance is supported.

NOTE:

As MiCC Enterprise server software is supported only on the US English version of Windows Server, if the SQL Server is installed on the same host as the MiCC Enterprise server software, it too must be the English-language version. This is in accordance with Microsoft specifications that state that a localized SQL Server must be the same language as the Windows Server that it is installed on.

Client Hardware Requirements

Client hardware requirements depend on the number of applications and services being run on client computers. As you add applications concurrently on a single computer, your CPU, RAM, and hard disk space requirements increase. The following minimum figures apply for a full MiCC Enterprise client installation, including all available functions:

CPU Performance	Intel i3, 3 GHz or faster	Or equal or better performance on other architecture
Memory	4 GB	In addition to OS memory needs
Disk	15 GB	For application software and log files

Client Software Requirements

The following table defines which software technologies are supported by MiContact Center Enterprise. In accordance with Microsoft best practices, we advise you to update your Windows operating system with the recommended security patches, hotfixes, and service packs. For more information, consult your Microsoft documentation.

NOTE:

If there is a technology that is not included in this guide and you are unsure whether it is supported, please contact your approved Mitel vendor. For information on support requirements for Microsoft technologies, see http://www.support.microsoft.com.

Operating Systems	
Windows 11	Only exists in 64 bit
Windows 10	32 or 64 bit

Supported Technologies

WebRTC based Softphone in Web Agent

The integrated soft phone capabilities in the Web Agent application require an MBG providing WebRTC Gateway functionality to the agents.

Browsers

Supported Web Browser is in this initial release Chrome and Edge. Other browsers supporting WebRTC might work as well, but Chrome and Edge are the browsers that Mitel has fully validated and will support.

WebRTC Gateway

Mitel Border Gateway release configured to act as WebRTC Gateway is supported.
See the document Initial Configuration-Configure MBG for WebRTC available in the MiCC Enterprise documentation library for configuration details.

SMS

The SMS Gateway included in MiCC Enterprise supports two different connectivity methods:

Modems

Any SMS modem that supports SMS AT commands in PDU mode can be used. Text mode is not supported.
The SMS modem should either have a COM port series port interface or a virtual COM port via USB. Up to 4 modems can be handled by the SMS Gateway

SMS-C

The MiCC Enterprise SMS Gateway can connect to SMS Service Providers that support either SMPP protocol version 3.4, 4.0 or 5.0.

CRM integrations

CRM Connector

The CRM Connector offered by Advanced Services can be used together with MiCC Enterprise. It currently supports plugins to these and other CRM systems:
- Salesforce
- Microsoft Dynamics 365 (CRM)
- Zendesk
- Oracle CX (B2B/B2C)
- ServiceNow
- Zoho CRM

Using CRM Connector agents can click to dial, have screen popups with contextual information and take advantage of many other innovative features to increase their productivity and enhance the customer service they provide. More information about the CRM Connector can be found at Content Hub accessible via the partner portal MiAccess.

Older type integrations
SIEBEL CRM

MiCC Enterprise is compatible with the following versions of Siebel CRM:

Siebel 7.5, 7.8, 8.0 and 8.1

SAP CRM

MiCC Enterprise is compatible with the following versions and interfaces of SAP CRM:

SAP CRM 4.0. 5.0, 6.0 and 7.0 for server-side integration for use with SAP's web-based application

SAPPhone 3.x for desktop-side integration

BAPI for Server-side integration providing access to SAP Business Objects, from within the Script Manager, via RFC (Remote Function Calls)

OTHER CRM SYSTEMS

For other CRM systems, we will typically suggest our general-purpose integration points. These are:

- Script Designer for server-side integration of database access and/or web service APIs software
- Agent Service Open API for server-side integration
- For agent-side integration:
    - Launching of URLs as part of Agent Actions, with IVR data as arguments
    - DDE/COM/.NET interface for MiContact Center Agent

Please refer to the product documentation for details of the information and the operations that are available via these interfaces.

Server Virtualization

Server visualization, like client virtualization, allows for the virtualization of the underlying hardware on which the Windows operating system is running. Using server virtualization enables organizations to manage hardware, reduce hardware faults that can interrupt critical user services, and provide disaster recovery for the IT infrastructure.

Planning for Server Virtualization

When deploying MiContact Center Enterprise servers using virtualization, you must first carefully plan and size the virtualization infrastructure.

Virtualization infrastructure vendors provide tools and information on how to plan, reserve, and implement the appropriate virtual resources for all guest operating systems running within the infrastructure.

When running existing services on physical hardware and moving to a virtual infrastructure, we recommend you measure the average and peak resource allocation across disk, CPU, and memory to aid in scoping and sizing the resources to commit to each guest operating system.

Deciding which virtual hosts will service each virtual guest system is a critical planning step. The host must be provisioned to handle the average and peak resource utilization of all guest systems homed to that host, in addition to the performance overhead incurred by the hypervisor.

Mitel makes all efforts to validate and test against virtualization infrastructure and underlying hardware manufacturers' products. Support and engineering staff may request additional resources on virtualization servers, or additional resources on associated guest operating systems, to adequately cover usage by MiContact Center Enterprise services and to eliminate resource starvation as a possible cause of software issues.

For more information on planning resource allocation and virtual infrastructure sizing, please refer to your virtualization vendor's documentation.

The following section details the supported server virtualization technologies.

VMware ESXi

VMware ESXi supports both a single host environment and larger multi-host environments. Each host runs the same base operating system (VMware ESX) but the management software differs

when using multi-host clustered environments as you require VMware vCenter server. Supported technologies for VMware ESXi include:

- VMware vSphere

This release for MiContact Center Enterprise supports VMware ESXi 6.x and 7.x.

Nutanix AHV

MiContact Center Enterprise has been validated to be running on Nutanix AHV.

Proxmox Virtual Environment

MiContact Center Enterprise has been validated to be running on Proxmox 8.4.

Microsoft Hyper-V

Microsoft Hyper-V supports both a single host environment and larger multi-host clustered environments. Single host environments support a server running Windows Server 2016, 2019 or 2022. For multi-host clustered environments, an additional server capable of running the Microsoft System Center Virtual Machine Manager is required.

Hyper-V supports failover and live migration using Microsoft System Center Virtual Machine Manager. A Storage Area Network is required to support this.

Customers using Hyper-V can use Version 2016, 2019 or 2022 for the hypervisor and should stay up to date with patches and service packs.

In addition, it is strongly recommended to follow all Microsoft best practices for setting up, configuring, and maintaining your Hyper-V hypervisor servers. For more information, see **Hyper-V Technology Overview** on learn.microsoft.com.

Best Practices for Virtualization

MiContact Center Enterprise hardware and software recommendations do not change when running the MiCC Enterprise Server(s) in a virtualized environment.
When translating the physical hardware specifications outlined in this guide to your virtualized environment, you need to be aware of the makeup of the current physical processor, such as the type of processor, gigahertz speed, and number of cores available. For information on calculating the number of virtual CPUs required based on physical hardware specifications, please refer to your virtualization vendor's documentation.

You must use dedicated resources (as opposed to resource scheduling) when running MiContact Center Enterprise, TAS and OAS to ensure optimal performance and voice quality. When using shared resources, you may experience a degradation in performance and call quality caused by either the MiContact Center Enterprise being starved of processor resources or the hypervisor providing a lower processor priority for the MiContact Center Enterprise operating system instruction execution. If using shared resourcing, ensure you have sufficient resources to run the software according to the hardware specifications as outlined in this guide.
When the MiContact Center Enterprise server is starved for resources, you may experience the following adverse effects:

- Degradation of audio quality in IVR, when listening to music on hold and queue announcements, and during voice calls and degraded voice quality for MiCC Enterprise Agents using the integrated soft phone.
- NOTE: When OAS is used together with the MiVoice MX-ONE telephony platform then queuing and Music on Hold is provided by the MX-ONE. When TAS is used towards any of

the supported call managers (including MX-ONE) then all voice services including Music on Hold are provided by the external Media Server(s). Resource starvation for the Media Server(s) will result in degraded voice quality for all IVR sessions and agent conversations.

- Delays of call control commands such as answering calls, transfers, and ending calls
- Delays of user interface notifications of new interactions in MiCC Enterprise applications.
- Virtual host server requirements must be greater than the sum of all virtual machines that will run concurrently. Applications running on the host machine as well as other virtual machines configured on the host can affect the functionality of the MiContact Center Enterprise software. Please refer to your virtualization vendor's documentation for specific hardware and software requirements.
- While MiContact Center Enterprise is expected to function properly in a virtual environment, there may be performance implications that can invalidate the minimum system requirements as outlined in this guide.
- If Mitel support or engineering staff suspect that the virtualization layer or software are the root cause of a problem, you may be required to install the software on a non-virtualized server to eliminate virtualization as a root cause.
- Contact the appropriate vendor to resolve the virtualization layer issue
- For detailed information and specifications regarding running Microsoft or other third-party software in virtualized environments, please consult your virtualization vendor.

For additional information related to MiCC Enterprise and virtualization please see the description "*Virtualization Description, MiCC Enterprise*" in the user documentation library and available on the Doc Center accessible via the MiAccess portal.

Group Policies

Microsoft Group Policy infrastructure allows you to implement specific configurations for users and computers. Group Policy settings are contained within Group Policy Objects which are linked to Active Directory Service containers such as sites, domains, or Organizational Units. Group Policies are typically   implemented to control Windows features and their functionality for local and domain users.

Due to the large number of configuration settings and varying requirements for implementation across different organizations, we do not verify the implementation of Group Policies on Microsoft Windows Servers or client operating systems for MiContact Center Business. We recommend that the MiContact Center Enterprise Servers be placed in an Organizational Unit with a Group Policy that has the minimal Group Policy Settings, as deemed acceptable by your organization, applied.

Mitel support and engineering staff may, through the course of fault or performance diagnosis, require the   MiContact Center Enterprise Servers or client computer to be placed in an Organizational Unit with no Group Policy restrictions to isolate the fault from possible Group Policy conflicts.

Automatic Speech Recognition and Text to Speech

MiContact Center Enterprise integrates with Nuance Recognizer, enabling IVR applications to collect caller speech with which to populate variables and make menu selections.

MiContact Center Enterprise integrates with Nuance Vocalizer to support Text to Speech for IVR applications and to provide   prompts including TTS based Welcome and Queue messages.

These speech services are available for both OAS and TAS based systems by using the MRCP v2.0 protocol toward the Nuance Speech Server (NSS).

MiCC Enterprise has been tested with Nuance Speech Server 11.0.09 up to version 11.0.13. Older versions of NSS must be upgraded to this release.
Nuance Recognizer can be co-located on the same server as Nuance Vocalizer. Automatic Speech Recognition Servers and Text to Speech servers should not be co-located on any of the MiCC Enterprise, OAS or TAS servers.

For additional information for planning for, installing and configuring Nuance, see the included instructions in the MiCC Enterprise User Documentation library and the Nuance documentation.

The MiCC Enterprise IVR supports to execute VoiceXML applications in its integrated VoiceXML browser. VoiceXML 2.1 is supported.

NOTE: Microsoft is in the process of phasing out Nuance Speech Server (NSS). NSS has already been phased out for both Capex and Opex new sales, and a End Of Service has been announced for June 2026. Existing customer can continue to get support if their system is under SWA up to that date.

Performance and scalability

The agent and interaction traffic capacity results displayed below demonstrate the maximum interactions   for voice, email, chat, open media, and SMS in a blended environment, as verified for MiContact Center Enterprise on the supported call manager types and versions.

Verification Environments

Performance tests were conducted against the supported call manager platforms to validate the call manager platforms as specified in the section *Supported Call Managers* above. All tests are done in a VMware ESXi environment using meeting the HW and SW requirements stated in section *System Requirements* above.

Table: Verified system capacities

UP TO	WORKS WITH
50 agents and 1000 calls/h	MiCC Enterprise and OAS/TAS co-hosted on an Application Server Unit (ASU II or newer)
250 agents and 6000 calls/h	MiCC Enterprise and the OAS or TAS co-hosted on a single server.
10,000 calls/h	All of OAS or TAS on a single dedicated server.
500 agents	All of MiCC Enterprise on a single dedicated server. TAS or OAS on separate server(s)
6,000 agents	MiCC Enterprise distributed over two or more servers: - One or more for traffic processing services - One or more for data storage (SQL) and processing - Multiple OAS or TAS servers on separate hosts
60,000 calls/h	One MiCC Enterprise system with 6 OAS or TAS servers

OAS Media Server:
  -60 IP media ports
  -100 IP media ports
  -500 IP media ports
	-All of OAS on a single server
	-One host dedicated to the Media Server of the OAS
	-6 servers for one OAS:
	  - 1 for CTI link, NRM and OAS basic services
	  - 5 IP media servers

TAS (ACS) Media Server: -Up to 500 connection points	-An active call for an agent using a soft or desk phone requires 2 connection points, and each IVR call, and queued call requires 1 connection point.
-Number of Media Servers per TAS	-up to 5 (no hard coded limit but 4+1 has been tested and validated under full traffic load)

NOTE:

The supported number of "calls" mentioned above is the sum of all supported transaction types. Each agent interaction (voice call, e-mail, SMS, chat, and open media) is counted towards the maximum number of transactions supported, which is 60,000 per hour.

High Capacity settings

In systems with high it could be necessary to disable live updates of filter dialogs in MiCCE Agent. If the Agent application becomes sluggish or un-usable when the Contacts tab is opened, or the Monitor or Force agent status dialogs are opened then this can be avoided by disabling live updates of agent status in these dialogs. This is done by using the SecCfg registry utility on the MiCCE server and in the Agent Service tab enable the *Suppress Updates for Filter Dialogs* check box.
It could also be necessary to disable the automatic lookup of customer history for each incoming call to agent if the load on the SQL server gets too high. This can also be done using SecCfg and enable the check box for *Disable Auto History Search* in the Agent Service tab.

Verification topology

The following figure demonstrates a typical verification topology of the MiContact Center Enterprise performance lab.

Figure: MiContact Center Enterprise Performance Lab Topology
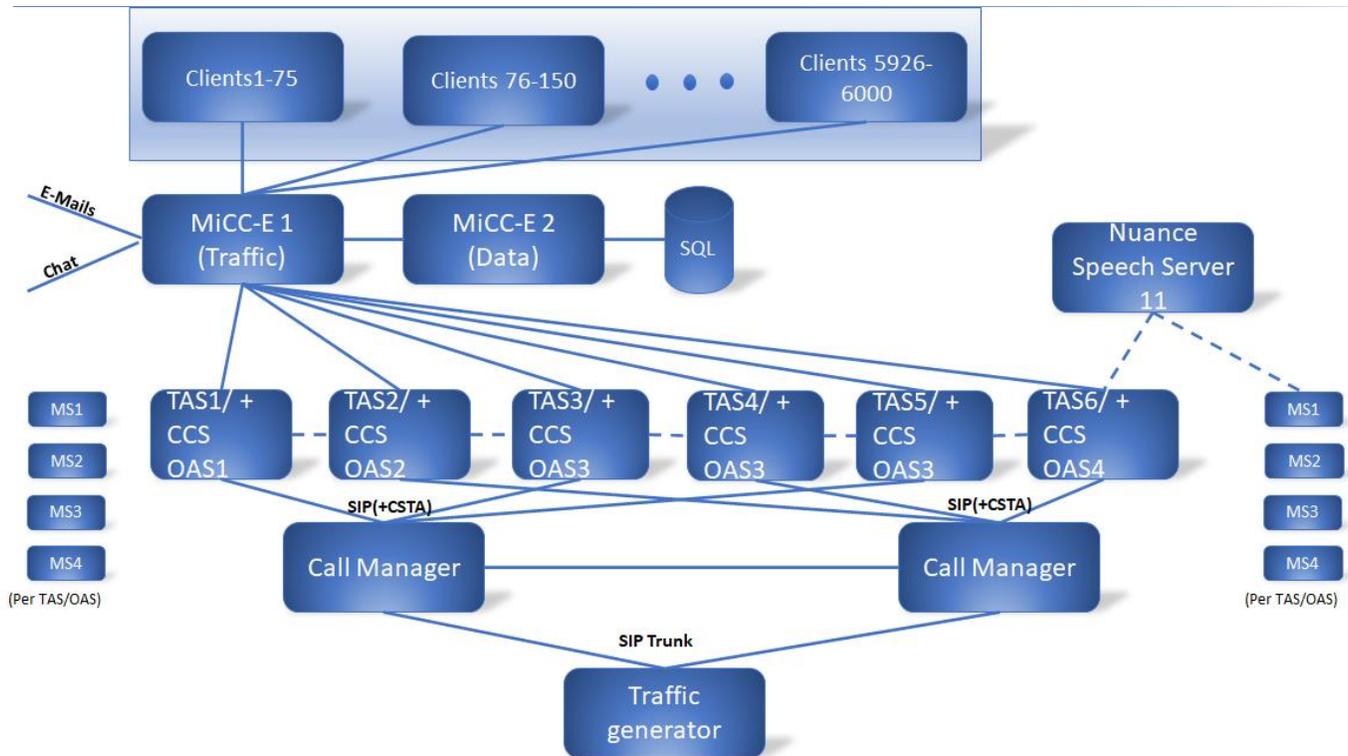
Interaction characterization

An interaction is a completed interaction between a contact center agent and a customer. A single interaction for each media type is characterized as:

- Voice – inbound only, where handling time is relative to the total interactions per hour
- Email – one email, with no attachments, with an average handling time not exceeding one hour
- Open Media – one OM session with associated screen pop URL, where handling time is relative to the total interactions per hour

Total number of interactions in both the TAS and OAS labs are a combination of Voice, E-mail and Open Media traffic reaching the maximum capacity of 60,000 completed interactions per hour sustained load.

Pass Conditions

A performance test is considered passed if the MiContact Center Enterprise Server, while under load for a minimum of 120 hours, met the following conditions:

- The application experienced no service failures, crashes, or high processor and memory usage
- Client applications were able to log in and begin service activities in less than 30 seconds
- Real-time statistics experienced no longer than a 3 second latency
- Memory usage remained below 85% during the test period
- Average CPU usage did not exceed 75% on any of the servers during the test period
- Factors excluded from performance testing that could affect system stability and overall performance are:
  - Network latency – All testing performed using virtual switches on a single VMware ESXi host
  - Network jitter and packet loss
  - Additional co-located applications including anti-virus scanners. Anti-virus SW is installed on the servers and auto-protection is enabled, but active scanning is not performed during the peak traffic test period
  - Network bandwidth

Bandwidth and Storage Requirements

This section describes requirements and considerations for bandwidth and storage when deploying a MiContact Center Enterprise system or a MiContact Center Enterprise client.

Disk Space Requirements

To successfully deploy the MiCC Enterprise Server and client desktop applications, you must ensure adequate disk space is available for the software installation and for the daily operation of all applications and services. This section describes the initial disk space requirements and provides guidance for determining your data growth over time.

The following table outlines the disk space requirements for installing the client applications and the Enterprise Server software.

Table: Disk space requirements for software installation

	Minimum required initial disk space	**Recommended Initial Disk Space**
MiCC Enterprise Server	60 GB	200 GB
Client Applications	10 GB	15 GB

Filesystem Growth

As data is collected and your contact center goes into production operation, data growth of the filesystem must be considered. It is mainly log file information that will cause continuous growth of the file system. The amount of information logged depends on which logging functions are enabled and the level of detail in the logs. The tools to control logging varies for the different components.

MiCC Enterprise Server

The number of log files to be stored before the system starts to overwrite existing log files, and the maximum size of each log file is configured in the System Properties using Configuration Manager. The default values are 5MB file size and to store 30 log files before overwriting.
The log level, which sets the level of detail that is logged, is set individually for the core services using the SecCfg registry editor. The higher log level (from 1 to 9) makes the log files fill up quicker. Mitel recommends keeping the default log level (3) unless asked by Mitel service personnel to increase the log level.

IVR, Script Manager

The log file size and the number of log files can be configured by using the Script Manager Configuration utility. The default values are to keep the last 100 log files and the log file size is set to 1024 KB. The log level can also be set for each individual component using the Script Manager Configuration utility. Mitel recommends keeping the default log levels unless asked by Mitel service personnel to make changes.

Open Application Server (OAS)

Only logging for the core component NRM is activated by default. The OAS Trace Service will write the log into a number of trace files (100 files by default).

When creating these files, the Trace Service will replace the oldest file with a new one so that the

number of trace files does not exceed the maximum number of allowed files.

The number of Trace files can be modified by changing this registry key:
HKLM\SOFTWARE\Wow6432Node\Mitel\OAS\OTS\ MaxFiles

Note: Even if the number entered in the Registry is larger than 255, the number of files will still be limited to 255 by the OAS trace service.

The file size of a complete log file is 8 MB. Mitel recommends keeping the logged components at the default settings unless directed by Mitel service personnel to make changes.

Telephone Application Server (TAS)

The log levels and maximum number of log files (one per day) for the TAS component as well as Media Server can be modified using the TASConfig utility.

The TAS logging is by default set to Trace level 3 and 14 days of logs with max log file size set to 512MB. The Media Server is also set to Trace level 3 but for 10 days of unlimited size.

Mitel recommends keeping the log settings at the default settings unless directed by Mitel service personnel to make changes.

SQL database

The MiContact Center Enterprise uses an SQL database (nextccdb) to store all configuration and activity (historical) data.

Please refer to the updated document "*Estimating Database Size*" in the user documentation library and available on the Doc Center accessible via the MiAccess portal to calculate expected database growth. The growth is dependent on expected traffic volumes and retention time, i.e., how many months or years of data expected to be available online in the nextccdb.

To be able to calculate the growth more accurately in your system the following SQL query can be run on the nextccdb database using the SQL management Console:

```
SELECT
    t.NAME AS TableName,
    s.Name AS SchemaName,
    p.rows,
    SUM(a.total_pages) * 8 AS TotalSpaceKB,
    CAST(ROUND(((SUM(a.total_pages) * 8) / 1024.00), 2) AS NUMERIC(36, 2)) AS TotalSpaceMB,
    SUM(a.used_pages) * 8 AS UsedSpaceKB,
    CAST(ROUND(((SUM(a.used_pages) * 8) / 1024.00), 2) AS NUMERIC(36, 2)) AS UsedSpaceMB,
    (SUM(a.total_pages) - SUM(a.used_pages)) * 8 AS UnusedSpaceKB,
    CAST(ROUND(((SUM(a.total_pages) - SUM(a.used_pages)) * 8) / 1024.00, 2) AS NUMERIC(36, 2)) AS UnusedSpaceMB,
    IIF(p.rows > 0,(SUM(a.total_pages) * 8) * 1024 / p.rows, 0) as RowSizeBytes
FROM
    sys.tables t
INNER JOIN
    sys.indexes i ON t.OBJECT_ID = i.object_id
INNER JOIN
    sys.partitions p ON i.object_id = p.OBJECT_ID AND i.index_id = p.index_id
INNER JOIN
    sys.allocation_units a ON p.partition_id = a.container_id
LEFT OUTER JOIN
    sys.schemas s ON t.schema_id = s.schema_id
WHERE
    t.NAME NOT LIKE 'dt%'
    AND t.is_ms_shipped = 0
    AND i.OBJECT_ID > 255
GROUP BY
```

```
        t.Name, s.Name, p.Rows
ORDER BY
    TotalSpaceMB DESC, t.Name
```

This will create a list of all tables in the nextccdb database and in the last column show the average record/row size in your system. This is useful since the record size could vary significantly between systems. Many record columns are of variable size and indexes will vary from site to site. Mitel recommends running the system in production for a while and then running the query to monitor the growth over time.

The Database Maintenance utility can be used to backup and delete activity data on a monthly basis. It can also be used to restore backed up activity data to make it available online again.

Multimedia Search Storage

The MiCC Enterprise system optionally stores detailed session history information in the SQL database. These Call Detail Records (CDRs) contain detailed, step by step, information related to voice call, e-mail, SMS, and chat activity. By default, this is not activated in the system. The user can activate storage of e-mail, SMS and chat sessions in the System Properties using Configuration Manager.

Different levels of storage can be set. For e-mails the selection of details to be stored includes:
- None (default)
- Headers Only
- Minimal Message Body
- Full Message Body
- Complete (Full Message plus attachments)

Storage levels for chat include:
- None (default)
- Text Only
- Complete (Text plus attachments)

The database maintenance utility can be used to backup and delete e-mail, SMS and chat CDR records.

Network connectivity requirements

The following table details the connections required for different server and client roles to ensure data is being sent and received correctly. These are the minimum recommended requirements. Your individual   network connectivity requirements may exceed those outlined here depending on your overall contact center traffic and use of features and applications.

Table: Network connectivity requirements

Server or client role	Required network connection
Enterprise Server	100 Mbps network connection speed is the minimum requirement

Remote Server	25 Mbps download connection speed and 10 Mbps upload connection speed are the minimum requirements for data collection only
	NOTE: The connection speed between a local call manager platform and a remote server must be a minimum of 10 Mbps
Client	2 Mbps download connection speed and 1 Mbps upload connection speed are the minimum requirements

NOTE:

For a full list of ports required for MiContact Center Enterprise, see the document "*Port Numbers, MiCC Enterprise*" available in the documentation library and on the Doc Center accessible via the MiAccess portal

MiContact Center Enterprise server should not be installed on a publicly accessible network.

MiContact Center Enterprise bandwidth requirements

The following section outlines the bandwidth requirements and recommendations on maximum latency for the MiContact Center Enterprise Server and MiContact Center Enterprise clients.

MiContact Center Enterprise Server
Bandwidth

The MiContact Center Enterprise Server requires available bandwidth to service client connectivity, service web requests and manage data streams from connected call managers, mail servers and other systems.

The minimum requirement for bandwidth for a Tier 1 type system (as specified above) is 100 mbps. For Tiers 2 and 3 type configurations 1 gigabit ethernet is required.

The tool SecCalc, which is available in the Tools folder on the media kit, can on the last tab (SeC Traffic) be used to calculate network traffic based on the number of agents and calls, taking into consideration how the system is configured (number of queues and agent groups etc.).

Network Delay

The one-way network delay on network paths listed below should typically be:

- 50 ms or less for a good user experience and little or no perceived slowness.
- 250 ms or less for an acceptable user experience, where system response is at times slow, but still functional

The delay limits apply to each of the following network paths:

- MiContact Center Agent - MiCC Enterprise Server
- MiCC Enterprise Server – OAS/TAS
- OAS/TAS - MX-ONE (or other call manager)
- Accumulated MiContact Center Agent – MiCC Enterprise Server – OAS/TAS

For VoIP media streams, the network delay must be less. For advice on VoIP requirements on the network, see the document *MX-ONE System Planning* in the latest MX-ONE documentation library.

Client applications

For client machines, it is recommended that machines have a 10 Mbps connection to support typical agent PC and MiContact Center Enterprise application usage.

The same requirements related to Network Delay as specified above apply and the SecCalc tool can be used to calculate bandwidth needs for one or several agents. This could be useful, for example, in a branch office situation where several agents are situated remotely over a WAN or VPN connection.

Other considerations

Translated languages and supported operating systems

The following table details the languages supported by MiContact Center Enterprise applications.

Table: Translated MiContact Center Enterprise applications

Language/Application	AR*	DA	DE	ES	FI*	FR*	NL*	PTB	SE	RU*	IT*	EU*
Configuration Manager	x		x	x		x		x		x	x	
Information Manager			x	x	x	x		x		x		
Report Manager			x	x	x	x		x		x		
Script Builder			x	x		x		x		x		
MiContact Center Agent	x	x	x	x	x	x	x	x	x	x	x	x
Web Manager	x		x	x	x	x	x	x	x	x	x	
Web Agent	x	x	x	x	x	x	x	x	x	x	x	

AR = Arabic, DA = Danish, DE = German, ES = Spanish, FI = Finnish, FR = French,
NL = Dutch, PTB=Brazilian Portuguese, SE=Swedish, RU=Russian, IT = Italian, EU=Basque

All applications have translated online help except for languages marked "*". Note that Configuration Manager online help is available only in English.

For an overview of supported languages in voice, automatic speech recognition and text to speech, refer to the following documents: "*ASR and TTS Overview*" and "*System Prompts*" available in the documentation library and online on the Doc Center accessible via the MiAccess portal.

Synchronized time settings in MiContact Center Enterprise

MiContact Center Enterprise relies on synchronized time and clock settings for all component computers within the system to enable accurate time-based reporting and real-time statistics. The components of MiContact Center Enterprise (such as MiCC Enterprise servers, remote servers, and client desktops) and third-party elements (such as Microsoft SQL servers and virtual machine hosts) must have accurate time settings and must be synchronized with the same time server.

CAUTION: Computers that do not have accurate time settings or are not time synchronized with other computers and systems in the configuration may yield inaccurate data and cause functionality issues within MiContact Center Enterprise applications.

Backing up Data

We highly recommend backing up MiCC Enterprise Server data on a regular basis as a preventative measure in case of events that could cause loss of data and necessitate system restoration. The frequency of backups depends on how important the data is to your business, your Recovery Time Objective (RTO), and the Recovery Point Objective (RPO). Finding the balance between the importance of data, your RTO   and RPO, and your enterprise backup and restoration strategy will strongly dictate how MiContact Center Enterprise backup and restoration integrates into your overall disaster recovery strategy.

We strongly recommend storing backup files in a location outside of the MiCC Enterprise Server in order to   maintain essential data in the case of a hardware failure or catastrophic event. Using backup software Data can be stored automatically on a UNC share or a SAN storage system.

MiCC Enterprise server

All configuration data and historical report data for the MiCC Enterprise system is stored in the SQL database. In addition to performing monthly backups of the monthly activity and configuration data using the Database Maintenance (DBMT) utility, Mitel recommends performing daily backups of the nextccdb database either using tools built into Microsoft SQL server or other 3rd party backup tools. These backups should be done during off-peak hours since they could adversely affect server performance.

If the integrated voice call recording function is used, the voice recording folder (secrecord$ share point) should also be backed up regularly. Other network shares that should be backed up regularly are Nextccreport$ and SeCGreeting$.

If the IVR (Script Manager) is used, the IVR configuration and IVR scripts should be backed up. That should be done at the same time as DBMT is run to back up the MiCC Enterprise configuration data and can also be done by backing up the ScriptManager\Config folder under the MiCC Enterprise installation path, typically <drive>:\Program Files (x86)\Mitel\MiCC Enterprise

OAS server

The OAS configuration data is stored in several repository files stored in the OcsRepository folder under the OAS installation path, typically <drive>:\Program Files (x86)\Mitel\Oas. Also, the recorded prompts stored in the root_container folder under the OAS installation path should be backed up regularly or when changes have been made.

TAS server

The TAS server and ACS Media Servers maintain configuration data in the Windows Registry. To back this up an Export of the HKLM\Software\WOW6432Node\Mitel\TAS and the HKLM\Software\WOW6432Node\Aastra\Mediaserver hives should be done. The prompt files stored on the Media Server in the folder configured as Audio Files Prefix should also be backed up.

Statement of Support for Windows Updates

We advise that you update your client/server Windows operating systems with the recommended security patches, hotfixes, and service packs in accordance with Microsoft best practices. You may install Windows Security Patches at any time and any issues pertaining to the installation of Windows Security   Patches are covered under the standard terms of the Mitel support contract. Mitel constantly tests and validates the MiContact Center Enterprise solutions against the latest versions of Microsoft operating systems that are released along with any security patches or service packs issued by Microsoft. This does not guarantee that future Microsoft patches or updates do not cause any problems; only that the risks are minimized. In the event of our encountering any issues,

Mitel informs partners and customers using standard Technical Service Bulletin and Content Hub "Recent news entries" processes and works promptly to resolve them.

Licensing

There are two separate licensing models for MiCC Enterprise. The traditional CAPEX license model and the Opex based MiCC Enterprise Subscription (MLA) model. MLA (Mitel License Agreement) model is a Opex model where billing occurs monthly based on actual usage of the system.

CAPEX

The is the traditional license mode for MiCC-E where the customer acquires perpetual licenses and in order to receive product support and the ability to upgrade the system to newer releases, Software assurance is offered. All user-based licenses are based on concurrent usage. That means a license is acquired when a licensed application is started, and the license is freed up when the application is closed. There is an option to have Agent feature licenses for email, chat, and open media to only be acquired when the Agent is made Ready to handle that type of media. The license is then freed for somebody else to use when the Agent is made Not Ready or logs off.

Starter Packs

There are two different start packs for MiCC Enterprise Capex:
- MiContact Center Enterprise MultiMedia Lite (also sometimes referred to as MiCC Enterprise SME)
- MiContact Center Enterprise MultiMedia

The main difference is that the Lite package is capped at 50 agents. The system cannot grow beyond that number. If additional agents beyond 50 required for a Lite system, then it first must be upgraded to a full Multimedia system.
Both start packages include the same amount of agent licenses (5) but with a different system version license making the initial purchase price and corresponding Software Assurance cost significantly lower for the Lite system. Another difference is that the Lite starter pack includes 4 media channel licenses whereas the MultiMedia system includes 8.

There is also an IVR start pack that can be added to any Lite or MultiMedia system. This package includes 4 IVR session and 1 Configuration Manager license.

For more detailed information related to Starter Packs refer to the "*Ordering Guide-MiContact Center Enterprise*" available on the Content Hub.

Prior to release 9.4 of MiCC Enterprise there was a 3rd Starter Pack available, MiCC Enterprise Lite Voice. This was similar to the MultiMedia Lite package in that it capped the number of agents to 50 but with the difference that these agents could only handle voice calls. No multimedia feature licenses were possible to add. MiCC Enterprise Voice systems from release 9.3 or lower that are upgraded to release 9.4 or later will automatically be converted to MiCC Enterprise MultiMedia Lite. There is no difference in cost of add-on licenses or SWA between these system types.

Agent types

There are several different types of agent licenses in the MiCC Enterprise system. The following table shows which agent applications can be used by each different license:

Agent kit	Allows you to use				
	MiCC Enterprise Agent Multimedia	MiCC Enterprise Agent Multimedia Lite	MiCC Enterprise Web Agent	MiCC Enterprise Phone Agent	Mobile Agent application **
MiCC Enterprise Agent Multimedia	Yes	N/A*	Yes	Yes	Yes
MiCC Enterprise Agent Multimedia Lite	N/A*	Yes	Yes	Yes	Yes
MiCC Enterprise Web Agent	No	No	Yes	Yes	Yes
MiCC Enterprise Phone Agent	No	No	No	Yes	Yes

* Cannot exist in same system
** Will log agent on as a
Phone Agent

MiCC Enterprise Subscription (MLA)

This model is available to partners who have signed an addendum to the Mitel partner agreement allowing them to offer this subscription service. The following start packs exist for MLA orders:

- Base package
  Includes system licenses, agent licenses (including multimedia features) and use of management applications. This package is mandatory.
- IVR package
- SMS-C package
- Progressive dialer package
- Open Media package

When ordering an MLA system, a fully open license is provided. Once the system is installed and configured it will automatically send monthly license usage information to the Mitel billing center. Based on this report the billing center will invoice the partner for maximum concurrent usage of agents, IVR ports, applications and features during the month.

For more detailed information related to MLA Starter Packs refer to the "*Ordering Information - MiCC Enterprise Managed-service License Agreement*" available on Content Hub. There is also a sales presentation published there, "*Sales Presentation - MiCC Enterprise Managed-Services License Agreement (MLA*)", that provides additional information.

Subscription based OEM licenses

The following subscription-based OEM licenses are possible to add to MiCC Enterprise systems (Capex or MLA).

- Mitel Interaction Recording (MIR)
- Calabrio WFM
- Neverfail

They can be ordered via the Contact Center OEM Apps Subscription model in CPQ.

MX-ONE SIP trunk licenses

When TAS is being used connected to MX-ONE an adequate number of SIP Trunk channel licenses must be available in MX-ONE. In the simple setup with only one TAS this is not complicated, but in a multi-TAS setup with SIP host or SIP SRV record load balancing setup in DNS this can become a bit more difficult.

Single TAS

Each incoming call to TAS requires one MX-ONE SIP trunk channel license. For each call connected to IVR or just queuing, one SIP trunk channel will be used. For active agent conversations there is a difference between agents using the Agent soft phone capability and agents using a telephone connected to the call manager (MX-ONE). Since Agent soft phones are registered in TAS they do not require any additional SIP trunk channels for their conversations. For call manager connected telephones an additional SIP trunk channel is used for incoming and outgoing service calls to and from the agent.

The formula for number of licenses is:

SIP trunk channel licenses = (Max number of queuing calls + Max number of concurrent IVR sessions) + (Number of agents using MX-ONE connected phone * 2) + Number of agents using Agent soft phone

An example: A customer expects up to 150 calls in queue plus they have 30 IVR session licenses. They have 200 agents where they expect 75 to use the MiCC Agent soft phone. The number of required SIP trunk licenses would be:

   150+30+(125*2)+75=405

Note: WebRTC connected Web Agents are registered via the MBG to MX-ONE and will thus require 2 SIP channel licenses each.

Multi-TAS with load balancing

In multi-TAS environments the calculation of required SIP Trunk channel licenses is a bit more complex. This is because in addition to having a load balanced SIP trunk that terminates in all TAS servers, each TAS server also needs its own dedicated SIP trunk which is used for calls that need to reach a specific agent logged on to a different TAS server than where the call currently is managed.

A simple common scenario here would be that a call arrives to a queue in TAS 1. MiCC Enterprise performs agent selection, and an idle agent is selected. This agent happens to be logged on to and monitored via TAS 2. The multi-TAS logic built into the system now dictates that we need to move the call in queue in TAS 1 over to TAS 2 and from TAS 2 send the call to the selected agent, i.e., the call and agent need to be managed by the same TAS server. This is where the dedicated SIP trunk comes into play. Let's look at an example system that consists of 3 TAS servers and has 300 agents. When these agents log on, the agent balancing feature of MiCC Enterprise will place 100 agents in

each TAS server. Assume load balancing of incoming calls from the call manager distributes calls evenly between these 3 TAS servers. That means there is a 2 out of 3 chance that the selected agent is located in a different TAS than the incoming call, i.e., we need 200 SIP trunk channel licenses in each dedicated SIP trunk to the 3 TAS servers.

In addition, the load balanced SIP trunk will need SIP trunk channels according to the same formula as used to calculate licenses for a single TAS system but with the difference that we should not consider any difference between agents using Agent Soft phone and agents using desk phone, i.e., calculate all agents as desk phone users.

As a rule, we can say that the dedicated SIP trunk needs channel licenses to be based on total number of agents multiplied with number of TAS servers-1 divided by number of TAS server. This means for a 300 agent system with 3 TAS servers the formula would be: 300*(2/3)=200

Statements of support

The following section includes statements of support for our applications and integrated products.

Statement of Support of Software from other vendors

The current document specifies a number of supported compatibilities between MiCC Enterprise and third-party products: operating systems, database servers, messaging servers, and many others. We would like to emphasize the fact that MiCC Enterprise continues supporting these third-party products only when their manufacturer continues supporting them. Support of MiCC Enterprise in combination with a given third-party product will stop when the manufacturer of this third-party product ends its support. The fact that a given version of MiCC Enterprise supports, at installation time, a given third-party product is thus not a guarantee that it will continue supporting it until the end of life of that MiCC Enterprise version.

NOTE:

For the Microsoft products, the end date of the "extended support" is taken into account. However, if paid services need to be requested from Microsoft (like paid support and paid hotfix support), they will be available only if the end-customer pays them. Mitel will never bear such cost.

Compatibility with other Mitel solutions

This table lists the compatibilities between MiCC Enterprise and other Mitel applications:

Mitel solution	Supported Version
Enterprise License Manager (ELM)	2.1 SP14
BluStar Web / CMG	9.1, 9.2 and 9.3
Mitel Interaction Recording (MIR)	7.3
Mitel Border Gateway	12.0, 12.1 and 12.3

Statement of support and Software Assurance for MiContact Center Enterprise software

Technical support is provided for all MiContact Center Enterprise systems that have an active SWA subscription. The level of support varies depending on the version of the system. Systems older than release 9.0 (e.g., releases 7.0 and 8.x) have been formally phased out and have reached End of Life. These systems will be supported on a best effort basis with the objective to bring the system back to service. MiCC Enterprise release 9.x systems lower than the current release (9.8) are provided full support and critical faults can be escalated in order to receive a hot fix. The only difference is that non-critical faults are only corrected in the next service pack or fix pack for release 9.8 or next release (9.9 and/or release 10.0) whichever comes first, and customers should upgrade to the current (actively sustained) release in order to take the benefit of all fault corrections.

A mandatory, minimum one year Software Assurance subscription must be purchased with all new MiContact Center Enterprise system sales. If you optionally purchase 3 years of Software Assurance at the same time, you are entitled to a 7% discount and a 10% discount if you opt for 5 years.
If you have less than one year remaining in your Software Assurance plan and purchase add-on products,   additional Software Assurance for your add-on products will not be required until the renewal date for your MiContact Center Enterprise software system.

If you have more than one year remaining in your Software Assurance plan and purchase add-on products, you will be required to purchase additional Software Assurance for your add-on products so that your   expiry aligns with the expiry of your MiContact Center Enterprise software system.

You have a 30-day grace period after your system expiry during which you can renew your Software Assurance package without incurring a re-enlist fee. The purchased subscription is retroactive to the original expiry date. Software Assurance entitlements are not extended during the grace period if there is no   active subscription. After 30 days you will be required to pay a re-enlist fee equal to the value of one year   of Standard Software Assurance coverage for your system.

You can either use the Mitel Configure Price Quote (CPQ) tool to calculate annual years of Software Assurance or email to miccrenewal@mitel.com for a renewal quote.

Supported browsers

The following browser versions were verified as supported with MiContact Center Enterprise Version 9.8 applications:
- Google Chrome (Version 126 or higher)
- Microsoft Edge (Version 126 or higher)
- Mozilla Firefox (Version 126 or higher)
- Safari (Version 12 or higher)

NOTE:
- Web Agent using SoftPhone in WebRTC mode is supported on the Chrome and Edge browsers.
- Mitel constantly makes best efforts to test and validate the latest versions of all supported browsers. The recommendations given here are not for the versions you must be running, but for the minimum version of the browsers required for MiContact Center Enterprise to function.
- Modern browsers are updated frequently and often without user interaction. As a result, deployed versions of these browsers may be newer than the versions that were tested prior to the release of MiContact Center Enterprise Version 9.8. Web applications should continue to function through all browser updates. If an update released by a browser manufacturer causes

adverse behavior, Mitel will make every effort to resolve the issue as per support and service level agreements.

- Due to Microsoft's statement of end of life for Internet Explorer 11 as of June 15, 2022 users should use Microsoft Edge or other supported Web browsers like Chrome, Firefox, or Safari.

Supported Telephone Systems

The following table lists telephone systems that are supported for MiContact Center Enterprise Version 9.8:

Table: Supported telephone systems

Telephone System	Supported Version
MiVoice MX-ONE (with OAS or TAS)	7.7 SP1, 7.8 SP1 and 8.0
Cisco UCM (with TAS)	11.5, 12.5
Telepo (with TAS)	5.1

The latest MX-ONE hotfix should be installed.

Supported Phones

MiCC Enterprise agents can use either the MiCC Agent in soft phone mode or any telephone connected to the call manager. For MX-ONE that means any desk phone (except ISDN terminals), DECT/SIP DECT and remote/mobile extensions can be used. For Cisco and Telepo any phone connected to these call managers can be used.

Please note that, depending on the type of terminal, certain features might be limited in CTI mode:

- For some terminals, calls cannot be answered from the MiCC Agent client. They have to be answered from the terminal itself.
- The same applies in some cases for hanging up calls.
- When making a call from MiCC Agent, the user can first be prompted to lift the handset of the terminal before the outgoing call is actually placed.
- Intrusion features (Assist and Monitor) can be restricted depending on the terminal used by the supervisor.
- DTMF digits cannot be sent by MiCC Center Agent when used in combination with some types of terminals
- Typical types of terminals having some of these limitations are: cordless DECT, analog, remote/mobile extensions, and third-party SIP terminals.

The SIP desk phone families of 6800 and 6900 are supported by MiCC Enterprise. Older models in the 6700 family are no longer supported by MX-ONE and are known to have incompatibility issues with SIP components in MiCC Enterprise.

When using the XML application for ACD available for selected SIP telephone sets registered in MX-ONE, the following sets are tested and supported: 6867i, 6869i, 6873i, 6920, 6930 and 6940.

For more information on this feature refer to "*Mitel MiContact Center Enterprise ACD User Guide*" in the user documentation library and available on the Doc Center accessible via the MiAccess portal.

Audio Codec Support

When a call is connected to MiContact Center Enterprise, the system performs codec negotiation to determine which audio codec to use. There are different components in a MiCC Enterprise system that use codecs, Open Application Server (OAS), Telephony Application Server (TAS) and the soft phone embedded in the MiCC Agent application.

Open Application Server

OAS use SIP extensions in MX-ONE to provide media services to the contact center.
The following codecs are supported by OAS:
- PCMA (G711.A (aLaw))
- PCMU (G711.U (uLaw))
- GSM (amr_nb)

Mitel recommends that G711.A or U is used.

Telephony Application Server (TAS)

TAS uses the ACS Media Server to provide media services to the contact center.
The following codecs are supported by TAS/ACS Media Server:
- PCMA (G711.A (aLaw))
- PCMU (G711.U (uLaw))
- G722.g (wide band)
- G729
- RFC 2833 (for in-band DTMF detection)

Mitel recommends that G711.A or U is used, especially if Nuance Speech Server is used.

MiCC Agent soft phone

The embedded softphone in the MiCC Agent application supports the following codecs:
- PCMA (G711.A (aLaw))
- PCMU (G711.U (uLaw))
- G722
- G729a/b
- G.723
- iLBC
- speex

Statement of support for virtualization

CAUTION: Any virtualization maintenance, such as snap shots, copying large files, and updates on the host server can affect guest image performance and availability.

MiContact Center Enterprise server applications are supported in virtualized environments. Product testing has been limited to VMWare ESXi,Nutanix AHV, Microsoft Hyper-V, Proxmox and Azure.

MiContact Center Enterprise application hardware and software recommendations do not change when running the Enterprise Server in a virtualized environment.

We highly recommend you use dedicated resourcing. If you use shared resourcing, please ensure that you have sufficient dedicated resources to run our software according to the hardware specifications as described in this guide. See *"Server hardware requirements"*.

Virtual host server requirements must be equal to or greater than the sum of all virtual machines that will run concurrently. Applications running on the host virtual machine as well as other virtual machines configured on the host can affect the functionality of the MiContact Center Enterprise software. Please refer to your Hyper-V, Nutanix, Proxmox and VMware documentation for specific hardware requirements.

Should Mitel service or engineering suspect that the virtualization layer/software is the root cause of

a problem, the customer may be required to install the software on a non-virtualized server to determine if the problem still exists. Contact the appropriate vendor to resolve the virtualization layer/software problem

Virtualization models

Virtualization is a method of partitioning a single physical computer (known as the virtual host) into multiple 'virtual' computers (known as virtual machines), giving each the appearance and capabilities of running its own dedicated machine. Each virtual machine functions as a full-fledged computer and can be independently controlled. The layer that controls these virtual machines is known as the hypervisor. The types of hypervisors are shown in the following figure.

Figure: Types of hypervisors

TYPE 1
native
(bare metal)
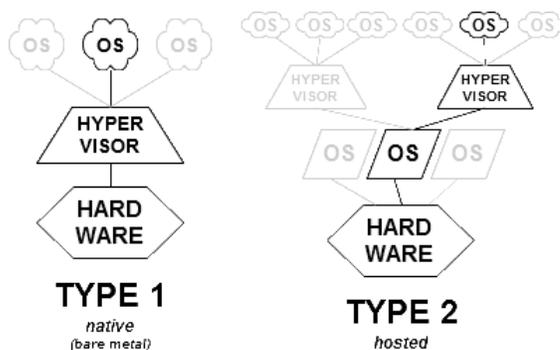
TYPE 2
hosted

There are two main types of hypervisors. Type 1 hypervisors, also known as native or 'bare metal' hypervisors, run directly on the hardware of the virtual host, whereas type 2 hypervisors (hosted hypervisors) run on the operating system layer. Type 1 hypervisors include Microsoft Hyper-V, VMware ESX/ESXi, Nutanix AHV,and Citrix Hypervisor. Type 2 hypervisors include VMWare Workstation, Microsoft Virtual Server and Microsoft Virtual PC.

MiCC Enterprise servers used in production, including TAS and OAS) are only supported when running on Type 1 (bare metal) hypervisors. Moreover, only VMware ESXi, Nutanix AHV and MS Hyper-V have been validated by Mitel.

Statement of support for remote agents

Remote agents require network access from their client machines to the MiContact Center Enterprise Server to ensure full-feature functionality. Each client machine must be able to communicate with the MiCC Enterprise Server as though it were on the corporate network regardless of the physical location or available network access for that client. Typically, this is achieved using Virtual Private Network (VPN) infrastructure providers, such as Juniper Networks, F5 Networks, SonicWall, or Cisco, or using network access technologies, such as Microsoft DirectAccess. When leveraging VPN or network access technologies, communication between the client and the MiCC Enterprise Server is accomplished by configuring connectivity over the MiContact Center Enterprise ports. Information about which ports are used can be found in the document "*Port Numbers, MiCC Enterprise*" available in the documentation library and on the Doc Center accessible via the MiAccess portal.

Support for agents working remotely over VPN and network access technologies is considered best effort and, at any time as an appropriate troubleshooting step, Mitel may require the client to be connected directly to the network to eliminate remote access infrastructure as the cause of unexpected behavior.
For additional information on configuring, supporting, maintaining, and testing VPN and network access technologies please refer to the appropriate vendor or manufacturer's documentation.

Statement of support MiCC Enterprise Multimedia
Mail Server Support

NOTE: Email routing to blind-copied queues is not supported.

Office365
MiCC Enterprises 9.8 uses the Microsoft Graph API and OAuth2.0 when configured to connect to Office365.

Other E-Mail Services
MiCC Enterprise 9.8 uses direct IMAP/SMTP integration towards other e-mail servers than Office365. Any messaging servers supporting the IMAP4 and SMTP protocols may be used, for example Gmail, MS Exchange etc. The messaging servers must support basic authentication using username/password. Oauth is not supported. For Gmail and Yahoo based email services, you can generate an app password for the master account and use that when configuring IMAP and SMTP in the MiCC Enterprise settings.

Providing access to customer Chat and other Web Applications over Internet

MiContact Center Enterprise Chat and other web applications are provided by web services running on IIS on the MiCC Enterprise server, or if so wanted/needed these web services can be deployed on a separate IIS in the DMZ. The following figures show different deployment methods.

VPN
In a VPN-based configuration, mobile users establish a VPN connection to the LAN in which their device is thus temporarily included.

VPN Server

IIS
MiCC Enterprise
services
Web Apps
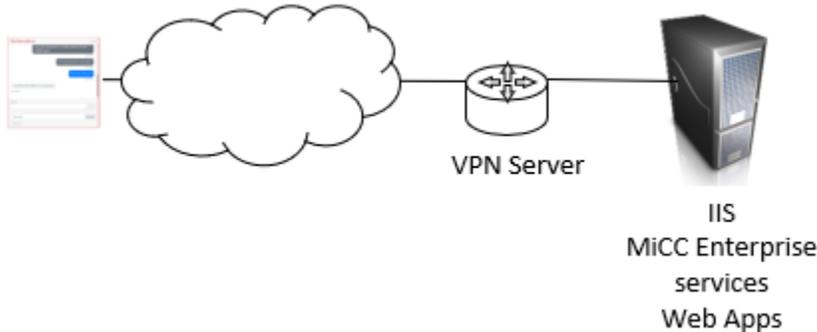
MiCC Enterprise Web Services in DMZ

Company servers accessible from the internet are generally grouped in a DMZ area isolated from the LAN. By installing the MiCC Enterprise web services on a server in the DMZ, they can be reached from mobile devices.
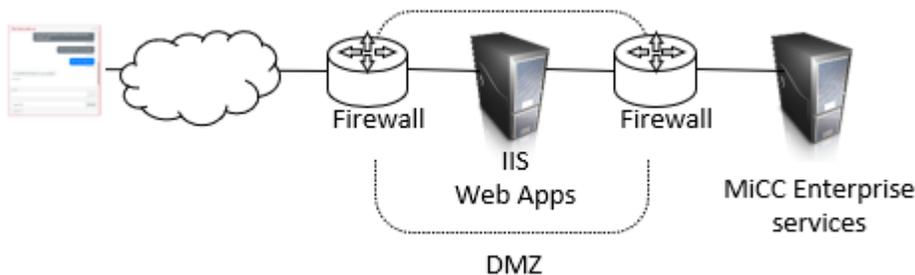

In this architecture, however, multiple connections must be allowed between this server and the other MiCC Enterprise server(s) located in the LAN.

Reverse Proxy in DMZ

It is possible to avoid making MiCC Enterprise web services directly accessible from the internet and to minimize the number of connections between the DMZ and MiCC Enterprise servers by using a **reverse proxy**.

Located in the DMZ, the reverse proxy acts as an intermediary component between client devices and MiCC Enterprise web services. HTTP is the only protocol that needs to be allowed between the DMZ and the LAN.
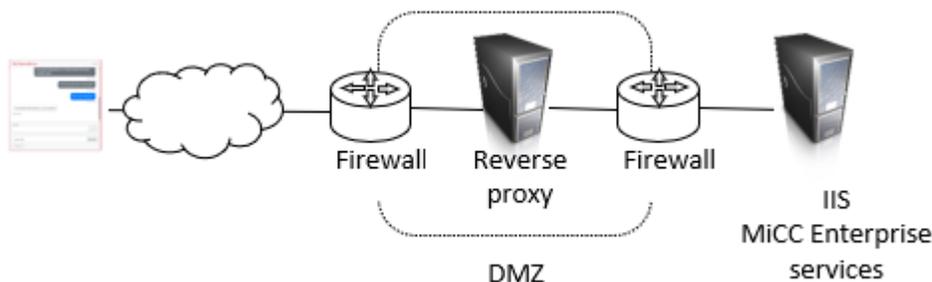
In addition to forwarding client requests and returning server responses, the reverse proxy may also provide additional functionality.
- **URL rewriting**, allowing the web apps to be accessed from another URL than the default one.
- **SSL offloading**, forwarding HTTPS requests over HTTP to the MiCC Enterprise web services.
- **Caching** of static resources such as HTML, JavaScript, and CSS files.

As an independent system, the reverse proxy is not limited to Microsoft Internet Information Server. Other software packages and operating systems can be chosen such as Nginx or Apache on Linux.

SMS service support

The SMS Gateway service integrates with 3rd part SMS service providers using the standard SMPP protocol. SMPP versions 3, 4 and 5 are supported.

Spellchecker support

MiContact Center Enterprise contains support for spell checking when agent replies to E-mails, SMSs, or types a response to a chat message. By default, the English spelling dictionary is loaded into the system. Additional language dictionaries may be installed by placing the language dictionaries on the MiCC Enterprise server. Language dictionaries must be in Open Office format and a good place to download from is at http://extensions.openoffice.org/.

For details how to install additional dictionaries please refer to "*Email Configuration – Operating Instructions*" available in the user documentation library and available on the Doc Center accessible via the MiAccess portal.