Mitel Open Integration Gateway

ENGINEERING GUIDELINES

Release 4.2 SP4

May 2023

Mitel®

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.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

TRADEMARKS

Mitel Open Integration Gateway

Engineering Guidelines
Release 4.2 SP4

May 2023

About this Document

Overview

These guidelines are provided to help integrate Mitel® Open Integration Gateway (Mitel OIG) solutions into a customer system, including OIG-based MiVoice Integration applications. These guidelines are intended to highlight specific areas of the Mitel OIG that need to be considered. These guidelines will evolve as product improvements are made, and as new services become available. Also, field experience is used to highlight specific areas that might not have previously been covered. Therefore, these guidelines should not be considered as a comprehensive list, but as useful information that should be considered.

The information in this guide is focused on system configuration information, application deployment considerations, and performance data relating to Mitel OIG and Mitel products (MiVoice Businesses and applications).

Configuration

This information relates to the setup of a Mitel OIG and MiVoice Business system. For example, this section includes supported system configurations, hardware requirements and software requirements.

Design

This information relates to Mitel OIG services. For example, when making a call from a phone, a MiVoice Business call status event is generated. An application can poll the Mitel OIG for the event or receive the event asynchronously through an application event handler.

When the system is integrated with MiContact Center Business, the call status events come from MiContact Center.

Performance

This information relates to the impact of the Mitel OIG on a MiVoice Business system under different operating conditions. For example, number of applications that can communicate with one Mitel OIG.

Overall

The content of this document is intended to gather general Mitel OIG engineering guidelines. Where the guidelines are specific to a service or a use of a product, this document may refer to other documents that can provide more details.

Audience

Engineering Guidelines help MSA Developers, Mitel Sales, Mitel Marketing, and Mitel Dealers to properly define supported system configurations involving applications that use the Mitel OIG. These Engineering Guidelines are also valuable to Mitel MSA support and Mitel Product Support.

Scope

This document addresses Mitel OIG communication with MiVoice Business controllers. The data in this document was derived using the following platforms and software loads:

Table 1: Software release line-up for this guide

MITEL PLATFORM	SOFTWARE RELEASE
Mitel Open Integration Gateway	Release 4.2 SP4
MiVoice Business	Release 10.0 SP1
MiVoice Border Gateway (Proxy)	Release 11.5 SP1
MiContact Center Server	Release 9.4
MiVoice Integration for Google	Release 1.3.4.0
MiVoice Integration for Salesforce	Release 2.5.52.0

Mitel Solutions Alliance Web Portals

Mitel Solutions Alliance (MSA) web portal (InfoChannel MSA) is accessed through the Mitel MiAccess portal (miaccess.mitel.com). As part of MSA enrollment, all authorized users under the MSA membership receive MiAccess credentials. Authorized users who experience problems accessing the MiAccess portal should request assistance by opening a support ticket at miaccess.support@mitel.com

MSA account credentials must remain active to access MSA resources. User credentials remain the same each year, and even for users who have other kinds of Mitel credentials these MSA credentials are the only ones enabling access to MSA-specific resources. Note that MSA credentials are automatically deactivated after three months of inactivity, so it's important to log on to the MiAccess portal at least once every three months. If you discover that your credentials have been deactivated, contact MSAInfo@mitel.com.
MSA credentials cannot be shared. Every person within an MSA member organization who needs access to the MSA web portals must obtain their own set of credentials associated with the company MSA membership and with their individual unique company email address (i.e., generic or distribution emails such as "support@mycompany.com" cannot be used). Additional users from an MSA member organization can obtain their own credentials by contacting https://www.mitel.com/developer/join-msa.

Technical Information

MiAccess and InfoChannel MSA are the primary points of access to most MSA developer resources, including most APIs and SDKs, interface descriptions, API and related technical documentation, and most product documentation.

To access the InfoChannel MSA portal:

- Log in to MiAccess either by clicking **Login** at the top right of the page at www.mitel.com, or directly at https://miaccess.mitel.com/.
- Click **InfoChannel** in the left sidebar.
- Select Mitel Solutions Alliance

Technical Assistance

MSA Developer Support is available to all current members of the MSA program in good standing who have sufficient Developer Support Tech Credits available. Members engage MSA Developer Support for assistance via the TechCentral Tracker for MSA web-based ticketing system.

TechCentral Tracker (TCT) for MSA is an incident management web portal for MSA members that is used to report a problem and supply full problem information to MSA Developer Support. MSA members can use the TCT-for-MSA web portal to create, modify, track and close Developer Support incidents, and to add log files and other supporting attachments to new or existing incidents.

Developer access to TCT-for-MSA requires an active MSA Membership with non-zero Tech Credit balance, active MiAccess credentials, and a valid MSA Developer TechID. Note that MiAccess and TechID credentials are all unique to an individual user and cannot be shared.

Additional users from an MSA member organization can obtain their own credentials by contacting MSAInfo@mitel.com.

The TechCentral Tracker and the *TCT User Guide for MSA Developers* are available on the InfoChannel MSA web portal to aid in incident creation and management.

Contact TSN@Mitel.com with questions regarding access to, or use of, the Tech Tracker for MSA portal.

Contact MSAInfo@mitel.com to order additional Developer Support Tech Credits.

Other Assistance

General questions regarding the MSA program and MSA membership, and inquiries or other issues that are not related to APIs, API documentation, or technical issues with developer lab equipment, can be directed to MSAInfo@Mitel.com.

Mitel OIG Overview

The Mitel Open Integration Gateway is a software solution that runs on industry standard hardware. The Mitel OIG software (OIG Base Packages or MiVoice Integrations Base Packages) requires the Mitel Standard Linux (MSL) operating system. The Mitel OIG software can be installed from the MSL server manager blades panel. The MSL administration interface allows a user to download and install the Mitel OIG software from the Mitel AMC server or a Mitel OIG OVA file can be downloaded from the Mitel Software Download Center portal and installed in a virtualized environment. See the *Mitel OIG Installation and Maintenance Guide* for more details.

The Mitel OIG offers web services to applications. For detailed information about services and how an application communicates with a Mitel OIG, see the Mitel OIG Developer Guides.

> **Note:** In the OIG guides, the term “MiVoice call manager” or “MiVoice call controller” is used to refer to MiVoice Business.

Mitel OIG System Configurations

This section considers the following:

- MiVoice Business system
- Internet access
- Connection limits
- Deployments
- MiVoice Integration applications performance
- Integration with MiContact Center

A typical Mitel OIG system has one Mitel OIG installed on a Mitel MSL server. Several applications use the one Mitel OIG to access services offered by several MiVoice Business controllers in one system cluster (See Figure 1).

The Mitel OIG can also be installed in a virtual operating system environment; so many instances of the Mitel OIG can be installed on one hardware server.

More than one Mitel OIG Is required only for system configurations requiring:

- More than 250 MiVoice Business call managers
- More than 1500 applications or application instances
- More than one MiVoice Business system cluster
- More than 90,000 CPH

Or

- More than 1500 hot desk or ACD hot desk users (in a MiContact Center installation)

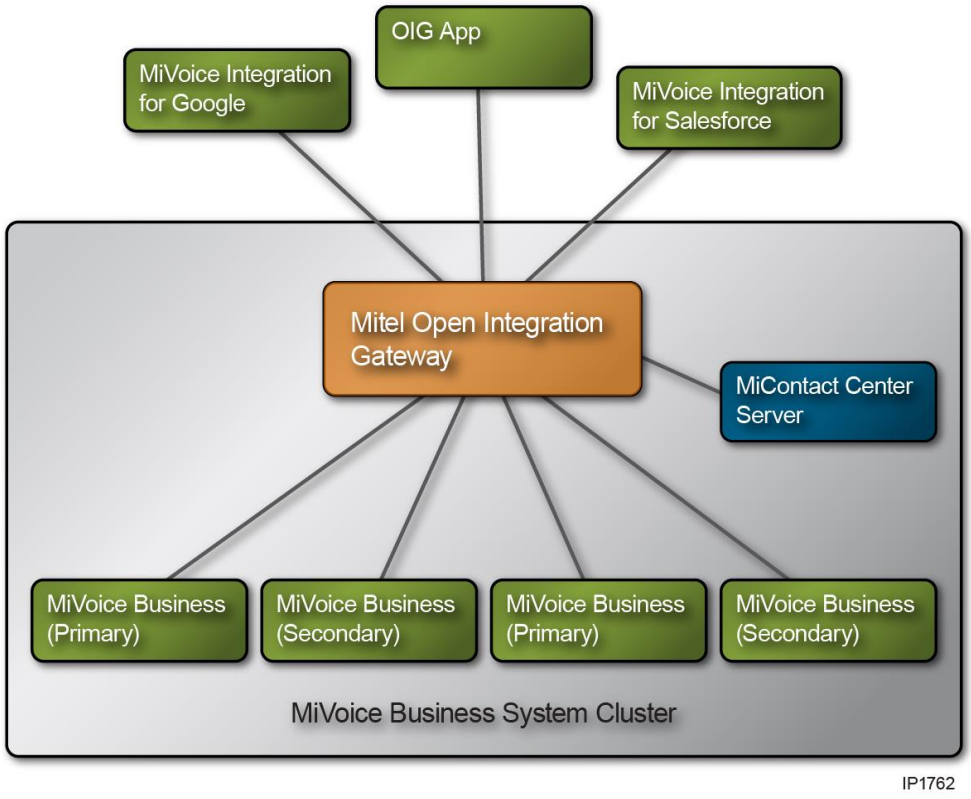
The Mitel OIG must be added to the MiVoice Business SDS sharing network if:

- An application uses Mitel OIG Data Access Service.
- A customer plans to use the MiVoice Integration for Google application.
- A customer plans to use the MiVoice Integration for Salesforce application, with or without being integrated with MiContact Center.
- Mitel OIG is required to support MiVoice Business controller IP phone resiliency.

MiVoice Call Manager System

- The Mitel OIG can communicate with a single MiVoice Business or a cluster of MiVoice Business controllers. When there are two or more MiVoice Business controllers, the MiVoice Businesses must be configured in a cluster.
- The Mitel OIG server must be configured for SDS sharing with the MiVoice Business controller or cluster, and an SDS Sync must be performed.
- The Mitel OIG cannot communicate with more than one MiVoice call manager cluster (See Figure 1).

Figure 1: Mitel OIG with MiVoice Business system cluster



Note: One OIG Server instance can sync with one MiVB or one MiVB cluster only. Once Mitel OIG Sever is added and synced to a MiVB or MiVB cluster, a different MiVB or MiVB cluster (with a different Network Element name) cannot be synced with the same OIG Server.

Supported Mitel Call Manager Platforms

The Mitel OIG supports the following Mitel call manager platforms:

- MiVoice Business on dedicated hardware controllers:
    - MXe III and MXE III-L Controller
    - CX II Controller
    - CXi II Controller
    - EX Controller
    - AX Controller
    - SMB Controller
- MiVoice Business for Industry Standard Servers
- MiVoice Business Virtual
- MiVoice Business on Public Cloud
    - AWS
    - Azure

Refer to the MiVoice Business documentation for a description of the various platforms.

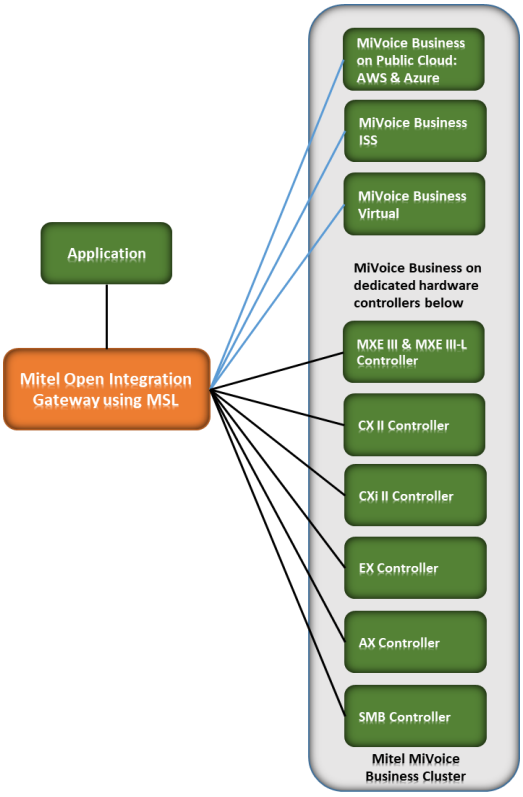


Figure 5: Mitel OIG uses various MiVoice Business Platforms

Remote OIG applications

A MiVoice Border Gateway web proxy (Release 11.4 SP1 and up) is required for any Mitel OIG application instances (users) that are deployed outside the enterprise.

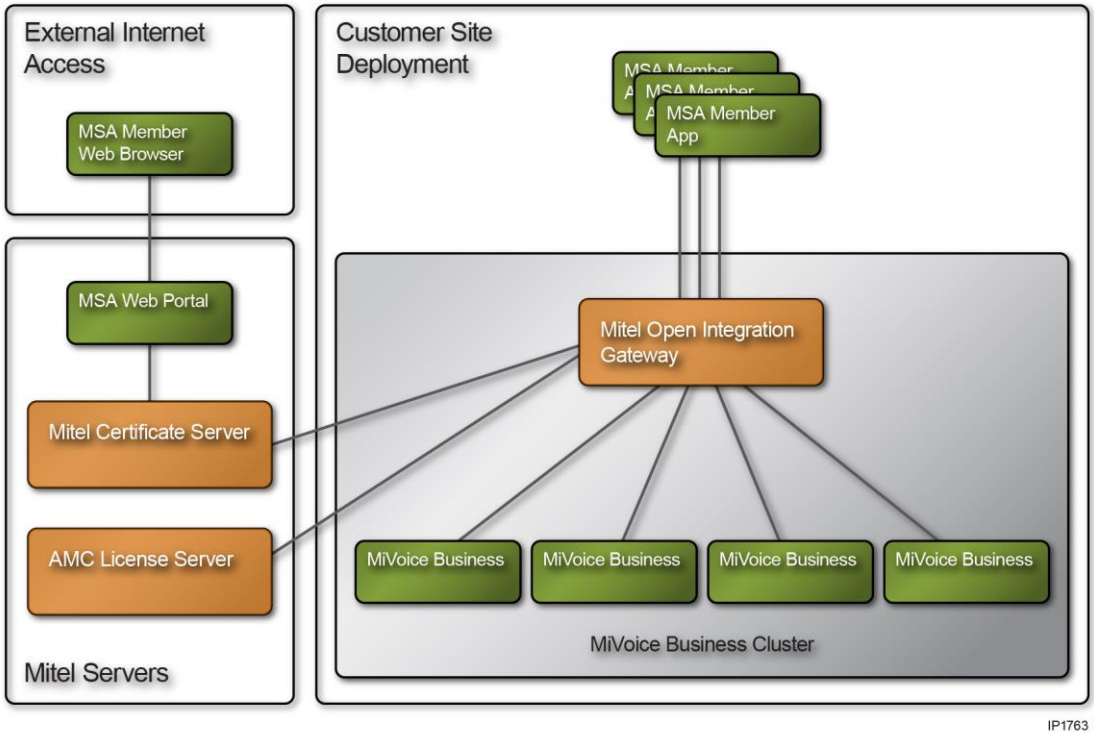
MSL Server firewall configuration

To allow the Mitel OIG to communicate with MiVoice Business controllers, the Mitel MSL server firewall must be configured to allow connections from each MiVoice Business IP address.

Internet Access

- The Mitel OIG must have access to the Internet.
- The Mitel OIG server must be configured with a third-party CA certificate when using MiVoice Integrations.
- The Mitel OIG must obtain licensing from the Mitel AMC server.
- The Mitel OIG must communicate with the Mitel Certificate Server to obtain an Access Control List (ACL).
- The ACL indicates what applications are authorized to use the Mitel OIG (See Figure 2).

Figure 2: Mitel OIG requires Internet access to MCS and AMC



Connection Limits

- The Mitel OIG can communicate with up to 1500 different applications or application instances (this includes MiVoice Integrations). The Mitel OIG supports a maximum of 1500 total applications or application instances.

This limit relates to communication sessions between the Mitel OIG server and an application. Each time an application successfully opens a communication session with a Mitel OIG, this counts toward the limit as one of the 1500 instances.

- The Mitel OIG can communicate with up to 250 MiVoice Business controllers.
- One MiVoice Business can communicate with up to six Mitel OIGs.
- Mitel OIG does not restrict the number of Mitel OIGs an application can connect to.
- The number of times a Mitel OIG application (communicating with a Mitel OIG server) is deployed at different sites is unlimited.
- One Mitel OIG can host up to 1500 instances of MiVoice Integration (one user per application)
- One Mitel OIG connects to one MiContact Center server when MiVoice Business is also in the system.

MiVoice Integration for Salesforce

- MiContact Center: supports a maximum of 1500 hot desk ACD agents.
- General Business: supports maximum of 1500 users

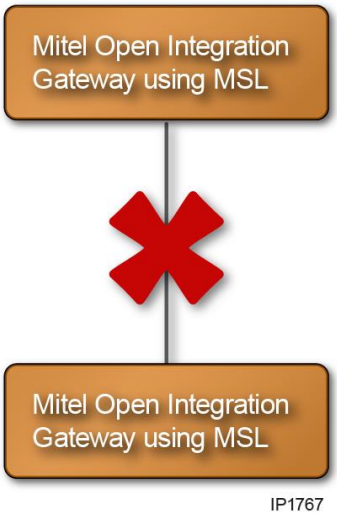
Mitel OIG Deployments

- The Mitel OIG cannot be deployed in an enterprise DMZ.
- The Mitel OIG does not provide firewall protection.
- The Mitel OIG cannot be deployed with the Mitel MSL server in gateway mode (on network edge).
- The Mitel OIG must not be deployed on the Internet without additional firewall protection.
- The Mitel OIG has been tested with the Mitel MBG; it is used to provide the web proxy feature. Thus, the Mitel MBG will web proxy HTTPS requests to the Mitel OIG server within the enterprise. When using the web proxy feature, the MBG and OIG servers must be configured with a third-party CA certificate. Refer to the Mitel MSL server on-line help related to certificate management for specific details about configuring Mitel OIG with a third-party CA certificate. A separate MSL server is needed to deploy MBG when the MBG is offering the web proxy feature.
- With MBG 11.4 SP1 and above, all OIG Services are supported across MBG Web Proxy.
- The Mitel OIG must be deployed within an enterprise.
- The Mitel OIG must be on the same LAN as the MiVoice call manager or MiVoice call manager system cluster.
- The Mitel OIG can use a VPN connection to communicate with a MiVoice call manager.
- Applications can use a VPN connection to communicate with a Mitel OIG (See Figure 3).
- When considering deployments that will use VPN, lab testing is recommended to confirm behavior.
- Two or more Mitel OIGs can be in the same LAN or virtual LAN (See Figure 4).
- Mitel OIGs do not communicate with each other.
- The number of times a Mitel OIG application (communicating with a Mitel OIG server) is deployed at different sites is unlimited.

Mitel OIG on Mitel Standard Linux (MSL)

- Mitel OIGs cannot be connected (i.e., Mitel OIGs do not communicate with each other).
- Each Mitel OIG is a standalone server (See Figure 6). Multiple instances of OIG Virtual can be installed on one hardware server in a virtualized environment. Also see the capacity graphs of OIG Virtual vs. RAM, and OIG Virtual vs. CPU usage, below.
- The Mitel OIG cannot be installed / co-resident with other MSL-based applications.
- Mitel OIG Blade can be installed on MSL deployed on Azure or AWS Cloud.

Figure 3: Mitel OIG to Mitel OIG not supported



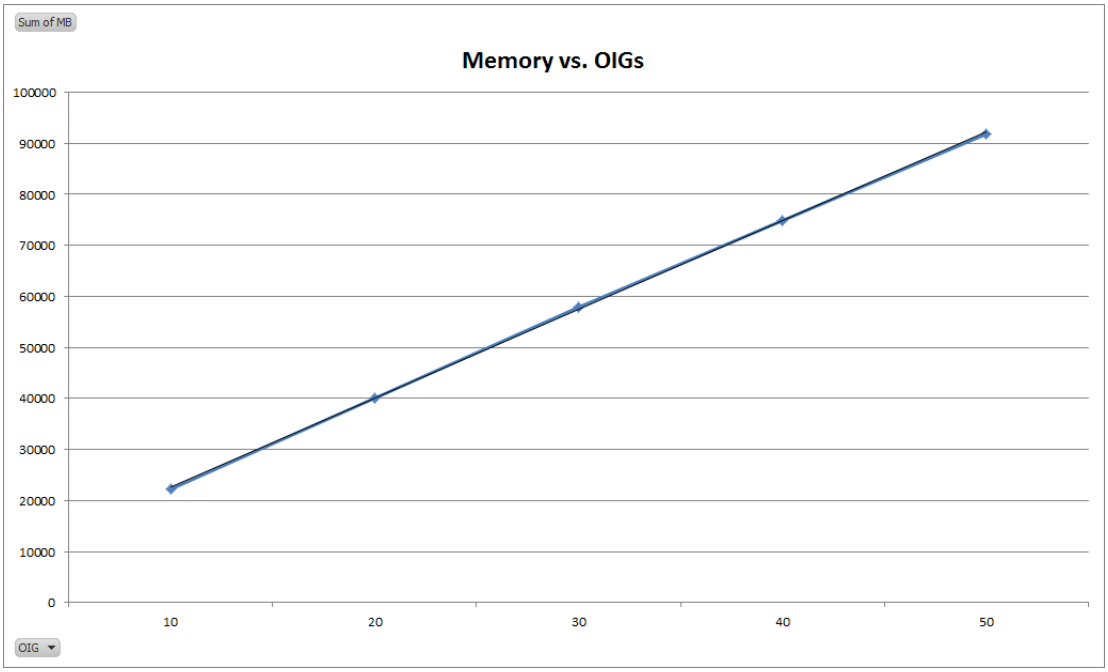
MiVoice Integration Applications Performance

The Mitel OIG software can be installed in a VMware virtualized environment (Microsoft Hyper-V is also supported) or in a Cloud Deployment (AWS and Azure are supported). Several instances of Mitel OIG can be installed on the same physical server with a virtual operating system. The following charts indicate the number of Mitel OIG instances that have been tested at Mitel on the following hardware. The testing was limited to using two Mitel applications; MiVoice Integration for Google and MiVoice Integration for Salesforce. The testing used 10 calls per hour per application. Mitel recommends that lab testing be done with applications that are expected to support such configurations when using Mitel OIG instances in a virtualized environment.

Server Specifications

SPECIFICATION	VALUE
Speed (GHz)	2.0
Processors	12
Total GHz available	24
Total Memory Available	192
Hyperthreading	Yes

The figure below indicates the amount of RAM used against the number of virtual OIG instances.



The figure below indicates the percentage of CPU usage against the number of OIG instances.

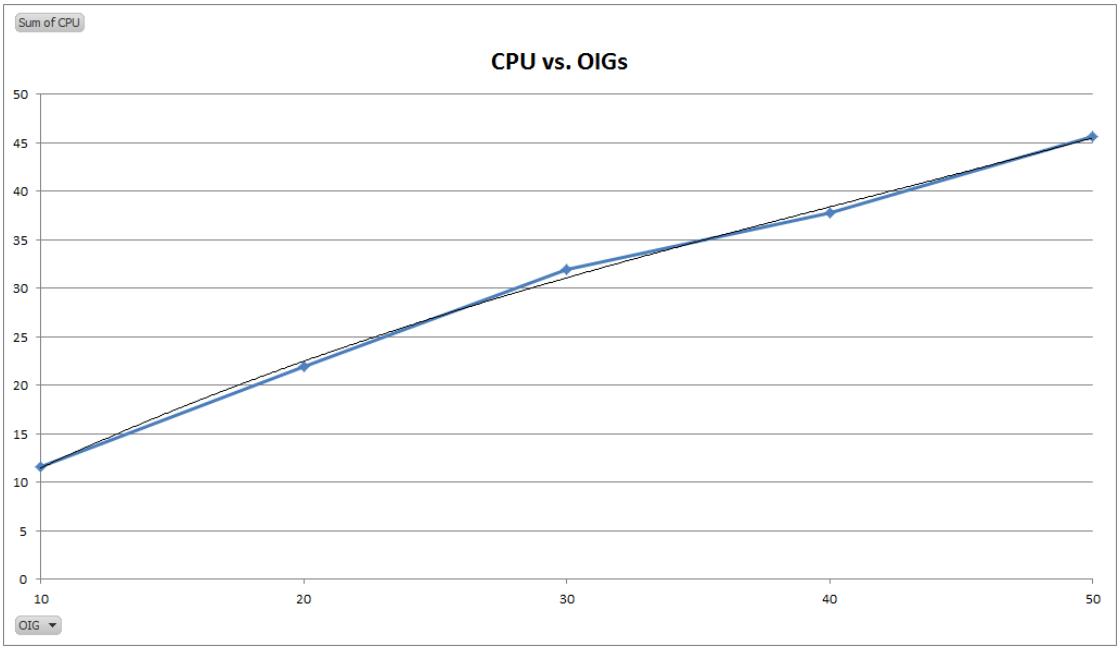


Figure 4: Applications over VPN

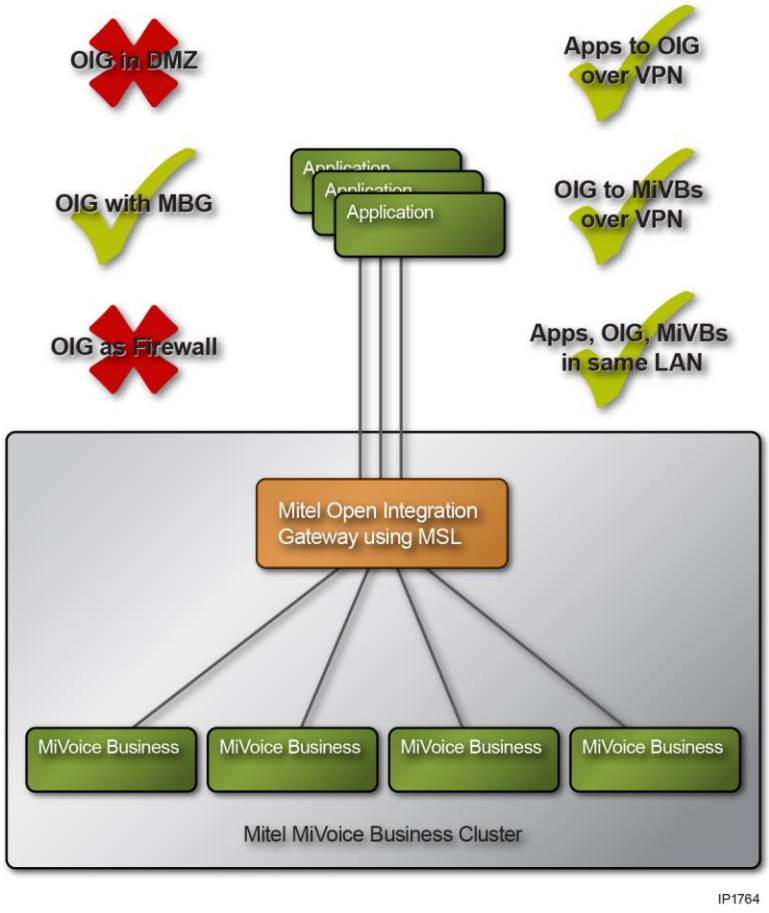
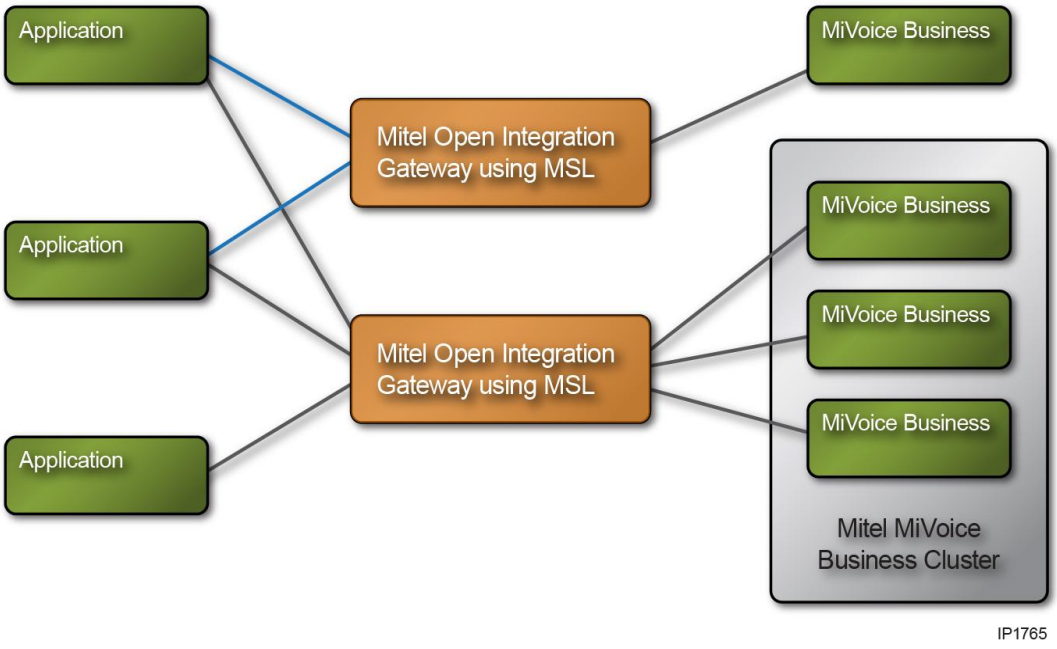


Figure 5: Applications using two Mitel OIGs



Remote MiVoice Integration applications

A MiVoice Border Gateway web proxy is required for any MiVoice Integration application instances (users) that are deployed outside the enterprise. This is true of other OIG applications as well. Recommended version with OIG 4.2 SP4 is MBG 11.5 SP1.

Mitel OIG connected with MiContact Center 9.4

- MiContact Center: supports a maximum of 1200 hot desk ACD agents.
- The Mitel OIG will act as a web proxy for any MiContact Center operations required by the Salesforce application.

Configuration considerations for MiVoice Integration for Salesforce

The following conditions define MiVoice Integration for Salesforce users' access to Make Busy and Do Not Disturb (DND) features:

- Hot desk ACD Agents can use Make Busy features.
- Hot desk users and Hot Desk Agents can set Do Not Disturb.
- MiVoice Integration for Salesforce (through Mitel OIG) sends Make Busy codes to the MiVoice Business controller.

For MiVoice Integration for Salesforce to use account codes and classification codes correctly, the following conditions must be true:

- MiContact Center is configured with account codes and classification codes.
- The classification codes are mapped to ACD paths. For example, a call to an ACD path requires a classification code for a specific hot desk ACD agent.
- Mitel OIG does not store MiContact Center codes. When needed, the Mitel OIG requests specific codes from the MiContact Center.
- Hot desk ACD Agents can use classification codes.
- MiVoice Integration for Salesforce (through Mitel OIG) sends classification codes back to MiContact Center but not to the MiVoice Business controller.
- MiVoice Integration for Salesforce (through Mitel OIG) sends account codes to the MiVoice Business controller.

Configuration considerations for E.164

The OIG Admin provides an interface to set the following E.164 values for a MiVoice Business Network Element. The custom E.164 values are applicable for MiVoice Integration Salesforce and MiVoice Google Integration only.

- Outside Prefix: The digits used to make an outbound trunk call.
- Local Country Code: The country code where the MiVoice Business is located.
- Long Distance Prefix: The prefix used for making a long-distance call. For example, in North America, use "1".
- International Prefix: The prefix used when making an international call.
- Local Area Codes: The local area codes (comma-separated) where the MiVoice Business system is installed.

- Max extension length: The maximum number of digits expected in Outside Prefix field.

The Mitel OIG Administration UI allows an admin to define a system set of default values for these settings or they can be set for a specific instance of the MiVoice Business. If all the MiVoice Business systems are in the same country and area code, the Administrator only needs to set the default values because the settings for all the MiVoice Business controllers will be the same.

If the MiVoice Business systems are in different area codes and countries, each MiVoice Business instance must be configured correctly for E.164 support and to match inbound or outbound calls to specific customer telephone numbers. For a complete description of the OIG Admin interface, see the *Mitel OIG Installation and Maintenance Guide*.

Mitel OIG Hardware and Software Requirements

This section provides the hardware and software system requirements for Mitel OIG. The Mitel OIG software executes in a Mitel MSL server. For compatible hardware, refer to the MSL Qualified Hardware List.

Mitel OIG Hardware Resources

The minimum recommended workstation resources for the Mitel OIG are shown in the table below. This applies to both a physical server and a virtualized environment.

For virtualized and cloud environments, since Mitel OIG is a multi-thread application, we recommend at least 2 CPUs. Mitel vOIG is configured to have 2 GHz reservation for each vCPU out of the box. The virtual RAM can be configured as low as 2 GB; however, the default is 4 GB when deployed. The hard disk space defaults to 20 GB, but Mitel vOIG uses 5.6 GB of real hard disk when deployed for fewer than 50 users.

Mitel has successfully tested 50 vOIG instances on one hardware server (VM server) with the following physical profile:

- Processor - Intel Xeon CPU E5-26200 @ 2.00 GHZ (12 - CPU Hyperthreading enabled)
- RAM - 192 GB installed with ESXI 5.5.
- Each VM instance (vOIG):
  - CPU - Reservation: 0 MHz, Limit: 4000 MHz
  - RAM - Reservation: 4 GB, Limit: 192 GB.

For detailed and up-to-date capacity, resource, and limit information for virtual appliances, including vOIG refer to the *Virtual Appliance Deployment Solutions Guide* on MiAccess > Document Center > Technology > Virtualization.

For detailed information for cloud deployments in AWS and Azure, please refer to the *Mitel MiVoice Business Solution and Engineering Guidelines* on MiAccess > Document Center > Technology > Virtualization.

Mitel OIG is supported in multi-core (e.g., quad core processors), virtualized and cloud environments.

- Hardware supported: Currently shipping Intel Xeon E3v2 / E5 / E7 Server Class series processors with a minimum of 4 cores, 2 GHz, Hyper-threading enabled, and Extended Page Table support (http://ark.intel.com/). For the latest hardware requirements for deployment in virtualized environments, refer to the *Virtual Appliance Deployment Solutions Guide*.
- Legacy server technology may also be used but must meet the minimum requirements listed in the *Virtual Appliance Deployment Solutions Guide*.

Also, see the VMware Hardware Compatibility Guide
here: http://partnerweb.vmware.com/comp_guide2/search.php

The following configurations were used at Mitel when testing the Mitel OIG. The first column indicates the Windows PC used for the test application. The remaining three columns present the off-the-shelf server hardware used by the Mitel OIG.

Note: Some of the hardware configurations below (used for testing) do have resource limits less than the recommended minimum.

Hardware used in testing the Mitel OIG

APP PLATFORM	OIG CPU	OIG HARD DRIVE	OIG MEMORY
Windows 7 Intel i3-2350M CPU @ 2.3 GHZ 8 GB RAM	Virtual 1 vCore - HP DL380 G7 Intel® Xeon® E5620 (2.40 GHz/12 cores), 64 GB RAM, 450 GB HD	20 GB	4 GB RAM
Windows 7 Intel i3-2350M CPU @ 2.3 GHZ 8 GB RAM	Virtual 2 vCore - HP DL380 G7 Intel® Xeon® E5620 (2.40 GHz/12 cores), 64 GB RAM, 450 GB HD	20 GB	4 GB RAM
Windows 7 SP1, Quad Core Intel Xeon W3550 @ 3.07 GHz, with 12.0 GB RAM	Virtual 2 vCPU - HP DL380 G7 Intel® Xeon® E5620 (2.40 GHz/12 cores), 64 GB RAM, 450 GB HD	20 GB	4 GB RAM
Windows 7 SP1, Dell Intel® Core ™ i5-2540M CPU @ 2.60 GHz, 8 GB RAM	Virtual 2 vCPU - HP DL380 G7 Intel® Xeon® E5620 (2.40 GHz/12 cores), 64 GB RAM, 450 GB HD	20 GB	4 GB RAM
Windows 7 Intel Core 2 Duo 2.93 GHz, 4 GB RAM	Physical 4 Core Intel(R) Xeon(R) CPU E31220 @ 3.10 GHz	240 GB	4 GB RAM
Windows 7 Intel Core 2 Duo ,2.93 GHz, 4 GB RAM	Physical 4 Core Intel(R) Core(TM) i5-2320 CPU @ 3.00 GHz	450 GB	4 GB RAM
Windows 7 Intel Core 2 Duo 2.93 GHz, 4 GB RAM	Physical 4 Core Intel(R) Core(TM) i3-2100 CPU @ 3.10 GHz	240 GB	8 GB RAM
Windows 7 Intel(R) Core(TM) i5-2320 CPU@ 3.00 GHz, 2.99GHz, 2.94 GB RAM	Physical IBM System X3250 M4, Intel(R) Xeon(R) CPU E31220 @ 3.10 GHz	240 GB	4 GB RAM

Note: Remote MiVoice Integration applications require use of a MiVoice Border Gateway 9.3 SP1+ web proxy.

MSL Platforms

Refer to the MSL Qualified Hardware List for MSL hardware compatibility.

1. Log in to MiAccess
2. Select “Document Center” in the left sidebar, then select “Technology”
   - Select “Mitel Standard Linux” for MSL product documentation
   - Search for “Mitel Standard Linux Qualified Hardware List” for MSL qualified hardware list of required versions.

Mitel OIG Software Version Compatibilities and Requirements

Applications use Mitel OIG WSDL files to enable communication with a Mitel OIG. A Mitel OIG solution requires an application using a WSDL version, a Mitel OIG server version, and a call manager version (MiVoice Business) that are compatible with each other. The Mitel OIG must also be installed on the compatible MSL version. Compatibility is also affected by the type of operations the applications are performing.

- MiVoice Business 10.0 SP1 is fully compatible with OIG 4.2 SP4.
- The WSDL version used by an application cannot be more recent than the version of the Mitel OIG server. An application using a given version of WSDL files can communicate only with a Mitel OIG with the same version or newer. For example, when an application uses the WSDL files provided with Mitel OIG 4.2 SP4, the Mitel OIG server itself must be upgraded to Mitel OIG 4.2 SP4. The Mitel OIG version number must be equal to or greater than the WSDL file version used in the application, i.e., 4.2.
- Mitel recommends that applications use Mitel OIG 4.2 SP4 and MiVoice Business Release 10.0 SP1.

The table below shows the compatibility between an application using Mitel OIG WSDL files, a Mitel OIG server, and a MiVoice Business call server. Applications must use Mitel OIG WSDL file versions that align with Mitel OIG server versions and the call server (MiVoice Business).

OIG Version Compatibility

OIG SERVER VERSION	APPLICATION WSDL VERSION	MIVOICE BUSINESS VERSION	MICD MULTI INSTANCE	MSL VERSION	CONSIDERATIONS	
4.2. SP4	4.2 SP4	10.0 SP1	NA	11.0.106.0	MiVoice Business: All OIG features and operations are supported	Recommended deployment
		9.4	NA			
		9.3	NA			
		9.2	NA			
		9.1 SP1	NA			
		9.1	NA			
		9.0 SP3	NA			
		9.0 SP2	NA			
		9.0 SP1	NA			
		8.0	2.0 SP1			

OIG SERVER VERSION	APPLICATION WSDL VERSION	MIVOICE BUSINESS VERSION	MICD MULTI INSTANCE	MSL VERSION	CONSIDERATIONS	
4.2. SP3	4.2 SP3	9.4 SP1	NA	11.0.102.0	MiVoice Business: All OIG features and operations are supported	Recommended deployment
		9.4	NA			
		9.3	NA			
		9.2	NA			
		9.1 SP1	NA			
		9.1	NA			
		9.0 SP3	NA			
		9.0 SP2	NA			
		9.0 SP1	NA			
		8.0	2.0 SP1			
4.2 SP2	4.2 SP2	9.4	NA	11.0.93.0	MiVoice Business: All OIG features and operations are supported	Recommended deployment
		9.3	NA			
		9.2	NA			
		9.1 SP1	NA			
		9.1	NA			
		9.0 SP3	NA			
		9.0 SP2	NA			
		9.0 SP1	NA			
		8.0	2.0 SP1			
4.2 SP1	4.2 SP1	9.3	NA	11.0.90.0	MiVoice Business: All OIG features and operations are supported. AWS and Azure Deployments supported	Recommended deployment
		9.2	NA			
		9.1 SP1	NA			
		9.1	NA			
		9.0 SP3	NA			
		9.0 SP2	NA			
		9.0 SP1	2.0 SP1			
		8.0				
4.2	4.2	9.2	NA	11.0.84.0	MiVoice Business: All OIG features and operations are supported	Recommended deployment
		9.1 SP1	NA			
		9.1	NA			
		9.0 SP3	NA			
		9.0 SP2	NA			
		9.0 SP1	NA			
		8.0	2.0 SP1			

OIG SERVER VERSION	APPLICATION WSDL VERSION	MIVOICE BUSINESS VERSION	MICD MULTI INSTANCE	MSL VERSION	CONSIDERATIONS	
4.1 SP5	4.1 SP5	9.1 SP1 9.1 9.0 SP3 9.0 SP2 9.0 SP1 8.0	NA NA NA NA NA 2.0 SP1	11.0.64.0	MiVoice Business: All OIG features and operations are supported	Recommended deployment
4.1 SP4	4.1 SP4	9.1 9.0 SP3 9.0 SP2 9.0 SP1 8.0	NA NA NA NA 2.0 SP1	11.0.63.0	MiVoice Business: All OIG features and operations are supported	Recommended deployment
4.1 SP3	4.1 SP3	9.0 SP3 9.0 SP2 9.0 SP1 8.0	NA 2.0 SP1	10.5.25	MiVoice Business: All OIG features and operations are supported MiVoice phones 6905 IP and 6910 IP devices are supported only in this and subsequent configurations (MiVoice Business 9.0 SP3/ OIG 4.1 SP3)	Recommended deployment
4.1 SP2	4.1 SP2	9.0 SP2 9.0 SP1 8.0	NA 2.0 SP1	10.5.25	MiVoice Business: All OIG features and operations are supported	Recommended deployment
4.1 SP1	4.1 SP1	9.0 SP1 8.0	NA 2.0 SP1	10.5.25	MiVoice Business: All OIG features and operations are supported MiCollab ACD Softphones are supported in this configuration for Data Access Services only (MiVoice Business 9.0 SP1/ OIG 4.1 SP1)	Recommended deployment
4.1	4.1	9.0 8.0	NA 2.0 SP1	10.5.25	MiVoice Business: All OIG features and operations are supported Analog-FXS phones are supported in this configuration for Data Access Services only (MiVoice Business 9.0/ OIG 4.1)	Recommended deployment

OIG SERVER VERSION	APPLICATION WSDL VERSION	MIVOICE BUSINESS VERSION	MICD MULTI INSTANCE	MSL VERSION	CONSIDERATIONS	
4.0	4.0	8.0	2.0 SP1	10.5.15	MiVoice Business: All OIG features and operations are supported MiVoice 6900 Series phones are supported only in this and subsequent configurations (MiVoice Business 8.0+/ OIG 4.0+)	Recommended deployment
3.1	3.1	7.2	2.0 SP1	10.3	MiVoice Business: All OIG features and operations are supported	Recommended deployment
3.0	3.0	7.2	2.0 SP1	10.3	All OIG features and operations are supported	Recommended deployment
2.2	2.1 or 2.2	7.1	2.0	10.3	All OIG features and operations are supported	
2.1	2.0 or 2.1	7.0 SP1	2.0	10.2	All OIG features and operations are supported	
2.0	2.0	7.0	1.2 SP2	10.1	All OIG features and operations are supported	
2.0	2.0	6.0 SP3	1.2 SP1	10.1	OIG Standard Call Control service operations only, including MiVoice Integration for Salesforce	
2.0	1.2	7.0	1.2 SP2	10.1	OIG Standard Call Control service operations only, including MiVoice Integration for Salesforce	Compatible combinations
2.0	1.2	6.0 SP3	1.2 SP1	10.1	OIG Standard Call Control service operations only, including MiVoice Integration for Salesforce	
1.2	1.2	6.0 SP3	1.2 SP1	10.0	All OIG 1.2 features and operations are supported, including MiVoice Integration for Salesforce. MCD 6.0 SP3 is required for call server IP Phone resiliency	
1.2	1.1	6.0 SP3	1.2 SP1	10.0	All OIG 1.1 features and operations are supported. MCD 6.0 SP3 is required for call server IP	

OIG SERVER VERSION	APPLICATION WSDL VERSION	MIVOICE BUSINESS VERSION	MICD MULTI INSTANCE	MSL VERSION	CONSIDERATIONS
					Phone resiliency
1.1	1.1	6.0 (all SPs)	1.2 SP1	10.0	All OIG 1.1 features and operations are supported
1.1	1.0	6.0 (all SPs)	1.2 SP1	10.0	All OIG 1.0 features and operations are supported
1.0	1.0	6.0 (all SPs)	1.2 SP1	9.4	All OIG 1.0 features and operations are supported

The Mitel OIG provides a web-based administration interface that can be used with the latest versions of Windows Internet Explorer, Google Chrome, and Firefox.

Notes:

1. Mitel OIG is supported in AWS and Azure deployments.
2. Mitel OIG is supported in a virtualization environment (VMware vSphere ® 5.5, 6.0 and 7.0, Standalone (single ESXi) or Managed (vCenter ® 5.5, 6.0 and 7.0 Server) modes.
3. Mitel OIG administration from a Windows PC supports web browser access (Google Chrome, Microsoft Internet Explorer) on the following operating systems: Windows 11 (64-bit version), Windows 10 (both 32 and 64-bit versions), Windows 8 (both 32 and 64-bit versions), Windows 7 Professional (both 32 and 64-bit versions), Windows XP Professional SP3.
4. Co-residency guidelines: One Mitel OIG per MSL server. Co-residency of OIG software with other applications is not supported.
5. Co-location guidelines: The Mitel OIG must be co-located in the enterprise LAN or VLAN with the MiVoice call manager or MiVoice call manager cluster. If there is also a MiContact Center server, it must also be on the same LAN with the OIG server and the MiVoice call manager server.

Mitel OIG IP Port Number Usage

This section presents the IP ports used by the Mitel OIG.

PORT RANGE	DIRECTION	PURPOSE
TCP 22 (SSH)	Mitel OIG to Internet	The Mitel OIG must connect to the Mitel AMC server over the Internet using SSH port 22. Allow outbound packets (and replies) on TCP port 22 for registration, software and license key downloads, alerts, and reporting.
	Internet to Mitel OIG	Remote SSH access (Optional). The Mitel OIG administrator may need access to the MSL server to retrieve maintenance information. The Mitel OIG administrator collects maintenance information using SSH port 22.
	Admin PC to Mitel OIG	The Mitel OIG administrator may need access to the MSL server to retrieve maintenance information. The Mitel OIG administrator collects maintenance information using SSH port 22.

PORT RANGE	DIRECTION	PURPOSE
TCP 443 (HTTPS)	Admin PC to Mitel OIG	The Mitel OIG administrator needs access to the MSL server manager UI and to the Mitel OIG UI. The administrator will use a web browser, so the Mitel OIG server must allow access on HTTPS port 443.
	Mitel OIG to Internet	The Mitel OIG must connect to the Mitel MCS server on the Internet using HTTPS port 443. The Mitel OIG must communicate with MCS to get the ACL (Access Control List). The Mitel OIG retrieves the ACL from MCS using a web service call over HTTPS.
TCP 5320 (SSL)	Mitel OIG to MiVoice Business	The Mitel OIG must connect to each MiVoice Business using IP port 5320 on the MiVoice Business. After this one-way connection is established (Mitel OIG to MiVoice Business), the Mitel OIG sends a message to the MiVoice Business with its IP address information. The MiVoice Business then connects to the Mitel OIG using this IP address on port 49500. **Note:** The Mitel OIG MSL server firewall must be configured to allow each MiVoice Business (IP address) to communicate with the Mitel OIG.
TCP 49500 - 49600 (SSL)	MiVoice Business to Mitel OIG	Allow incoming and outgoing packets for TCP port 49500 - 49600 between the Mitel OIG and a MiVoice Business.
443 (HTTPS)	Application to Mitel OIG	Applications send SOAP/XML or REST/JSON messages to the Mitel OIG using HTTP or HTTPS (ports 80 and 443). Applications may register to receive Mitel OIG events asynchronously. When asynchronous event response is requested, the Mitel OIG must be able to send back events to the application using HTTP or HTTPS (ports 80 and 443). The application indicates HTTPS or HTTP when registering an event handler with the Mitel OIG. The Mitel Hosted Virtual Test Lab supports only application event handlers that use HTTPS port 443.
80 (HTTP)	Application to Mitel OIG	Applications send SOAP/XML or REST/JSON messages to the Mitel OIG using HTTP or HTTPS (ports 80 and 443). Applications may register to receive Mitel OIG events asynchronously. When asynchronous event response is requested, the Mitel OIG must be able to send events back to the application using HTTP or HTTPS (ports 80 and 443). The application indicates HTTPS or HTTP when registering an event handler with the Mitel OIG. The Mitel Hosted Virtual Test Lab supports only application event handlers that use HTTPS port 443.
443 (HTTPS)	Mitel OIG to Application	Applications send SOAP/XML messages to the Mitel OIG using HTTP or HTTPS (ports 80 and 443). Applications may register to receive Mitel OIG events asynchronously. When asynchronous event response is requested, the Mitel OIG must be able to send events back to the application using HTTP or HTTPS (ports 80 and 443). The application indicates HTTPS or HTTP when registering an event handler with the Mitel OIG. The Mitel Hosted Virtual Test Lab supports only application event handlers that use HTTPS port 443.
80 (HTTP)	Mitel OIG to Application	Applications send SOAP/XML messages to the Mitel OIG using HTTP or HTTPS (ports 80 and 443). Applications may register to receive Mitel OIG events asynchronously. When asynchronous event response is requested, the Mitel OIG must be able to send events back to the application using HTTP or HTTPS (ports 80 and

PORT RANGE	DIRECTION	PURPOSE
		443). The application indicates HTTPS or HTTP when registering an event handler with the Mitel OIG. The Mitel Hosted Virtual Test Lab supports only application event handlers that use HTTPS port 443.

Mitel OIG Application Design Considerations

This section provides application design considerations relating to Mitel OIG performance. Additional design considerations are provided in the Mitel OIG Developer Guides.

Mitel OIG Licensing for Call Control Service

One Mitel OIG user license provides two monitors. In simple MiVoice call manager systems, one user may map to one monitor (e.g., each user has one phone, and the application only needs to monitor the phone prime line). If a Mitel OIG application requires more than two monitors per user (e.g., user has a phone with two-line appearances resulting in three monitors), then more user licenses are needed. The Mitel OIG tracks monitors created by applications, not users in the MiVoice call manager system.

Mitel OIG support for MiVoice Business IP Phone Resiliency does not consume an extra licensed monitor when opening a monitor on a Secondary MiVoice Business. Thus, Mitel OIG AMC licensing for Standard or Advanced Call Control Service is not affected by support for MiVoice Business IP Phone Resiliency.

Entitlement of MiVoice Integration applications (for Salesforce or Google) on OIG Base Packages (P/Ns 54005784 or 54005785) requires purchase of the associated MiVoice Integration part numbers.

To use the MiVoice Integration for Salesforce Release 2.1+ with MiContact Center, you also need the MiContact Center Business licensing.

Impact of Mitel OIG on MiVoice Call Manager Performance

Impact of Mitel and Legacy MiTAI on MiVoice Business

When MiTAI applications are connected to a MiVoice Business and applications that use Mitel OIG are also connected to the same MiVoice Business (using call control monitors), there is a performance impact. Prior to the release of Mitel OIG, applications used the legacy MiTAI API for call control services on the MiVoice Business.

Note: Mitel OIG applications using monitors do not affect performance in the same way as legacy MiTAI applications using monitors. Adding Mitel OIG to an existing MiVoice Business system that already has Mitel applications is expected to degrade performance by 50% less than what happens when adding legacy MiTAI applications. For example, adding two Mitel OIG monitors to a MiVoice Business has approximately the same impact as adding one legacy MiTAI monitor. Using the new MiTAI Driver monitors has the same impact as using Mitel OIG monitors.

Total and Shared Limits

The total limit is the maximum count of unique monitors on each MiVoice call manager. The shared limit is the maximum sum of monitors set by all the applications. If two applications ask for a monitor on the same device on the same MiVoice call manager, there is one total monitor and two shared monitors.

Table 2: Device and Feature Monitor limits

	CALL CONTROL LIMIT	APPLICATION LIMIT
DEVICE MONITOR LIMITS IN MIVOICE BUSINESS 6.0 SP3 (ICP 3300 RELEASE 12.0.3.34) TO MIVB 7.0		
x86-based processor	5600	10000
Power PC-based processor	2000	5000
FEATURE MONITOR LIMITS IN MIVOICE BUSINESS 6.0 SP3 (ICP 3300 RELEASE 12.0.3.34) TO MIVB 7.0		
x86-based processor	5600	10000
Power PC-based processor	2000	5000
DEVICE MONITOR LIMITS IN MIVOICE BUSINESS 7.0 SP1 ONWARDS		
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 700		
x86-based processor	5600	10000
Power PC-based processor	2000	5000
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 5600		
x86-based processor	17000	30000
Power PC-based processor	2000	5000
FEATURE MONITOR LIMITS IN MIVOICE BUSINESS 7.0 SP1 ONWARDS		
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 700		
x86-based processor	5600	10000
Power PC-based processor	2000	5000
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 5600		
x86-based processor	17000	30000
Power PC-based processor	2000	5000
DEVICE MONITOR LIMITS IN MIVOICE BUSINESS 7.2 SP1 ONWARDS		
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 700		
x86-based processor	5600	10000
Power PC-based processor	4000	5000
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 5600		
x86-based processor	17000	30000
Power PC-based processor	4000	5000

FEATURE MONITOR LIMITS IN MIVOICE BUSINESS 7.2 SP1 ONWARDS		
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 700		
x86-based processor	5600	10000
Power PC-based processor	4000	5000
Maximum Configurable IP Users and Devices license (on MiVoice Business) = 5600		
x86-based processor	17000	30000
Power PC-based processor	4000	5000

Example:

- Application A (MiTAI Client) has 100 monitors.
- Application B (MiTAI Driver) has 100 monitors
- Application C (Mitel OIG) has 100 monitors

If all three applications are monitoring different devices, the result is 300 total monitors in the MiVoice call manager, 100 shared for MiTAI client and 200 shared monitors for MiTAI Driver and Mitel OIG. If all three applications are monitoring the same device, the result is 100 total monitors in MiVoice call manager and 100 shared monitors in MiTAI Client and 200 in shared monitors for MiTAI Driver and Mitel OIG.

The total monitors in MiVoice call manager are shared by legacy MiTAI Client, new MiTAI Driver and Mitel OIG.

MiVoice Call Control Integration Design Model Considerations

The two major Call Control Integration design model considerations are:

- MiVoice Integrations
- Mitel OIG event data

MiVoice Integrations

Mitel OIG support for MiVoice Integrations does have an impact on Mitel OIG performance; a maximum of 1500 concurrent MiVoice Integration application instances are supported. Each type of MiVoice Integration is considered an application. Each MiVoice Integration application instance (i.e., browser-based client user) consumes one communication session with the Mitel OIG (e.g., MiVoice Integration for Salesforce®).

For example, the Mitel OIG considers 100 logged-in Salesforce CRM users as 100 communication sessions from 100 applications of the same application type; MiVoice Integration for Salesforce.

The Mitel OIG supports up to 1500 MiVoice Integration application users. These 1500 users consume 1500 Mitel OIG standard call control monitors; one monitor for each communication session (exception is MiVoice Integration for Salesforce with MiContact Center Business, which uses Mitel OIG advanced call control monitors). For Example, When Mitel OIG has 150 MiVoice Integration application users, the remaining allowable connection limit for applications is reduced to 1350.

Opening additional Salesforce tabs when using MiVoice Integration for Salesforce does not consume additional Salesforce user licenses. However, opening new browser windows containing MiVoice Integration for Salesforce, whether on the same PC or a different PC, still adds to the total consumed call control monitor licenses. Please refer to the *Mitel Open Integration Gateway – Installation and Maintenance Guide* for more details.

Mitel OIG Event Data (Single MiVoice Business System Compared to Multiple MiVoice Business Controllers in A System)

The Mitel OIG events (and data in the events) received by an application when connected to one MiVoice Business controller are different than the events received when connected to a MiVoice Business system cluster.

When all the phones being controlled and monitored by an application are on one MiVoice Business, the MiVoice Business call control engine has the complete details about all phones. Thus, the MiVoice Business can provide these details to the application. When phones are in a MiVoice Business system cluster, some MiVoice Business in the cluster do not have or receive the complete details about remote phones. Thus, the MiVoice Business cannot always provide complete details to the application.

Sometimes the Mitel OIG events provided to an application are different when comparing a single MiVoice Business to a MiVoice Business system cluster. For example, two phones (1 and 2) on MiVoice Business A create a conference with phone 3 on MiVoice Business B. In this case, a monitor on phone 3 on MiVoice Business B does not receive a conference party list (a list indicating phones 1, 2, 3 are in a conference).

There are many MiVoice Business call control scenarios. To understand the Mitel OIG event flow, refer to the *Mitel OIG Developer Guide - Call Control Services* for more details about the MiVoice Business call control model and the resulting Mitel OIG event flow.

Example: While the *Mitel OIG Developer Guide - Call Control Services* documents the web service API, the application developer should lab test the expected behavior to determine event flow and performance impact.

Mitel OIG and Device Behavior

MiVoice Business SIP Device Monitoring and Control

The Mitel OIG offers limited support for SIP devices. The OIG monitor event flow for SIP devices is different from the event flow for a MiVB IP Phone. With MiVB 9.0 SP2, MiVB has added enhancements to support the implementation of event packages. For details, please refer to the Talk and Hold event packages, which are an instantiation of the SIP specific event notification framework (as defined in RFC 3265 by Roach, A.B., “Session Initiation Protocol (SIP)-Specific Event Notification”, RFC 3265, Internet Engineering Task Force, June 2002. Available from http://www.ietf.org/). Please refer to the *OIG Developer Guide – Call Control* for a summary on SIP Behavior.

Below are some behaviors to consider:

- An application cannot use the Mitel OIG to make a SIP device go off hook or on hook (make, answer, or clear a call). Even though the API returns no failure, the user needs to manually handle the SIP device to successfully make, answer or clear call.
- For example, when an OIG makeCall API is invoked on a SIP device to another phone, the originator SIP device will ring. On answering the SIP device manually, a call is then made to the number requested in the makeCall command.
- Supervised and unsupervised transfer call scenarios result in different event flows. Some SIP devices require two lines to complete a transfer. Hence, the MiVB administrator must configure the SIP device with a second line appearance (this must be a multi-call appearance of the prime line) and the application must monitor multiple lines on the SIP device to track all the related call status event flow.
- A call hold and retrieve scenario is different on a SIP device (as compared to an ONS device).
- CampOn hard held local call is not supported and returns the error, "Feature not allowed".
- CampOn hard hold remote call is not supported and returns the error, "Feature not allowed".
- Send CallMeBack Message for Call is not supported and returns the error, "Feature not allowed".
- Set CallMeBack Message is not supported and returns the error, "Feature not allowed".

Note: Application developers developing applications that use Mitel OIG and SIP devices should lab test their behavior before rolling out a solution.

MiVoice Business External Hot Desk User Phones

A Mitel OIG application can monitor an external hot desk user (EHDU) phone. The response times and event flows from EHDU phones are different than for locally connected phones.

Note: Application developers interested in MiVoice Business EHDU should lab test such behavior before rolling out a deployment.

Impacts of MiVoice Business IP Phone Multi-Line/Key Line Monitoring

Applications can monitor line appearances on a Mitel IP phone. Line appearances can be programmed as key line or multi-call. Monitoring a line appearance is considered a monitor, in addition to the prime line monitor, for the phone. Monitoring line appearances has a significant performance impact on the MiVoice Business due to the increase in the number of events generated.

As an example of what NOT to do: consider a MiVoice Business configured to have the same phone number (DN) on 100 multi-call line appearances. Consider an application that is monitoring all line appearances and the prime line. When a call is received, 101 call received events will be generated at the same time. Now if a second call arrives immediately after the first is answered, another 101 call status events will be generated at the same time. Hundreds of events can be generated within a few seconds in this scenario. If several phones have the same configuration, the large number of call status events generated will have a performance impact on the overall system.

Note: Having more than ten-line appearances on one DN while having monitors on all lines is not recommended.

The following table shows the limits for monitoring line appearances on MiVoice Business phones.

Monitoring Line Appearances on one MiVoice Business Controller

CALL TRAFFIC (CPH) ACROSS ALL MIVOICE BUSINESS LINES + TOTAL BACKGROUND CALL TRAFFIC	PRIME LINE + LINE APPEARANCES AS MULTICALL	PRIME LINE + LINE APPEARANCES AS KEYLINE	NUMBER OF MONITORED IP PHONES	TOTAL LINES ON ALL IP PHONES
2500 + 2000	prime + 4		30	150
2500 + 2000	prime + 2		50	150
2500 + 2000		prime + 10	20	220
2500 + 2000		prime + 5	40	240
2500 + 2000		prime + 2	100	300

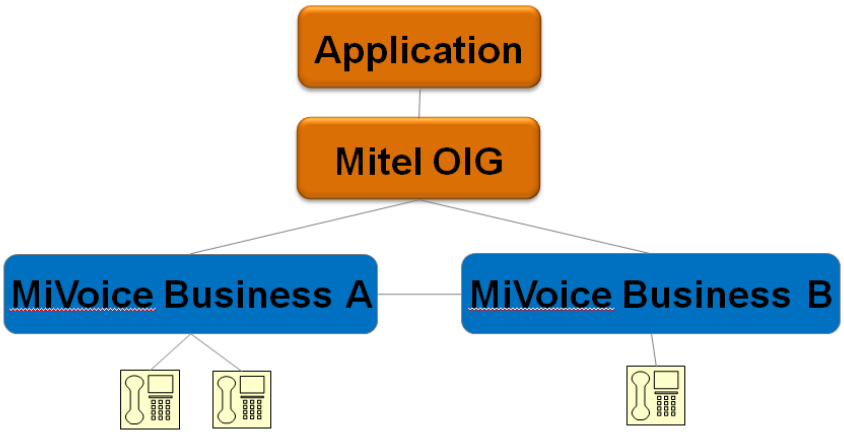
Impact of Legacy MiTAI on MiVoice Business IP Phones

Most Mitel IP phones have a default MiTAI monitor because of the features provided on the phone itself. For example, a Mitel IP phone call log feature uses MiTAI in MiVoice Business to collect call information, so at least one MiTAI monitor is created within the MiVoice Business controller for each IP phone with the call log feature. This means that even though no MiTAI application is connected to MiVoice Business, MiTAI still has a performance impact. Thus, the performance guidelines presented in the Mitel OIG engineering guidelines are affected when MiTAI is enabled, and many Mitel MiNET IP phones are being monitored.

Event Handling

Event Handler for Asynchronous Events from Mitel OIG

An application can either poll the Mitel OIG for events or provide an event handler to receive events asynchronously. However, an application cannot use both event methods at the same time. For most applications, polling for events will be more than sufficient. Mitel recommends that an application poll for events until an application developer determines that expected system size requires asynchronous event flow.



If the event handler approach is chosen, a web server framework is needed in the same workstation as the application. See the *Mitel OIG Developer Guide – Call Control Service Guide* for more details). The choice of web server framework can also affect performance. For example, here are the results of some testing:

- Microsoft IIS 6.0 produced poor performance results in Mitel lab testing.
- Windows Communication Foundation "ServiceHost" provided good results.
- Apache Tomcat provided good results.

Interactions among Mitel OIG, MiVoice Business, and MiContact Center

MiVoice displays information to the Salesforce user based on Mitel OIG call status events from the MiVoice Business controllers and call details from the MiContact Center server.

When a MiVoice Business controller redirects a call to another MiVoice Business controller (in a MiVoice Business cluster), some call details may be lost because of how call details are passed across the trunk between controllers. When this happens, MiVoice Integration for Salesforce cannot display the information to a Salesforce user.

The MiContact Center server uses MiTAI call status events to track calls. If MiTAI call status events to MiContact Center arrive out of order, Mitel OIG and MiVoice Integration for Salesforce must handle changes in call details from the MiContact Center server. For example, MiContact Center needs to know whether a call is from an ACD path or whether it is a direct call to a user or ACD agent. If a MiTAI call established event arrives before a MiTAI call is delivered, the MiContact Center server does not know that the call has come through an ACD path/queue.

More details about where and how information is used and stored in a system including MiVoice Integration for Salesforce:

- MiContact Center is configured with account codes and classification codes.
- Classification codes are mapped to ACD paths. For example, a call to an ACD path requires a classification code for a specific hot desk ACD agent.
- Mitel OIG does not store any MiContact Center codes. When they are needed, the Mitel OIG requests specific codes from the MiContact Center server.
- MiVoice Integration for Salesforce (through Mitel OIG) sends classification codes back to MiContact Center, but not to the MiVoice Business controller.
- MiVoice Integration for Salesforce (through Mitel OIG) sends account codes and Make Busy codes to the MiVoice Business controller.

Conditions for Mitel OIG Events per Second

The maximum recommended Mitel OIG event flow is determined for the following conditions:

- IP Phone call times remain within specifications under call traffic
- Event response times stay within one (1) second
- No Mitel OIG time-out software error log messages or server failures are recorded.

A call between two monitored phones triggers seven events from a MiVoice call manager (four events to the caller and three events to the called party when the caller generates the call with “make call” and called party answers and clears the call with “answer call” and “clear call”).

Mitel OIG Software Logs

The Mitel OIG executes in the Mitel MSL operating system. The Mitel OIG uses the MSL Tomcat component to generate software logs. A new Tomcat log file is created when the tomcat_current log file size reaches 1 MB. The Mitel OIG stores ten tomcat log files (1 MB each). The Tomcat software logs are found under the MSL /var/log/tomcat directory. The Mitel OIG administrator can either use the MSL server command line and view the log files or use the MSL server manager and go to Administration -View Log Files and select tomcat logs from the drop-down menu to view the log files

in a browser. The Mitel OIG Tomcat logs generated are tagged with log level (information – INFO, warning - WARN or error - ERR).

Mitel OIG Event Time

The EventTime in Mitel OIG events is a 64-bit Integer. For example, a MONITOR_SET event has an event time of 1349360583326. This number represents a millisecond value that is an offset from the Epoch, January 1, 1970 00:00:00.000 GMT.

General Messages

- The Mitel OIG rejects application commands to a MiVoice Business when the MiVoice Business is disconnected from the Mitel OIG.
- The Mitel OIG provides MiVoice Business connection status events to connected applications.
- The Mitel OIG supports a keep-live mechanism with each application to detect when to close a communication session with the application.
- By default, the Mitel OIG syncs with the AMC license server every four hours, or when manually triggered by the Mitel OIG administrator.
- If the Mitel OIG detects a license error, the following is sent to an application:
  - result.setResult(false);
  - result.setErrorDescription("No license available.");
- The Mitel OIG syncs with the Mitel Certificate Server every four hours or when manually triggered by the Mitel OIG administrator.
- When MiVoice Business COS settings needed for Mitel OIG monitoring are not set correctly, an application receives an error (PRIVILEGE_VIOLATION).
- When one or more MiVoice Business controllers are not ENABLED for Mitel OIG monitoring, an application receives an error (PRIVILEGE_VIOLATION).

Mitel OIG Performance Guidelines

This section summarizes the Mitel OIG performance guidelines. These recommendations are based on testing conducted in Mitel test labs with physical and virtualized hardware environments using both Mitel OIG and vOIG. Limits presented for the Mitel OIG are estimated or calculated from the data collected during lab testing. Mitel is not able to performance test all possible system combinations. Mitel recommends that each application developer conduct performance testing using test environments that simulate their own expected site deployments.

Considerations for Mitel OIG 4.2 SP4

All MiVoice Business controllers in the system cluster must be MiVoice Business 10.0 SP1.

- Avoid having PSTN trunks and all IP Phones on the same MiVoice Business; deploy PSTN trunk connections on a MiVoice Business Gateway, and IP Phones on a user MiVoice Business.
- Mitel assumes that the application developer will performance test expected deployment configurations before installing a Mitel OIG application at a customer site.
- Each MiVoice Business should have no more 30,000 calls per hour when communicating with a Mitel OIG.
- The Mitel OIG should have no more than 90,000 calls per hour from all MiVoice Business controllers in the MiVoice Business system cluster.
- A MiVoice Business can have a maximum of 5000 Mitel OIG monitors. Some MiVoice Business controllers have a monitor limit of 2000. Refer to the *MiVoice Business Engineering Guidelines* documentation for a description of the MiVoice Business capacities and limits.

The Mitel OIG can have a maximum of 50,000 monitors.

This guide provides engineering limits for the whole system, and engineering limits for individual components within the system. Application design must consider all limits and must not exceed any individual limit. Consider the following limits:

- 50,000 monitors for one Mitel OIG
- 5000 monitors for one MiVoice Business
- 250 MiVoice Business controllers for one Mitel OIG
- Each of the 250 MiVoice Business controllers cannot have 5000 monitors because the Mitel OIG allows a maximum of 50,000.
- 1 MiVoice Border Gateway to act as web proxy for 50 Mitel OIGs. This applies to a MiVoice Business system only.

Mitel OIG applications using Data Access Service read operations should lab test the read operation response time. Consider an application that wants the phone numbers for all phones within a large MiVoice Business cluster, where the cluster has 45,000 phones. Such a request would take longer than an application requesting the software version of a specific MiVoice Business.

Mitel OIG Call Control

Maximum Call Control Operations per Second

MiVoice Business:

- One MiVoice Business can support an average of 20 operations (commands) per second from one Mitel OIG when no MiTAI applications are connected to the MiVoice Business. A MiVoice Business controller may receive more operations (commands) per second than this, but warnings and errors may occur.
- One Mitel OIG can generate an average of 150 operations (commands) per second to a MiVoice Business cluster with eight or more MiVoice Business controllers. A Mitel OIG may generate more operations (commands) per second than this, but warnings and errors may occur.
- One application should generate only an average of 20 operations (commands) per second (to one MiVoice Business) to a Mitel OIG. An application may generate more operations (commands) per second than this, but warnings and errors may occur.
- When using the Mitel OIG Call Control Service, an application should avoid opening and closing a monitor for each call. Best practice is to open all needed monitors when an application starts, and to close all monitors before the application shuts down.
- A Mitel OIG server supports a maximum of 1500 applications or application instances. If all applications send 20 operations per second, then the total number of operations presented to the Mitel OIG would be 30,000 operations per second; more than the 150 recommended / allowed, so Mitel OIG applications should have exception handling to retry operations if these requests fail. If an application is experiencing many failing operations, the application should add delay between operation requests.

Maximum Call Control Events per Second

MiVoice Business:

- One MiVoice Business can generate an average of 60 events per second to one Mitel OIG when no MiTAI applications are connected to the MiVoice Business. A MiVoice Business may generate more events per second, but warnings and errors may occur.
- One Mitel OIG can generate an average of 175 events per second to one or more applications. A Mitel OIG may generate more events per second, but warnings and errors may occur.
- A Mitel OIG server supports up to a maximum of 250 MiVoice Business controllers. If all MiVoice Business controllers were sending 60 events per second to one Mitel OIG, then the total number of events would be 6000 events per second; more than the 175 recommended / allowed, so Mitel OIG applications should have exception handling to address missing or time-out events. If an application misses receiving one event, but later events indicate correct call status, the application should continue, but log that one or more events were missed.

Mitel OIG Call Control Service Impact on MiVoice Business

- The performance impact to a MiVoice Business controller incurred when Mitel OIG applications use monitors on MiVoice Business phones is 50% of the performance impact to a MiVoice Business incurred when MiTAI client applications (SDK 5.1) use monitors on MiVoice Business phones. MiTAI Driver applications (SDK 6.0 and above) have the same performance impact on a MiVoice Business as that of Mitel OIG applications.
- The performance impact to MiVoice Business IP phone MiNET call signaling times incurred when Mitel OIG applications use monitors on the same MiVoice Business IP phones is 5%.

For example, you can run call traffic through Mitel IP phones without Mitel OIG applications using monitors. Then you can repeat the timing tests on MiVoice Business IP phone MiNET call signaling with Mitel OIG applications using monitors. The delay in timing with Mitel OIG applications using monitors is approximately 5% compared with no Mitel OIG.

Mitel OIG Call Control Service Impact on Applications

- When monitoring thousands of phones, the Mitel OIG can send an application a burst of events at a rate of over 200 events per second. The application needs to be able to poll for events very quickly or provide a very efficient event handler. An application must be able to process events from the Mitel OIG at a rate of one event every seven milliseconds. If not, there is a risk that some Mitel OIG events from a MiVoice call manager system cluster may be lost.
- Mitel OIG event loss is indicated in the MSL server Tomcat software logs as message queue overflow.

Mitel OIG Call Control Service Message Size

CALL CONTROL SERVICE MESSAGE	SIZE (BYTES)	NOTES
Application request to Mitel OIG	500	
Mitel OIG operation response to an application	300	
Mitel OIG event to an application	500	Plus event data up to 300 bytes
Mitel OIG operation request to MiVoice call manager	50	
MiVoice Business operation response to Mitel OIG	50	
MiVoice Business event to Mitel OIG	50	Plus event data up to 300 bytes

Note: Message size between the Application and Mitel OIG is larger than message between Mitel OIG and MiVoice Business. The Applications messages are in XML.

The MiVoice Business messages are in binary.

APPLICATION OPERATIONS (APP TO MITEL OIG)	PACKET SIZE IN BYTES
loginEx()	651
getICPID()	459
getPhonenumberID()	467
monitorObject()	401
makecall()	412
getEvent()	391

RESPONSE FROM OIG (MITEL OIG TO APP)	PACKET SIZE IN BYTES
loginResponse	283
getICPIDResponse	446
getPhoneNumberIDResponse	294
monitorResponse	298
makecallresponse	264
logoutResponse	253

EVENT FROM OIG (MITEL OIG TO APP)	PACKET SIZE IN BYTES
MonitorSetEvent	491
CallReceivedEvent	1827
CallDeliveredEvent	2074
CallClearedEvent	1574

Mitel OIG Call Control Operation and Event Response Times

- Avg. Operation response time = 50 milliseconds
- Avg. time between Events = 7 milliseconds.

Mitel OIG Data Access Service

Data Access Service Impact on MiVoice Business

- Mitel OIG Data Access service read operations have no impact on a specific MiVoice Business, because the data is retrieved from the Mitel OIG server database.

Data Access Service Impact on Applications

- Mitel OIG applications using Data Access Service read operations should lab test the read operation response time. Consider an application that wants the phone numbers for all phones within a large MiVoice Business cluster, where the cluster has 45,000 phones. Such a request will take longer than an application requesting the software version of a specific MiVoice Business. The read request from an application is blocking so the read must complete before the application receives the response.
- When several Mitel OIG applications use Data Access Service read operations at the same time, the Mitel OIG server processes the read operations sequentially. The application developer should lab test read operation response time with several instances of the application using the same Mitel OIG.

Number of MiVoice Call Managers- Impact on Mitel OIG

- There is a performance impact to the Mitel OIG when testing the Mitel OIG with ten MiVoice Business controllers compared to one MiVoice Business, for example. Application design and overall system deployment with Mitel OIG and MiVoice call managers must consider the number of MiVoice call manager, number of users and phones on each MiVoice call manager, number of trunks in the system, the call traffic, and the data an application reads from the Mitel OIG. The engineering limits defined in this document must be considered when viewing the whole MiVoice call manager system cluster.

Number of Applications Impact on Mitel OIG

- There is a noticeable performance impact to the Mitel OIG when testing the Mitel OIG with one application compared to ten applications, each application monitoring the same phones. System design and overall system deployment with Mitel OIG and MiVoice call managers must consider the number of applications, number of users, what services each application will use, and what data an application reads from the Mitel OIG. The engineering limits defined in this document must be considered when viewing the whole system solution.
- There was no noticeable performance impact to the Mitel OIG when an application is polling for events compared to when an application is using an event handler.
- An application should not continuously send **start monitor** commands, followed by **close monitor** commands for the same devices on the MiVoice call manager.

For example, an application should not send 30 "start monitor" commands, then 10 seconds later send 30 **close monitor** commands for the same devices, and then repeat the sequence over and over again for many hours. Such behavior will result in command congestion within the Mitel OIG due to time to execute monitor commands in MiVoice call manager.

MiVoice Call Manager

Application Impact on MiVoice Call Manager

- The Mitel OIG is designed to limit the impact of an application sending too many start monitor requests to a MiVoice call manager. An application should consider sending no more than 20 start monitor requests per second to one MiVoice call manager. An application must consider the events that result from setting monitors. When starting a large number of monitors on a large number of MiVoice call manager, an application should be lab tested to verify that the application can properly process the responses to setting monitors and the application's ability to process the large number of resulting events.
- Mitel OIG Data Access service read operations have no impact on a specific MiVoice call manager as the data is retrieved from the Mitel OIG server database.

MiVoice Call Manager Impact on Application

- All Mitel OIG applications using a MiVoice call manager are affected when the Mitel OIG loses communication with that MiVoice call manager. The Mitel OIG will automatically recover all monitors. The application will receive communication status events for each connection to each MiVoice call manager (connected and not connected). The typical scenario for losing a connection to a MiVoice call manager is a MiVoice call manager reset.
- If a MiVoice call manager does not respond to an application operation or command (e.g., "makecall") in the required time, the application receives an error message (MCD_TIMEOUT_ERROR) indicating that the command has timed out. An application should retry failed commands due to time out.

MiVoice Business IP Telephony Resiliency Support

The following problems can cause a user's telephone to go out of service:

- Telephone crashes/reboots (loss of power)
- Network glitch
- Telephone switching between primary and secondary controller
- MiVoice call manager crash/reboot/shutdown

To ensure continued phone service on a MiVB failure, MiVB supports the configuration of a secondary MiVB. The secondary MiVB provides call support for IP phones that have lost their primary MiVB. When a primary MiVB fails, an IP phone fails over to a secondary MiVB and continues to work. If an IP phone is in a call when the primary MiVB fails, the IP phone will not fail over to the Secondary MiVB until the call is disconnected.

OIG supports resiliency for the following:

- Device monitors on resilient IP phones
- Device monitors on resilient Hot Desk Users
- Device monitors on resilient Hot Desk Agents

To support resiliency, the OIG has to simultaneously create both primary and secondary monitors of a resilient DN. This means the OIG needs to know the secondary MiVB IP Address if the application is allowed to monitor devices on the secondary MiVB. This helps OIG to maintain the information of primary MiVB and secondary MiVB, so that it can switch over the monitor to secondary MiVB during fail over.

Note: When an application is monitoring resilient objects and the Mitel OIG connects to the primary MiVoice Business, the Mitel OIG caches in memory the primary MiVoice Business and secondary MiVoice Business IP addresses for the resilient objects. Hence, Mitel OIG must communicate with the primary MiVB at least once to allow IP resiliency to work. It learns the primary and secondary MiVB list on first connection to the primary MiVB, when at least one resilient DN is monitored.

Note: OIG resiliency behavior is consistent for all OIG-based applications including MiVoice Integrations

However, there are a few cases of unsupported scenarios as well to consider, where MiVB resiliency is not supported by OIG:

- Device monitors on non-resilient phones (phones that do not fail over to the secondary)
- Device monitors on line appearances (line appearances are resilient in a MiVB, but OIG does not support the resiliency for monitor on line appearances)
- Please refer to the *OIG Developer Guide: Call Control* for complete list of unsupported entities for which Mitel OIG does not support resiliency and for Resilient Scenario examples in detail.

Mitel OIG with MSL CPU and Memory Usage

- The Mitel OIG consumes less than 20% CPU
- The Mitel OIG consumes approximately 1-2 GB RAM
- The Mitel OIG (including MSL) uses approximately 6 GB of hard disk space

Application connections to Mitel OIG on MSL ISS

See Table 1 for the hardware platforms used when collecting this performance data.

#1 – 1 Application Can Connect to 100 MiVoice Business Controllers

Test Description: Set 50,000 5340 IP phone monitors; 500 5340 IP phones on each MiVoice Business.

#2 – 100 Applications Can Connect to 10 MiVoice Business Controllers

Test Description: Login 100 Applications and have each application make one call; 20 5340 IP phones on each of 10 MiVoice Business controllers (200 phones for 100 calls).

#3 – 1 Application to 1 MiVoice Business averages 100 Events per Second

Test Description: Set 5000 5320 IP phone monitors on one MiVoice Business. Generate 50,000 CPH on 2000 phones.

- Call Traffic Duration: 2 hours
- Call Duration for each Call: 20 secs
- Answer call duration: 2 secs
- Total events: 700,000
- Average Events per Second: 100

#4 – 1 Application to 10 MiVoice Business Controllers Averages 78 Events per Second

Test Description: Set 5000 5340 IP phone monitors on 10 MiVoice Business controllers (500 phones on each MiVoice Business). Generate 40,000 CPH on 2000 phones (200 phones on each MiVoice Business).

- Call Traffic Duration: 3 hours
- Call Duration for each Call: 20 secs
- Answer call duration: 2 secs
- Total events: 840,000
- Average Events per Second: 78.

#5 – 10 Applications to 10 MiVoice Business Controllers Averages 70 events /second

Test Description: Set 50,000 5340 IP phone monitors on 10 MiVoice Business controllers (5000 phones on each MiVoice Business 5000 monitors from each application). Generate 35,000 CPH.

- Call Traffic Duration: 4 hours
- Call Duration for each Call: 30 secs
- Answer call duration: 2 secs

- Total events: 980,000
- Average Events per Second: 70

Applications Connections to Mitel OIG on MSL Virtual

See Table 1 for the hardware platforms used in defining these guidelines.

Note that where MiVoice 5300 series phones are used, the results also apply to the MiVoice 6900 series phones.

#1 – 1 Application can Connect to 100 MiVoice Business Controllers

Test Description: Set 50,000 5340 IP phone monitors (500 5340 IP phones on each MiVoice Business).

#2 – 100 Applications can Connect to 10 MiVoice Business Controllers

Test Description: Login 100 Applications and have each application make one call (20 5340 IP phones on each of 10 MiVoice Business controllers – 200 phones for 100 calls.

#3 – 1 Application to 1 MiVoice Business Averages 58 Events per Second

Test Description: Set 5000 5320 IP phone monitors on one MiVoice Business. Generate 30,000 CPH on 4000 phones.

- Call Traffic Duration: 3 hours
- Call Duration for each Call: 20 secs
- Answer call duration: 2 sec.
- Total events: 630,000
- Average Events per Second: 58

#4 – 1 Application to 10 MiVoice Business controllers averages 68 Events per Second

Test Description: Set 5000 5340 IP phone monitors on 10 MiVoice Business controllers (500 phones on each MiVoice Business). Generate 35,000 CPH on 4000 phones (200 phones on each MiVoice Business).

- Call Traffic Duration: 2 hours
- Call Duration for each Call: 20 secs
- Answer call duration: 2 secs
- Total events: 490,000
- Average Events per Second: 68

#5 – 2 Applications to 1 MiVoice Business Averages 175 Events per Second

Test Description: Set 5000 5340 IP phone monitors on 10 MiVoice Business controllers (500 phones on each MiVoice Business). Generate 45,000 CPH on 4000 phones (200 phones on each MiVoice Business).

- Call Traffic Duration: 3 hours
- Call Duration for each Call: 20 secs
- Answer call duration: 2 secs
- Total events: 1,890,000
- Average Events per Second: 87 on each App.

#6 – 2 Applications to 10 MiVoice Business Controllers Averages 136 Events per Second

Test Description: Set 5000 5340 IP phone monitors on 10 MiVoice Business controllers (500 phones on each MiVoice Business). Generate 35,000 CPH on 4000 phones (200 phones on each MiVoice Business).

- Call Traffic Duration 4 hours
- Call Duration for each Call 20 sec
- Answer call duration 2 sec
- Total events 1,960,000
- Average Events / Second 68 on each App.

#7 – 2 Applications to 3 MiVoice Business Controllers Averages 145 Events per Second

Test Description: Set 1500 5340 IP phone monitors on 3 MiVoice Business controllers (500 phones on each MiVoice Business). Generate 75,000 CPH on 1500 phones. Call Traffic Duration 6 hours,

- Call Duration for each Call: 20 secs
- Answer call duration: 2 secs
- Total events: 304,029
- Average Events per Second: 72 on each App.

Applications Connections to Multi-Instance Mitel vOIG on MSL Virtual

See Table 1 for the hardware platforms used in defining these guidelines.

#1 – 400 Applications can connect to 1 MiVoice Business Controller Through 1 vOIG Instance – with 40 vOIG Instances on One Virtual Hardware Server

Test Description: 400 MiVoice Applications on one vOIG instance using one MiVoice Business controller (using both versions 7.0 and 7.0 SP1). Run call traffic of 10 calls per hour for each

application (i.e., 2000 calls per hour per vOIG instance). Set 400 IP phone monitors on each MiVoice Business controller. Have 40 vOIG instances using 40 MiVoice Business controllers for a total of 16,000 MiVoice Applications.

- Call Traffic Duration: 12 hours
- Total events: 6,735,000
- Average Events per Second: 47

System Impacts on Mitel OIG Performance

The overall performance of the Mitel OIG is affected by:

- System IP network performance
- Configuration of the MiVoice Business (for example, number of trunks, voice mail programming, number of IP Phones connected, size of MiVoice Business database, and so on).
- Variants of the MiVoice Business platform (MiVoice Business in MXe III, MXe II, CX II, CXi II, AX, EX, SMBC, MiVoice Business Virtual, MiVoice Business on ISS, MiVoice Business on public cloud AWS and Azure deployments)
- Call rate in the MiVoice Business (maximum 30,000 CPH)
- How the application is designed to send operations and process events from the Mitel OIG
- The workstation hardware used by the application
- Having OIG applications and MiTAI applications in the same MiVoice Business system cluster.
- How many applications are using the same Mitel OIG services.
- What Mitel OIG services each application uses
- Whether the application using advanced services or standard services

Appendix A: Calculating Events per Second

The following example explains the relationship between Mitel OIG events per second and call per hour capacity. This example is based on having one application to one Mitel OIG to one MiVoice Business. One application monitors 96 IP phones (48 phones making calls to another 48 phones). Each Monitor on a phone making a call receives four basic call events and each monitor on the receiving phone receives three call events. Each event maps to one IP Packet being sent to the Mitel OIG from the MiVoice Business. Depending on the types of monitors used and the scenario being executed more events may be generated.

ACTION	OPERATION	PHONE A GENERATED EVENTS	PHONE B GENERATED EVENTS
Phone A makes call	MakeCall	CallOriginatedEvent	
		CallDeliveredEvent	CallReceivedEvent
Phone B answers call	AnswerCall	CallEstablishedEvent	CallEstablishedEvent
Phone B hangs up	ClearCall	CallClearedEvent	CallClearedEvent

These three operations generate seven events for each call. We calculate the number of events the application will receive.

- Calculation: (3600 calls per hour / 3600 seconds in each hour) * (events per call) = number of events per second received by the application.

For example: (3600 calls / 3600 seconds) *(7 events) = 7 events per second.

Glossary

ACD	Automatic call distribution
API	Application-Programmer Interface
COS	Class of Service
DLL	Dynamic Link Library
ICP	IP Communications Platform
IP	Internet Protocol
IVR	Interactive Voice Response
MiTAI	Mitel Telephony Application Interface
MSL	Mitel Standard Linux
MSP	Media Service Provider
OIG	Open Integration Gateway
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
TDM	Time Division Multiplexing
VOIP	Voice over IP