

Mitel Open Integration Gateway

DEVELOPER GUIDE - FUNDAMENTALS

Release 4.1

September 2018



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).

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>.

**Mitel Open Integration Gateway
Developer Guide - Fundamentals
Release 4.1
September 2018**

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2014-2018, Mitel Networks Corporation
All rights reserved

INTRODUCTION	1
Mitel MiAccess.....	1
Mitel eDocs - Technical Documentation	2
Mitel OIG documentation.....	2
Mitel Solutions Alliance Web Portals	3
Technical Information	4
Technical Assistance.....	4
Other Assistance	4
MITEL OIG 4.1 CHANGES	5
MITEL OIG OVERVIEW	5
Web Service Messaging Formats (SOAP and REST)	8
Mitel OIG Session Management Service	9
Standard	10
Advanced	10
Mitel OIG Call Control Service	10
Standard Call Control.....	10
Advanced Call Control.....	11
Call Control Service Key Concepts	12
Mitel OIG Data Access Service	13
Standard Data Access.....	13
Mitel OIG Licensing	14
MiVoice Integrations	15
Mitel Certificate Server (MCS) Overview	18
MCS General Requirements	19
GETTING STARTED WITH MITEL OIG	21
First steps	21
Mitel Hosted Virtual Test Lab.....	21
Install Mitel OIG	21
Mitel Sample Applications.....	21
MiVoice Business configuration	22
Mitel OIG System configuration	22
MiContact Center Configuration	23
Troubleshooting and testing	24
MiVoice Business and Mitel OIG Connection Failures	24
MiVoice Business connection recovery.....	24

CREATING YOUR OWN APPLICATION	25
Example: WSDL in Visual Studio using C#	25
Example: WSDL in Visual Studio using Visual Basic	26
REST / JSON Data Access Web Service	27
MITEL CERTIFICATE SERVER ACCESS AND REQUESTS.....	29
Application Registration in MCS Access Control List (ACL)	29
Application Registration Request.....	29
Application Registration Request Approval	31
Registration Request Denial	31
Revoking Applications	31
ACL Retrieval.....	31
Mitel Certificate Request.....	32
Certificate Request Process	32
Certificate Request Approval	34
Certificate Request Denial	34
Regenerating a Certificate for an Application	35
GLOSSARY	37

Introduction

The Mitel OIG is a web server that provides a single access point to web services available within a Mitel system. The Mitel OIG runs on the Mitel Standard Linux (MSL) operating system and can be deployed as an MSL software blade through the Mitel AMC licensing server, or as a virtual appliance downloaded from **MiAccess > Software Download Center**.

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

The Mitel OIG provides web services by integrating with a Mitel system (MiVoice call manager cluster or single MiVoice call manager node and Mitel applications). Mitel OIG supports the following web services:

- Session management service
- Call control services
- Data access services

In general, software developers are required to join the Mitel Solutions Alliance (MSA) at one of the Developer Advanced membership levels in order to develop or modify Mitel OIG-based applications.

Software developers also have the option to evaluate the Mitel OIG development capabilities in advance of joining MSA, either by ordering the Mitel OIG 60-Day Trial (for Mitel end-customers – P/N 54005933), or by requesting a one-month reservation on the Mitel OIG Hosted Virtual Lab (for prospective commercial developers, see <https://www.mitel.com/developer/join-msa>).

The following resources are available to support developers working with Mitel OIG.

- MiAccess
- Mitel eDocs - Technical Documentation
- Mitel Open Integration Gateway Training
- Technical Assistance

Mitel MiAccess

Mitel MiAccess (connect.mitel.com) is a web portal for information and resources about Mitel solutions, sales, support, training, partners, and more.

The Mitel corporate website, <http://www.Mitel.com>, also provides the link to MiAccess:

- In the ribbon along the top right section of the Mitel.com page, click **Login**.
- Log in to MiAccess.

Mitel eDocs - Technical Documentation

The Mitel eDocs Technical Documentation website provides the latest versions of the technical publications for Mitel products and solutions. Documents are organized by release under each product or solution.

The eDocs URL is <http://edocs.mitel.com/>.

eDocs can be accessed from the left sidebar after logging in to MiAccess.



Note: You must have a MiAccess account user name and password to view and download technical documentation.

Mitel OIG documentation

This document, *Mitel OIG Developer Guide - Fundamentals*, describes the Mitel Open Integration Gateway (Mitel OIG) and provides an overview of the Mitel OIG services for software developers creating applications that access a Mitel OIG.

The following Mitel OIG documentation is available on the Mitel Customer Documentation website (eDocs):

- Mitel OIG Product Bulletin
- *Mitel OIG Installation and Maintenance Guide*: This document provides details and instructions for installing the Mitel OIG and licensing it for applications and services.
- *Mitel OIG Engineering Guidelines*: The Engineering Guidelines provides guidance on network and system level requirements and performance.
- *Mitel OIG Developer Guide - Fundamentals (this guide)*: The fundamentals guide introduces the Mitel OIG application developer environment and general information that applies to developing applications relative for any of the Mitel OIG web services. This guide describes how to register an application with Mitel and request a Mitel certificate to be used in the application. The fundamentals document also includes a summary of the changes introduced for this release.



Note: Mitel recommends that you become familiar with the contents of this guide, the *Mitel OIG Developer Guide - Fundamentals*, before beginning to create Mitel OIG applications.

- *Mitel OIG Developer Guide - Session Management Service*: This developer guide provides application developers detailed requirements for working with the Session Management Service. This guide describes how an application opens a communication session with the Mitel OIG. Applications use this one communications session to access all other web services offered by the Mitel OIG.
- *Mitel OIG Developer Guide – Call Control Service*: This developer guide describes the Call Control Service details needed for creating applications that monitor and control devices and features configured within MiVoice call manager nodes.

- *Mitel OIG Developer Guide - Data Access Service*: This developer guide describes the Data Access Service details needed for creating applications that receive MiVoice call manager Data.
- *Global Call ID Developer Guide*: This guide provides guidelines for Mitel OIG applications that are written to track calls in a Mitel MiVoice call manager system using a system wide call ID. The guide is available on the InfoChannel MSA portal (under OIG).
- *Virtual Appliance Deployment Solutions Guide*: This guide provides engineering guidelines for deploying Mitel virtual appliances and applications in a VMware virtual infrastructure. The guide is available on the Mitel Customer Documentation (eDocs) website under the **Solutions Guides & Blueprints** heading - Virtual Appliance Deployment Solutions Guide.
- Mitel Standard Linux (MSL) documentation
- MiVoice Business documentation

The following MiVoice Integration guides describe administering and using the MiVoice Integration applications for Salesforce and Google. The MiVoice Integration documents are available on the Mitel eDocs website.

- *MiVoice Integration for Salesforce Administration Guide*
- *MiVoice Integration for Salesforce User Guide*
- *MiVoice Integration for Google Administration Guide*
- *MiVoice Integration for Google Quick Reference Guide*

Mitel Solutions Alliance Web Portals

MSA developer resources are accessed through the central Mitel MiAccess portal (connect.mitel.com) and InfoChannel MSA. 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 <http://www.mitel.com/mitel-connect-support-request>.

MSA account credentials must remain active in order 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 connect.support@mitel.com with your name, company name, and MSA Membership Account number to request reactivation, and also remember to cc MSAInfo@mitel.com on your request so that MSA can verify your MSA membership status for the portal support team. 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 completing the online form at <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 selecting **Login** at the top right of the page at www.mitel.com, or directly at <https://connect.mitel.com/connect/>.
- Select the InfoChannel button in the left sidebar.

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 completing the online form at <https://www.mitel.com/developer/join-msa>.

The TechCentral Tracker and the TCT User Guide for MSA Developers is 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 TCT-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 4.1 changes

The following summarize the changes included in the Mitel OIG 4.1 release.

- In the **Network Elements** tab of the Mitel OIG page, MiVoice Business type now has two additional fields “Login id” and “Password”.

Mitel OIG 4.1 supports authentication-based OIG connection to MiVB 9.0. This feature improves the security mechanism between Mitel OIG and MiVB when Mitel OIG attempts to connect to MiVB. Hereafter, when authentication is enabled, the Mitel OIG is authenticated using Login ID and Password provided in the above mentioned new fields.

Authentication can be enabled or disabled by the MiVB System Administrator using the new Shared System Option ‘CTI Application Authentication’ (by default, this option is disabled). The MiVB Administrator must also add an entry for the application with its respective Login ID and password in “User Authorization Profiles” form, against which OIG needs to be authenticated.



Note: Both ESM forms mentioned above must be sharable in a cluster, to support resiliency. The forms are by default within sharing scope of all network elements in a cluster.

After the option is enabled in MiVoice Business, the OIG Administrator must provide the Login ID and Password in the respective fields of “MiVoice Business” in Network Elements to establish a successful authenticated connection to MiVB

- In CallReceivedEvent, the Event Attribute Group Distribution Type has an additional distribution type, RINGGRP_LGMR to support MiVB 9.0 Last Group Member Routing feature for Ring Groups.

This feature allows a caller to connect a caller to the same Ring Group member that previously attended the call, when the caller has called back on the Ring Group from same CgPN or ANI within a specified duration between the calls.

- Bug Fixes: See the Mitel OIG 4.1 Release Notes for details.

Mitel OIG Overview

The Mitel Open Integration Gateway (Mitel OIG) is a web server that provides each Mitel OIG application a single point of access to web services available within a Mitel communication system. The Mitel OIG provides a service-oriented architecture. A Mitel OIG application opens a communication session with a Mitel OIG by logging in (i.e., sending a service

operation or request to the Mitel OIG). After the Mitel OIG application is authenticated and authorized, the application can use this one communication session to access all Mitel OIG web services the application is authorized to use.

The Mitel OIG is installed on the Mitel Standard Linux (MSL) operating system and can be deployed as an MSL software blade through the Mitel AMC licensing server, or as a virtual appliance downloaded from **MiAccess > Software Download Center**.

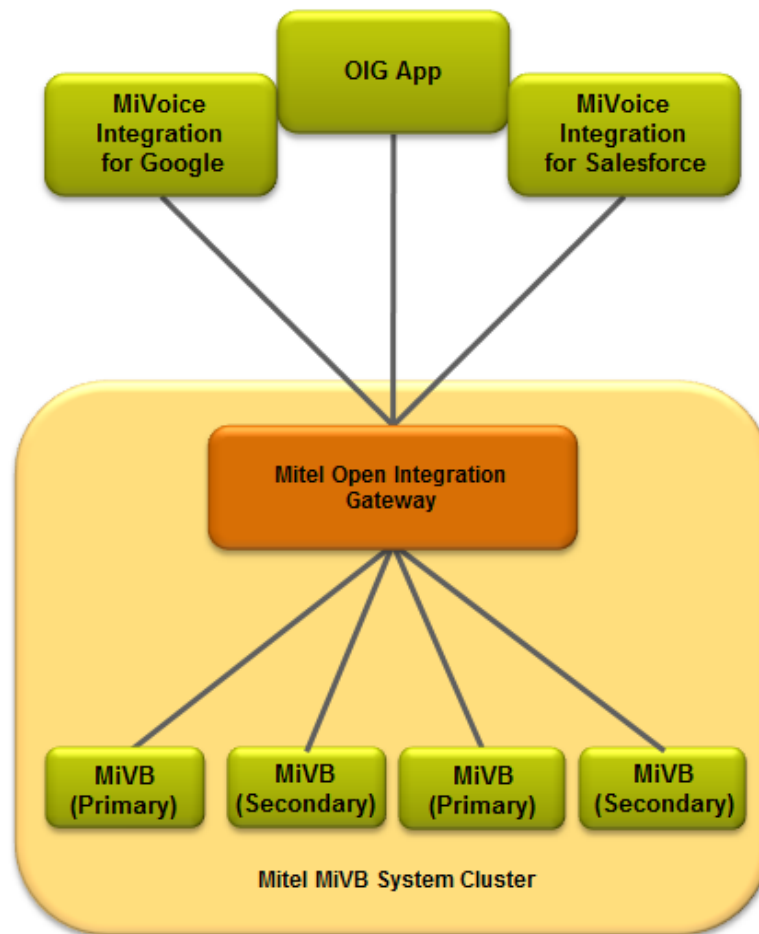
The Mitel OIG allows applications to access features and functionality offered by a Mitel MiVoice call manager system cluster (see Figure below).



Note: The Mitel OIG can communicate with a single MiVoice call manager or a cluster of MiVoice call manager instances. When there are two or more MiVoice call manager instances, the MiVoice call manager instances must be configured in a cluster. Mitel Open Integration Gateway cannot communicate with more than one MiVoice call manager cluster. The Mitel OIG assumes that the directory number (DN) of a Mitel phone is unique in the MiVoice call manager system cluster; two Mitel phones in the system cannot have the same DN.

Mitel OIG can also communicate with a single MiContact Center server. There can be one (only) MiContact Center Server connected to a Mitel OIG server.

Figure 1: Mitel OIG system configuration

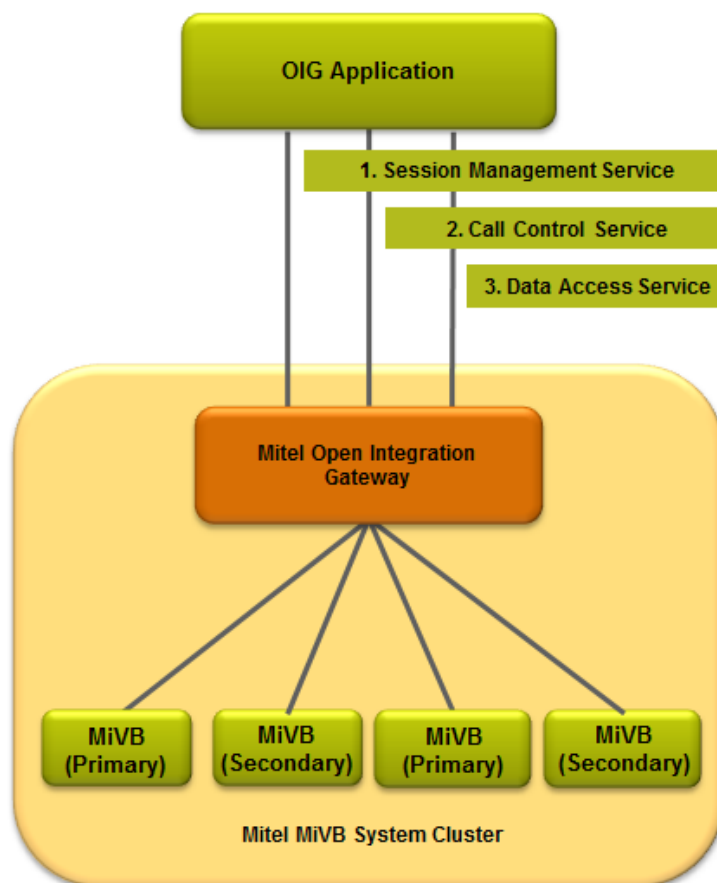


The Mitel OIG allows applications to submit requests using web service operations. The Mitel OIG processes each request and provides a response. Some requests result in a state change in the Mitel communication system and the Mitel OIG then initiates an event for the application. The Mitel OIG supports the following web services:

- **Session Management service** – Open communication session with Mitel OIG for services.
- **Call Control service** – Control and monitor CTI behavior in a Mitel communication system.
- **Data Access service** – Register for MiVoice Business configuration data change notifications and read MiVoice Business configuration data.



Note: Mitel also offers two applications that use the Mitel OIG; MiVoice Integration for Salesforce and MiVoice Integration for Google.

Figure 2: Mitel OIG application, server, and services relationship

The following sections provide more details about developing applications for Mitel OIG.

- Web Service Messaging Formats
- Mitel OIG Session Management Service

Web Service Messaging Formats (SOAP and REST)

Mitel OIG applications can access Mitel OIG services using two different web service messaging formats for Mitel OIG services.

- SOAP / XML
- REST / JSON

SERVICE	SOAP / XML	REST / JSON
Session Management Service	√	√
Call Control Service	√	x
Data Access Service	x	√

A Mitel OIG application can open a communication session (log in) with a Mitel OIG using either SOAP / XML or REST / JSON.

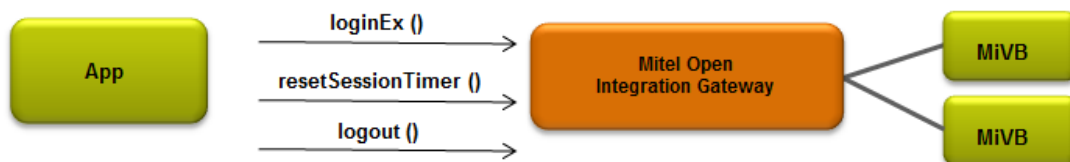
A Mitel OIG application must use SOAP / XML when accessing the Mitel OIG Call Control service. After being logged in using SOAP / XML, an application is allowed to use the Data Access service with REST / JSON.

A Mitel OIG application must use REST / JSON when accessing the Mitel OIG Data Access service. If an application only requires the Data Access Service, the application can log in using REST / JSON. If the application requires both Call Control service and Data Access service the application must log in using SOAP / XML.

Mitel OIG Session Management Service

Each Mitel OIG application uses the Mitel OIG session management service to communicate with the Mitel OIG. The session management service describes how an application logs in, logs out, and maintains a Mitel OIG communication session keep-alive timer. The application must reset a keep-alive timer before 10 minutes or the Mitel OIG will terminate the communication session.

Figure 3: Session Management



To log in to a Mitel OIG, each application needs the following parameters (Applications requiring advanced operations must also provide a Mitel certificate):

- company name
- application name
- application password
- local password
- version

The first three parameters are defined by the application developer when registering their application with Mitel. These three parameters do not change after they have been defined in the application. The fourth parameter (local password) is site-specific.

A Mitel OIG administrator uses the Mitel OIG Admin UI to create a local password specific to each application and a specific Mitel OIG. The local password controls the access of each individual application to each individual Mitel OIG. Each application that uses a Mitel OIG must provide a mechanism for a user to enter the local password and then the application must include the local password in the Mitel OIG loginEx operation, along with the other three parameters mentioned above.

The fifth parameter is a version number. The Mitel OIG application needs to provide the version in the application login request (loginEx operation). The version parameter allows the Mitel OIG to determine the service version used by the application. See the Mitel OIG Developer Guides for more details on Mitel OIG services, operations and events.

The Mitel OIG Session Management Service allows an application to open a communication session with a Mitel OIG. Once the communication session is established and the Mitel OIG application is authenticated and authorized, the application can use the one communication session to access all Mitel OIG web services.

By providing or not providing a Mitel Certificate during log in, the application indicates what overall type of web services the application needs to use with the Mitel OIG. The Mitel OIG offers two overall types of web services.

Standard

This type provides the basic operations within Mitel OIG services. Standard operations focus on a system user: what an application needs to control and monitor what a user does within the Mitel system. To request this web services type, an OIG application must be registered on the Mitel Access Control List (ACL). See the *Mitel OIG Installation and Maintenance Guide*.

Advanced

This type provides more sophisticated behavior within Mitel OIG services. Advanced operations focus on overall system behaviors for many users. Advanced web services include operations offered in the Standard web services type. To request the Advanced web services type, a Mitel OIG application must be registered on the Mitel Access Control List (ACL), and a Mitel Certificate must be obtained. See the *Mitel OIG Installation and Maintenance Guide* for more details about requesting an application account and requesting a Mitel certificate. See the Mitel OIG Developer Guides for more details on Mitel OIG services, operations, and events.

Mitel OIG Call Control Service

The Mitel OIG provides a Call Control service to control and monitor CTI functionality within a MiVoice call manager system. The Call Control service is offered based on the web services type selected by the Mitel OIG application (i.e., when application opens a communication session with the Mitel OIG). There are two web services types.

Standard Call Control

The standard call control service allows applications to monitor and control the telephony activity of Mitel physical and logical devices (devices programmed or configured in Mitel MiVoice call manager instances) including IP phones, Personal Ring Groups and line appearances on multi-line phones. The Mitel OIG Standard Call Control Service allows applications to control and monitor a Mitel desktop phone in a way that is similar to a user manually controlling the phone.

Advanced Call Control

The advanced call control service includes third-party call control capabilities and offers a full suite of functionality from simple call control to contact center monitoring and control.

Advanced Call Control Service provides monitoring and control of MiVoice call manager functions, e.g., Hot Desk Agent login (Internal and External), Trunking, Ring Groups, Hunt Groups, ACD2Path, ACD Express.

Control relates to functions not normally associated with a specific desktop phone user. Support for MiVoice call manager level monitoring (e.g., all conferences within a MiVoice call manager) is included. Setting device features like phone message waiting lamp and auto answer are also provided in Advanced Call Control.

The Mitel OIG Call Control service is defined by Web Service Description Language (WSDL) files provided by Mitel. The WSDL and XSD files describe the service, its commands (operations), its responses, status events, and data definitions. When importing the WSDL files into a development environment, operation and parameter choices are generated automatically for each operation.

The Mitel OIG Call Control service is provided using SOAP and XML over HTTPS. Applications do not require software from Mitel to communicate with a Mitel OIG. An application does not need to integrate or compile in any Mitel code. Application developers are free to choose a programming language, a software development environment, an operating system, and a hardware platform for their application. The web service model decouples the Mitel OIG software from the application; only the WSDL and XSD files are needed.

The Mitel OIG Call Control service is defined using a request, response, and then event model. An application sends a request to activate a service operation and the Mitel OIG responds with success/failure and return data. The application needs to check for the success or failure of each operation. Operations trigger changes in the Mitel OIG and the Mitel MiVoice call manager system. The changes are reported back to the application using events. An application must check the events returned following an operation before performing more operations. An application can poll the Mitel OIG for events or provide an asynchronous reporting mechanism (register an event handler with the Mitel OIG so that the Mitel OIG can send events to the application asynchronously; this reporting mechanism is described in the Mitel OIG Developer Guides.

Applications open monitors on devices and then receive events information about device state changes. For example, if an application opens a monitor on an IP Phone, the application will receive events when the IP Phone receives a call or makes a call. Opening a monitor also means the application is able to control the device. For example, an application can initiate a call on a monitored phone without any action by the phone user. Applications can also open monitors on phone features and receive events about phone feature state changes (e.g., phone Do-Not-Disturb (DND) status).

The Mitel OIG Call Control service uses a device model; not a user model or call model. An application receives call events, feature events, ACD events and system events. To allow an application to track a call in a MiVoice call manager system cluster, the Mitel OIG provides a Global Call ID in call status events. See the Global Call ID Developer Guide on the InfoChannel MSA web portal for more information.

To use the Mitel OIG Call Control service, an application must have information about the Mitel MiVoice call manager system (i.e., MiVoice call manager IP addresses, IP Phone prime line numbers, IP Phone line appearance button numbers, hot desk user numbers, etc.). The information required is defined in the Mitel OIG Developer Guides.

When using Mitel OIG, an application must provide the IP address of each MiVoice call manager that provides devices to be monitored. The Mitel OIG must connect to a MiVoice call manager to control and monitor the physical and logical devices configured in that MiVoice call manager. An application cannot connect to MiVoice A to monitor and control a device configured in MiVoice B. MiVoice Business A has no knowledge of the device on MiVoice B.



Note: To enable Mitel MiVoice Integration for Salesforce and MiVoice Integration for Google, the Mitel OIG provides web services using REST and JSON over HTTPS. The operations provided to the MiVoice Integration applications are a subset of the operations provided by SOAP and XML over HTTPS.

Call Control Service Key Concepts

Mitel OIG Object IDs – The Mitel OIG allows an application to request an Object ID for each object of interest (i.e., MiVoice call manager, IP Phone prime line, IP Phone line appearance button, hot desk user). The Mitel OIG provides the Object ID to the application. The application stores and uses the Object IDs in commands and for processing events. When an application is required to monitor an object, the application initiates a monitor operation (request) with the related Object ID.

Mitel OIG Operations – Each Mitel OIG service offers an application many possible operations. Operations are requests to the Mitel OIG. For example, an application requests an Object ID for a specific MiVoice call manager node using the `getIcpId` operation. The Mitel OIG Call Control Service is divided into Standard and Advanced operations. The Advanced operations offer more sophisticated control and monitoring. Therefore, a deeper knowledge of MiVoice call manager behavior is required for use of the advanced operations. A developer must specifically request the use of Standard or Advanced services when requesting an application account from Mitel. Refer to the *Mitel OIG Installation and Maintenance Guide* for instructions for requesting an application account from Mitel when registering OIG applications with Mitel.

Mitel OIG Monitors – To control and monitor an object (e.g., IP Phone), the application must open a monitor (i.e., the application initiates a monitor operation (request) with an IP Phone prime line Object ID). Once the application has created a monitor, the application can then send requests, get responses, and receive events related to the monitored object (i.e., IP Phone prime line, IP Phone line appearance button, hot desk user).

Mitel OIG Events – The Mitel OIG informs an application about status and state changes in objects (e.g., IP Phone prime line) using events. Each event has a name and associated event data. Each event also has a class name that defines the event data to expect. The event data provides specific details about monitored objects. An application uses events to confirm that initiated requests were actually completed and to determine what requests to initiate next.

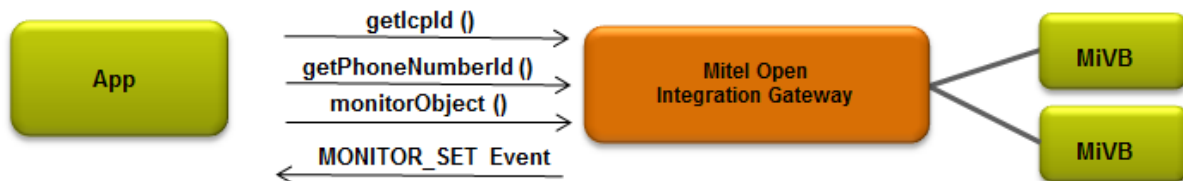
Mitel OIG Event Data – Each Mitel OIG event has data. The data provided depends on the event name and class. Events in the Call Event Class also have state and cause. The event

state defines the state of the object being monitored. The event cause defines why the event was reported. All events contain data about the object being monitored. For example, events related to a monitor on an IP Phone Prime line contain the IP Phone number, IP Phone type, and name associated with the IP Phone number. The application needs to process the XML data provided in an event based on event name, class, and in some cases, state and cause. A Mitel OIG event also has a time stamp. The time format is time_t. This time stamp counts the seconds elapsed since 00:00 hours, Jan 1, 1970 UTC. The time applied is from the Mitel OIG server and not from an individual MiVoice call manager controller.



Note: The Event Time in Mitel OIG events is a 64-bit Integer (e.g., a MONITOR_SET event has an event time of 1349360583326). The time is a millisecond value that is an offset from the Epoch, January 1, 1970 00:00:00.000 GMT.

Figure 4: Create IP phone monitor



Mitel OIG Data Access Service

The Mitel OIG Data Access Service provides a generic SQL like interface to the Mitel OIG PostgreSQL database using a REST/JSON messaging interface. Most views are read-only, but write features are offered for a small subset of views.

The data in the Mitel OIG PostgreSQL database is provided by the MiVoice Business nodes in the Mitel MiVoice Business communication system. To receive the MiVoice Business data, the Mitel OIG server must be added as a Network Element to one of the MiVoice Business nodes in the Mitel MiVoice Business communication system. Instructions for adding a Mitel OIG server to a MiVoice Business system are contained in the following sections.



Note: The Mitel OIG 4.1 Data Access service requires MiVoice Business 8.0+ and MSL 10.5.15+. MiVoice Business 9.0 is recommended

There are two data access service types:

Standard Data Access

The standard data access service allows applications to read and get change notifications on MiVoice Business configuration data related to Mitel physical and logical devices (devices programmed or configured in Mitel MiVoice Business) including IP phones, Personal Ring Groups and line appearances on multi-line phones. The Mitel OIG Standard Data Access Service allows applications to retrieve MiVoice Business data that is needed when using other Mitel OIG services (i.e., Application needs to know DN of MiVoice Business phone to create a monitor using Mitel OIG call control service).

The Mitel OIG Data Access service is defined in the *Mitel OIG Data Access Developer Guide*. This document describes the service and its commands (operations), responses, status events, and data definitions.

The Mitel OIG Data Access service is provided using REST and JSON over HTTPS. Applications do not require software from Mitel to communicate with a Mitel OIG. An application does not need to integrate or compile in any Mitel code. Application developers are free to choose a programming language, a software development environment, an operating system, and a hardware platform for their application. The web service model decouples the Mitel OIG software from the application.

The Mitel OIG Data Access service is defined using a request, response, and event model. An application sends a request to activate a service operation and the Mitel OIG responds with success or failure and return data. The application needs to check for the success or failure of each operation. Operations trigger changes in the Mitel OIG and the Mitel MiVoice Business system. The changes are reported back to the application using events. An application must check and process the events returned when registering for change notifications on the Mitel OIG server database. An application must poll the Mitel OIG for events related to data change notifications. The polling mechanism is described in the Mitel OIG Developer Guides.

Applications read Mitel OIG server data (configuration data collected from the MiVoice Business communication system) and then request data change notifications. For example, if an application reads phone view data and requests data change notifications on this view, the application will receive events when data in the phone view changes.

To use the Mitel OIG Data Access service, an application must have information about the Mitel MiVoice Business system (i.e., MiVoice Business IP addresses). The required information is defined in the Mitel OIG Developer Guides.

When requesting configuration data using Mitel OIG, an application must provide the IP address of a specific MiVoice Business node that will provide the data. The Mitel OIG must connect to the MiVoice Business communication system that has the MiVoice Business node to be able to retrieve the configuration data in that MiVoice Business node.

Mitel OIG Licensing

Licensing and delivery of the Mitel OIG software is similar to licensing and delivery of other Mitel software applications:

- Purchased by the Mitel customer (through their reseller)
- Downloaded and licensed via the Mitel Licensing AMC portal
- Deployed on Mitel Standard Linux (MSL)
- Available in physical and virtual versions.

The Mitel OIG software can be deployed as a Mitel MSL blade through the Mitel AMC licensing server, or as a virtual appliance downloaded from **MiAccess** > Software **Download Center**.

The Mitel OIG utilizes a Mitel Certificate Server (MCS) and Access Control List (ACL) to ensure that only authorized applications connect to a customer Mitel OIG. Refer to the *Mitel OIG Installation and Maintenance Guide* for more information.

The Mitel OIG hardware platform must have an Internet connection to allow the Mitel OIG software to connect to the Mitel AMC server to obtain application licenses. The Mitel OIG hardware platform also requires an Internet connection to allow the Mitel OIG software to connect to the MCS to obtain the latest ACL for confirmation of authorized applications.

The Mitel OIG is licensed to allow connected applications to use Web Services provided by Mitel MiVoice call manager instances.

The AMC licenses for the Mitel OIG are shared by all connected applications. Separate licenses are required for the MiVoice Integration for Salesforce and the MiVoice integration for Google.

The AMC licensing for the MiVoice call manager is separate from the AMC licensing for the Mitel OIG.



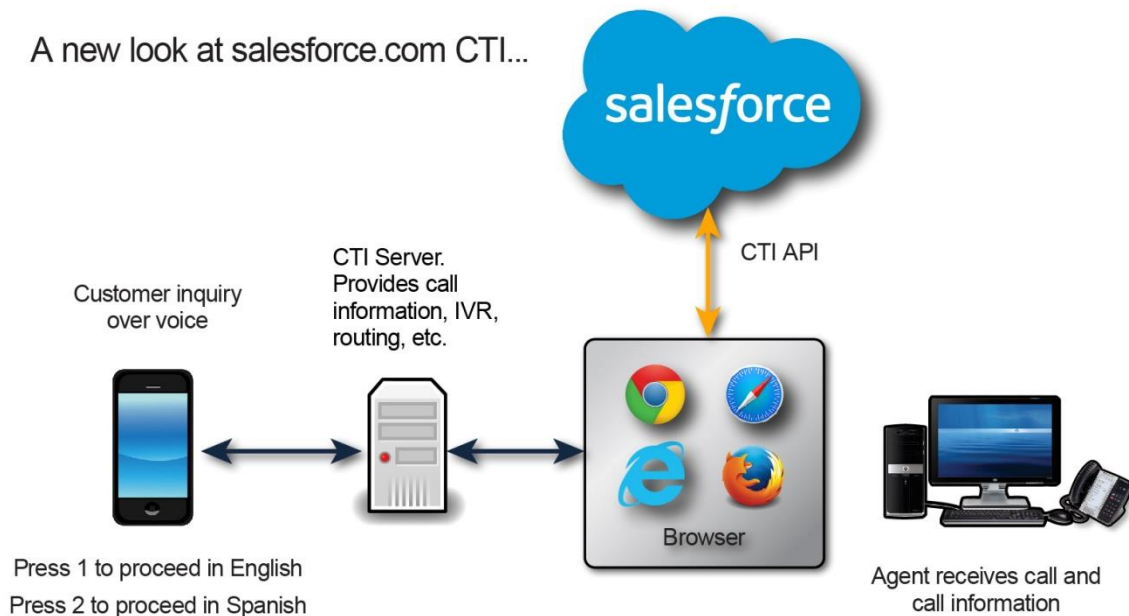
Note: Application Developers are responsible for communicating to Mitel Resellers and end customers the type of Mitel OIG application (Standard or Advanced) they provide. Application Developers are also responsible for communicating the number of Mitel OIG licenses typically required by their application. Refer to the *Mitel OIG Installation and Maintenance Guide* for more information about licensing.

MiVoice Integrations

The MiVoice Integrations are turn-key OIG-based applications that provide CTI functions (make call, answer call, transfer call, conference call, hold and retrieve call, and redirect call) to web browser users. When a user logs in, a web browser UI also displays a MiVoice UI. The MiVoice Integrations provide call-related features such as incoming call alert, access to a contact list, and ability to create a call log. The MiVoice Integrations use the Mitel OIG Call Control service to provide call features within each web browser UI. Refer to the MiVoice Integrations Guides for more details:

- *MiVoice Integration for Salesforce Administration Guide*
- *MiVoice Integration for Salesforce User Guide*
- *MiVoice Integration for Google Administration Guide*
- *MiVoice Integration for Google Quick Reference Guide*

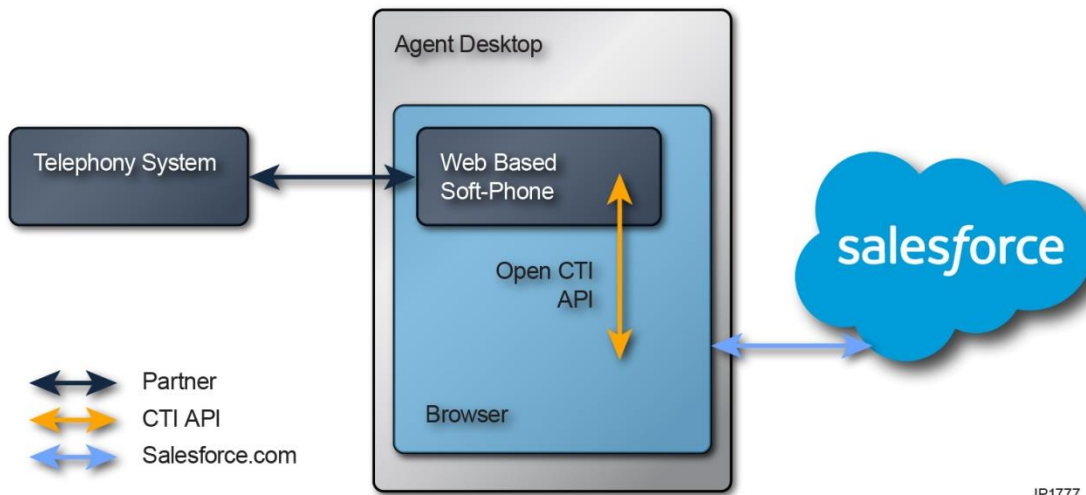
Figure 5: MiVoice Integration for Salesforce



IP1776

In this figure, the CTI server can be tightly integrated MiContact Center.

Figure 6: MiVoice Integration for Salesforce logical architecture



IP1777

Figure 7: MiVoice Integration for Google

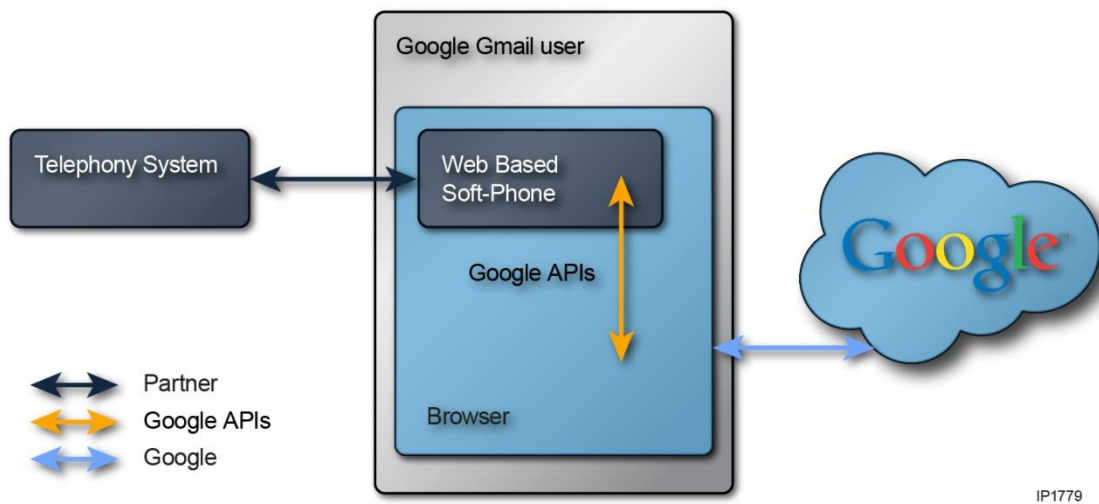
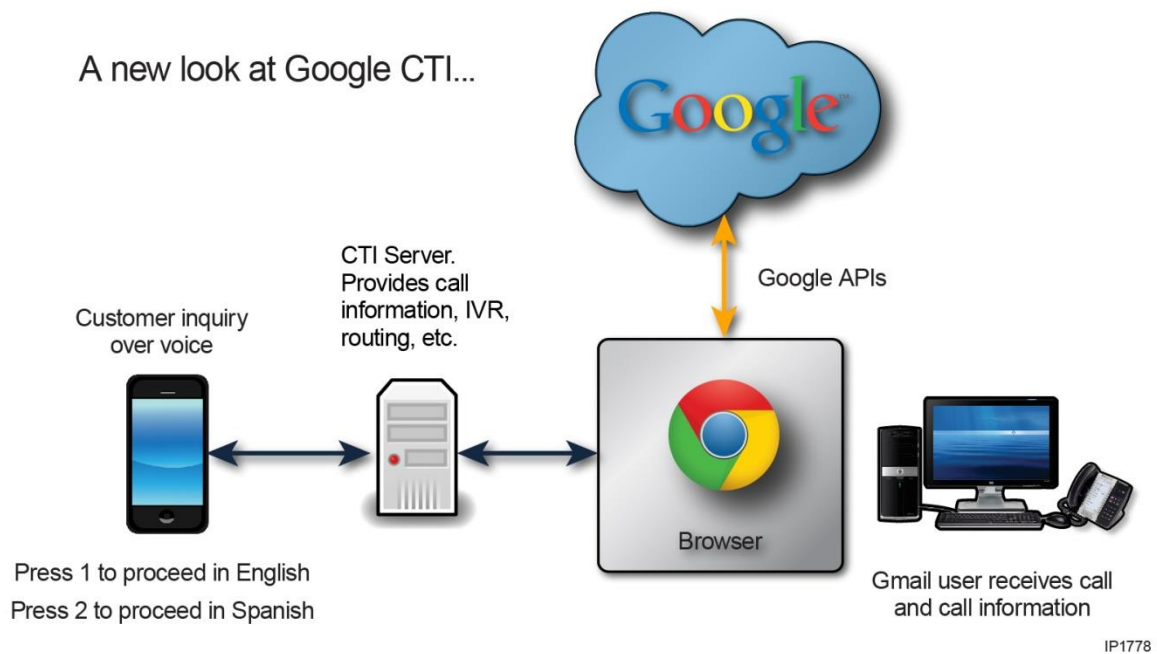


Figure 7: MiVoice Integration for Google logical architecture



Mitel Certificate Server (MCS) Overview

Before using the Mitel OIG, an application developer (MSA member) must register their applications with the Mitel Certificate Server (MCS). The MCS is accessible through the Internet. The Mitel OIG uses an Access Control List (ACL) from the MCS to identify approved applications. An application must be registered with the MCS and in the ACL before the application can communicate with a Mitel OIG.

The Mitel Certificate Server (MCS) also allows an application developer to request a Mitel certificate for their application. An application must have a Mitel certificate to use Mitel OIG Advanced Services like the Advanced Call Control Service.

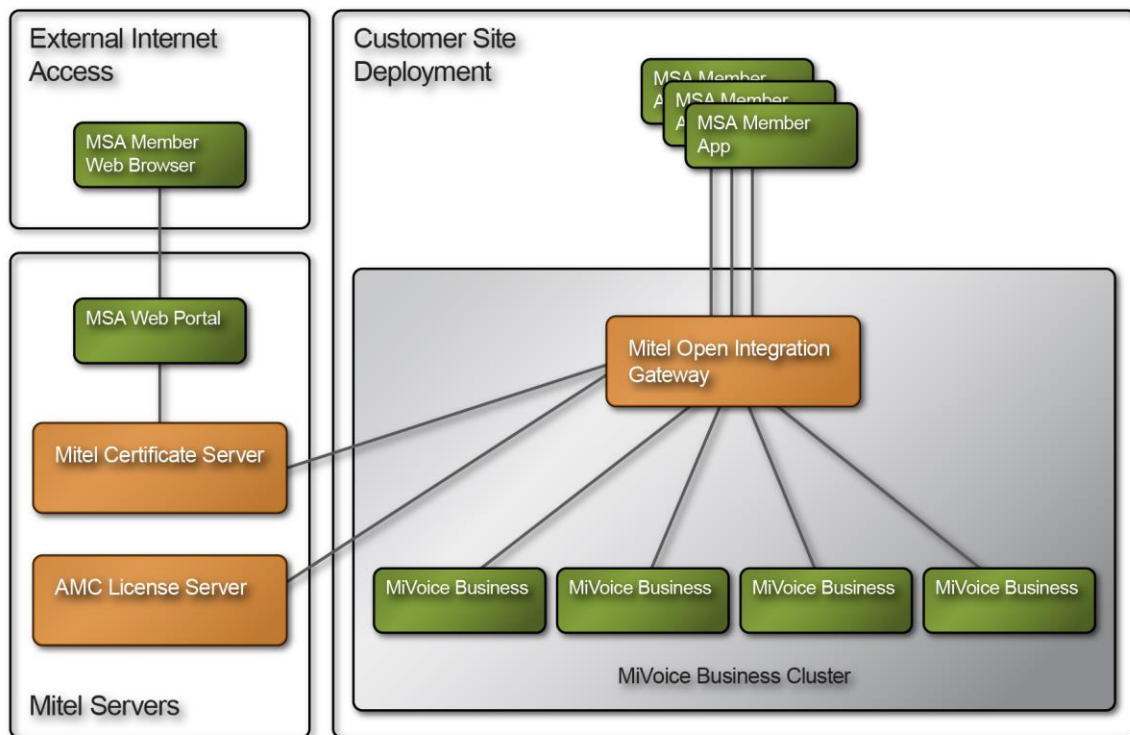
Before an MSA Authorized application can communicate with a deployed Mitel OIG, the following is needed:

- For Standard Mitel OIG communication, an MSA Authorized User (MSA member) must register a company name, application name and application password with Mitel. This registration information is added to the Mitel Access Control List (ACL) in the MCS.
- For Advanced Mitel OIG communication, an MSA Authorized User (MSA member) must request a Mitel Certificate. As part of the certificate the user also registers a company name, application name and application password with Mitel. This registration information is added to the ACL in the MCS. The Mitel Certificate is provided to the MSA Authorized User (MSA member) by the MCS.



Note: DO NOT use special characters like comma, \$, #, @, and so on, in any of the fields, while registering applications with the Mitel Certificate Server (MCS).

When requesting Mitel OIG access, an MSA Authorized User logs into MiAccess using their account credentials. In this case, the user must be an active MSA member and have an MSA account number (i.e. Mitel SAP number). Infochannel MSA portal web links direct the MSA Authorized User to web forms provided by the MCS. Refer to the *Mitel OIG Installation and Maintenance Guide* for details.

Figure 8: Mitel Certificate Server

IP1763

MCS General Requirements

The MCS can be accessed by MSA Authorized Users (MSA members or prospective Virtual Lab Users). Only MSA members can request Mitel Certificates or request application registration to the MCS ACL. Prospective MSA members can request a time slot on the Mitel Hosted Virtual Test Lab, after authorization by MSA.

MSA Authorized Users login to the InfoChannel MSA portal using their MiAccess account credentials. See section Mitel Certificate Server Access and Requests. The following web browsers are supported:

- Microsoft Windows Internet Explorer
- Google Chrome
- Firefox

If a Mitel Certificate request is approved, the MCS e-mails a Mitel Certificate and request approval to the MSA Authorized User and registers the MSA Authorized application in the ACL stored in the MCS.

If an application registration to ACL request is approved, the MCS e-mails the MSA Authorized User notifying approval and registers the MSA Authorized application in the ACL stored in the MCS.

The MSA Administrator has the ability to revoke an MSA Authorized application. If an application is revoked, the MCS will indicate the application revocation in the ACL. A revoked

application is denied access to all Mitel OIGs. An e-mail is sent to the application owner (MSA member) if an application is rejected. The e-mail will include instructions on how to contact MSA for more information.

Getting Started with Mitel OIG

Using the Mitel OIG is made easy with web services. The Mitel OIG web services are defined using WSDL files or through the use of REST / JSON. The Internet provides all the material needed to learn about web servers, web services, WSDL, SOAP / XML, REST / JSON, available toolkits, free development environments, tools, and sample code. This section provides information about how to get started and how to develop applications for the Mitel OIG.

First steps

The list below provides the recommended first steps to using the Mitel OIG:

1. Read the Mitel OIG user documentation.
2. Complete the Mitel OIG online training and certification process.
3. Use the Mitel hosted virtual test lab for the Mitel OIG (optional).
4. Install the Mitel OIG software.
5. Use Mitel OIG sample applications to execute different Mitel OIG service scenarios.
6. Create your own application.

Mitel Hosted Virtual Test Lab

Mitel offers Mitel OIG application developers access to a virtual test lab. The test lab allows developers to use provided sample applications to investigate how the Mitel OIG works. Developers are also allowed to create their own applications and test them against the Mitel OIG. The test lab has a predefined, ready-to-use configuration for ease of use. The Hosted Virtual Lab is intended for evaluation of the OIG platform and development environment, but it is not intended as a remote testing facility. Upon joining MSA, members are expected to establish an in-house Mitel OIG lab to meet their ongoing development and testing requirements

Refer to the *Virtual Test Lab User Guide* on the MSA web portal for more information.

Install Mitel OIG

When an application developer is ready to start using the Mitel OIG, the developer must obtain the Mitel OIG software from Mitel. Refer to the *Mitel OIG Installation and Maintenance Guide* for instructions on how to license and install the software.

Mitel Sample Applications

Mitel offers several sample applications for the Mitel OIG. The sample applications are very easy to install and use. Mitel OIG sample applications are available via the MiAccess > Software Download Center and InfoChannel MSA web portals, in the Mitel OIG Sample Application Package.

MiVoice Business configuration

A Mitel OIG can communicate with one or more MiVoice Business instances (maximum 250). To monitor and control phones on a specific MiVoice Business instance, the application must provide the IP address of a specific MiVoice Business instance.

The Mitel OIG can communicate with a single MiVoice Business instance or a cluster of MiVoice Business instances. When there are two or more MiVoice Business instances, the MiVoice Business instances must be configured in a cluster. Mitel OIG cannot communicate with more than one MiVoice Business cluster.

Each MiVoice Business system must have two Class of Service Options enabled, as defined in the table below. Refer to the *Mitel OIG Installation and Maintenance Guide* for additional Mitel OIG configuration information.

If either of these CoS options is disabled for a device, the Mitel OIG operations on the device do not function correctly.

CLASS OF SERVICE (COS) OPTIONS THAT MUST BE SET FOR EACH MONITORED DEVICE

HCI/CTI/TAPI Call Control Allowed: Yes
HCI/CTI/TAPI Monitor Allowed: Yes

EXAMPLES

Routing Devices use COS #1 only. If you are monitoring a routing device, COS #1 must have options set as indicated above.

The COS for an ACD Path and an Agent Group is defined by the COS of the first agent in the prime agent group for the ACD path. If you are monitoring ACD paths and querying ACD groups, the COS of the first agent must have options set as indicated above.

When monitoring ACD agents, the COS for each monitored agent must have options set as indicated above.

When monitoring trunks, the COS for each monitored trunk must have options set as indicated above.

When monitoring phones, the COS for each monitored phone must have options set as indicated above.

Mitel OIG System configuration

A single application can communicate with one or more Mitel OIGs.

The Mitel OIG can communicate with one or more applications or application instances (maximum of 1500). Additional requirements include:

- The Mitel OIG and MiVoice call manager instances must be co-located in the same Enterprise LAN.
- The Mitel OIG server must be added as a network element to the MiVoice Business System Data Synchronization (SDS) sharing network. For detailed information about SDS, see the *Using SDS Solutions Guide*, available on **MiAccess > eDocs**.

- The Mitel OIG server, MiContact Center server and MiVoice call manager controllers must be in the same LAN.

The Mitel OIG can be installed in a VMware server (Microsoft Hyper-V is also supported). The *Mitel OIG Engineering Guidelines* defines the number of OIG instances that can be installed on one server. See also the *Virtual Appliance Deployment Solutions Guide* for all limits and capacity information.

The Mitel OIG can now be licensed for service providers. Refer to the *Mitel OIG Installation and Maintenance Guide*. Also refer to the Mitel MiCloud Deployment and Blueprint documents and Engineering Guidelines for use of the Mitel OIG in Service Provider environments.



Note: The Mitel OIG assumes that the directory number (DN) for each device in the MiVoice Business system is unique. One Mitel phone cannot have the same DN as another Mitel phone in the same MiVoice Business system. For example; MiVoice Business A cannot have a phone configured with DN 1000 while MiVoice Business B also has a phone configured with DN 1000 (this constraint assumes MiVoice Business A and MiVoice Business B are not providing IP resiliency for each other).

- Up to six Mitel OIGs can communicate with one MiVoice Business.
- The Mitel OIG and MiVoice call manager instances must be co-located in the same Enterprise LAN.
- The Mitel OIG is not recommended for use in a DMZ or as a firewall to the WAN.

MiContact Center Configuration

- One Mitel OIG server can be connected to one MiContact Center server.
- The Mitel OIG server must have internet access.
- The Salesforce solution must use SSL for all web services communication.
- MiVoice Business call control status messages are different depending on if the MiVoice Business system has one controller compared to a MiVoice Business system with 2 or more controllers in a system cluster. For example, calls passed between two MiVoice Business controllers may lose call details.
- One MiContact Center server can connect to multiple Mitel OIG servers.
- Mitel OIG supports a total of 1500 hot desk users / hot desk ACD agents.
- The MiVoice Business controllers must be configured in an SDS sharing network.
- The Mitel OIG server must be configured with a CA certificate.
- Mitel OIG must be licensed with Advanced Call Control service if MiVoice Integration for Salesforce is to be used by hot desk ACD agents. Advanced call control service supports hot desk users.
- Mitel OIG can be licensed with Standard Call Control service if MiVoice Integration for Salesforce is to be used only by hot desk users.

- To allow remote MiVoice Integration for Salesforce users, the Mitel OIG server must use a MiVoice Border Gateway web proxy as a front-end. The external FQDN for Mitel OIG must match the internal FQDN. The MiVoice Border Gateway web proxy must have the same CA certificate as included in the Mitel OIG server. See the MSL Online Help for a description of how to request and install CA certificates.

Troubleshooting and testing

After installing the Mitel OIG, see the Mitel OIG Tools section in the Mitel OIG Developer Guides and the *Mitel OIG Installation and Maintenance Guide* for troubleshooting suggestions and for instructions about using the provided Mitel OIG tools. The Mitel OIG sample applications can also be used to check MiVoice call manager operation and communication.

MiVoice Business and Mitel OIG Connection Failures

When a connection failure occurs between the Mitel OIG and a MiVoice Business, the application is sent a system event “ICP_COMMUNICATION_EVENT” which includes the MiVoice Business IcpId and the connection state “CONNECTION_FAILURE”. The application will receive call events of event type “OUT_OF_SERVICE” for all device monitors that connected to the failed MiVoice Business.



Note: OUT_OF_SERVICE events for phones on a MiVoice Business are generated by the Mitel OIG. In the event of a network problem in which the OIG cannot access a MiVoice Business, but the phones can still access the MiVoice Business, it is possible that the phones are still IN_SERVICE. This is not common, but it is possible.

In most cases when the MiVoice Business connection fails, the phones become active on the secondary MiVoice Business and the application receives an IN_SERVICE call event from the secondary controller. After any MiVoice Business connection failure, the Mitel OIG tries periodically to reconnect to the MiVoice Business and recover all monitors.

MiVoice Business connection recovery

After monitors are started on a MiVoice Business, if the connection to the MiVoice Business fails or the MiVoice Business is restarted, the Mitel OIG tries periodically to reconnect to the MiVoice Business and recover all monitors. Monitors are only stopped when an application invokes the stopMonitor operation and there are no other sessions monitoring that device, or the session is terminated due to inactivity and no other sessions are monitoring that device.

When a connection to a MiVoice Business is recovered, the application receives a system event ICP_COMMUNICATION_EVENT with a connection state set to CONNECTED. When the monitors are recovered the application receives a MONITOR_SET event.

If connections to a device’s primary and secondary MiVoice Business controllers both fail, the Mitel OIG tries to recover both connections and restart the monitors.

Creating your own application

Application developers familiar with WSDL and web services will have little difficulty in creating an application. Developers are free to choose the workstation hardware, operating system, software development environment and programming language. The Mitel OIG WSDL files allow software development environments (Visual Studio, NetBeans, Eclipse) to auto-generate much of the code needed to communicate with the Mitel OIG. The specific application behavior is left to the developer.

The Mitel WSDL does not have an Internet-accessible target name space for XML schema definition. The developer must write code to access the correct location of the schema definitions. More information on this topic is provided with the Mitel OIG Sample Application Package.

The Mitel OIG Sample Application Package includes many sample applications available for developers. The entire package of source code and documentation are available online from the MiAccess > Software Download Center or the InfoChannel MSA portal.

Example: WSDL in Visual Studio using C#

If Microsoft Visual Studio is selected as the development environment and C# as the programming language, the following is an example of the simple steps needed to get started when creating an application.

1. Start Microsoft Visual Studio 2010.
2. Select **File > New Project > Windows Forms Application**.
3. Enter the name (e.g., Mitel OIGSampleApp)
4. Click **OK**.
5. Select **Project > Add Service Reference**, and click **Advanced**.
6. Click **Add Web Reference** and enter the URL that points to the SessionService.wsdl file (i.e., <http://10.40.224.130/mitel/oig/session/SessionService?wsdl>)
Where: 10.40.224.130 is the IP address of the Mitel OIG server)
7. Click the green arrow.
8. Enter Web reference name: "SessionService".
9. Click **Add Reference**.
10. Repeat the steps for the Standard Call Control Service by entering the URL to the StandardCCService.wsdl file (i.e., <http://10.40.224.130/mitel/oig/cc/StandardCCService?wsdl> where 10.40.224.130 is the IP address of the Mitel OIG server), enter Web reference name "StdCCService", and press "Add Reference".
11. Create an instance for the SessionService and StandardCCService in the C# form by selecting "Form1.cs" and clicking **View Code**.
12. Enter the following code in the public class Form1.

```
/*  
 * Sets up Mitel OIG Session service and Call Control service addresses.  
 */  
  
// Create the URI for the endpoint.  
sessionServer = new SessionService.SessionService();  
sessionServer.Url = "https://" + Mitel OIGServerAddr.Text + "/mitel/oig/session/SessionService";  
  
ccService = new StdCCService.StandardCCService();  
ccService.Url = "https://" + Mitel OIGServerAddr.Text + "/mitel/oig/cc/StandardCCService";
```

Then add application interfaces (full source for a C# sample application is available)

Example: WSDL in Visual Studio using Visual Basic

If Microsoft Visual Studio is selected as the development environment and Visual Basic as the programming language, the following is an example of the simple steps needed to get started when creating an application:

1. Start Microsoft Visual Studio 2010.
2. Select **File > New Project > Windows Forms Application**.
3. Enter the application name (e.g., Mitel OIGSampleApp).
4. Click **OK**.
5. Select **Project > Add Service Reference**.
6. Click **Advanced**.
7. Click **Add Web Reference** and enter the URL pointing to the SessionService.wsdl file - e.g., <http://10.40.224.130/mitel/oig/session/SessionService?wsdl>

Where 10.40.224.130 is the IP address of the Mitel OIG server.

8. Click the green arrow button.
9. Enter the Web reference name: "SessionService".
10. Click **Add Reference**.
11. Repeat steps for the Standard Call Control Service, enter the Web reference name "StdCCService", and click **Add Reference**.
12. Create an instance for the SessionService and StandardCCService in the Visual Basic form by selecting Form1.vb and selecting view code. Then enter the following code in the public class Form1:

```
'Create an instance of the Mitel OIG SessionService Web Service to login/logout  
Dim Mitel OIGSessionSrv As New SessionService.SessionService
```

```
'Create an instance of the Mitel OIG StandardCCService Web Service to access call  
control operations  
Dim Mitel OIGcc As New StdCCService.StandardCCService
```

13. Add code to create URLs to the Mitel OIG services:

```
Mitel OIGSessionSrv.Url = "https://" + Mitel OIGServerIpAddr.Text +  
"/mitel/oig/session/SessionService"
```

```
Mitel OIGcc.Url = "https://" + Mitel OIGServerIpAddr.Text +  
"/mitel/oig/cc/StandardCCService"
```

Then add application interfaces (full source for a Visual Basic sample application is available).

REST / JSON Data Access Web Service

Representational State Transfer (REST) describes a pattern for interacting with content on remote systems, typically using HTTP/HTTPS. REST describes a way to access and modify existing content and how to add content to a system.

JavaScript Object Notation (JSON) is a lightweight data-interchange format that is easy for humans to read and write. It is easy for machines to parse and generate and it is based on a subset of the JavaScript Programming Language: Standard ECMA-262 3rd Edition - December 1999.

The Mitel REST / JSON Data Access web service provides a simple API to retrieve MiVoice call manager configuration data and to be notified of configuration data changes. Since the web service is provided using standard HTTP(s) with a REST / JSON interface developers can choose their software language and development environment.

The following resources and operations are supported:

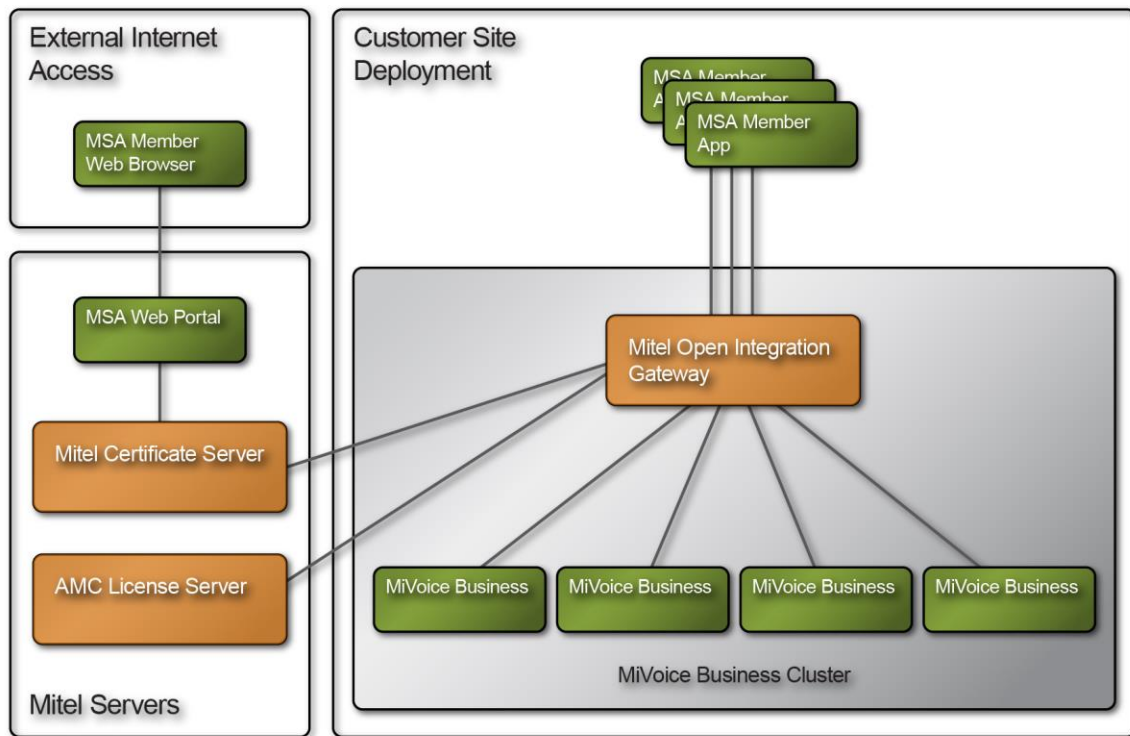
RESOURCE	OPERATIONS SUPPORTED
http://<Mitel OIGIPAddress>/Mitel /Mitel OIG/rest/resources/v1/sessions	
	Get – Get a session (equivalent to login) Delete – Delete a session (equivalent to logout) Put – Update session inactivity timer
http:// <Mitel OIGIPAddress>/Mitel /Mitel OIG/rest/resources/v1/databases	
	Get – Lists the databases accessible on this Mitel OIG
http:// <Mitel OIGIPAddress>/Mitel /Mitel OIG/rest/resources/v1/databases/views	
	Get – Get the views accessible for a database
http:// <Mitel OIGIPAddress>/Mitel /Mitel OIG/rest/resources/v1/databases/views/columns	
	Get – Get the columns for a view
http:// <MitelOIGIPAddress>/Mitel /Mitel OIG/rest/resources/v1/databases/sql	

RESOURCE	OPERATIONS SUPPORTED
	Get – Get result from SQL operation Delete – Delete SQL operation Post – Insert SQL operation Put – Update SQL operation
http:// <Mitel OIGIPAddress>/Mitel /Mitel OIG/rest/resources/v1/databases/views/events	
	Get – Get an event (trigger event)
http:// <Mitel OIGIPAddress>/Mitel /Mitel OIG/rest/resources/v1/databases/views/triggers	
	Post – Create a trigger on a view Delete – Delete a trigger on a view

Mitel Certificate Server Access and Requests

This section describes how application developers register with the MCS to enable communication between their applications and a Mitel OIG. To use the standard web services offered by the Mitel OIG, a developer must register each of their applications with the MCS. To use advanced web services offered by the Mitel OIG, a developer must request a Mitel certificate for each of their applications. A Mitel certificate request includes application registration. See details in subsections below.

Figure 9: Accessing the Mitel Certificate Server



Application Registration in MCS Access Control List (ACL)

Mitel OIG application developers must register their applications with Mitel. Mitel OIG applications developers planning to use standard services must register their application information. Mitel OIG application developers planning to use advanced services must request a Mitel certificate from Mitel. Application registration is included when requesting a Mitel certificate, no additional application registration is required.

Application Registration Request

To access the MCS, an MSA Authorized User (MSA Member) logs in through MiAccess using their login credentials.

- Log on to MiAccess (connect.mitel.com).

- Select **InfoChannel** in the left sidebar.
- Select **API and Interface Information** in the left sidebar.
- Select **MiVoice Business** in the left sidebar.
- Select **Mitel Open Integration Gateway (OIG) - Application Administration**. You will be directed to the Mitel Open Integration Gateway (OIG) Admin Portal.
- Select **Register OIG Application (Standard Call Control Only)**.

An MCS web form is presented. Click the **ACL Registration Request** tab. An ACL registration request form is presented.



Note: DO NOT use special characters like comma, \$, #, @, and so on, in any of the fields, while registering application with the Mitel Certificate Server (MCS).

Figure 10: ACL Registration request

Mitel Certificate Server

[Certificate Request](#)
[ACL Registration Request](#)
[Forgot Your Application Password](#)
[Change Your Email](#)
[Virtual Lab Request](#)

Please fill in the form to submit your ACL registration request. All fields are required.

Application Data

Application Name:
 Company Name:
 Application Password:
 Confirm Application Password:

MSA Authorized User Data

Email:
 MSA Account Number:
 Phone:
 Country:
 State/Province:
 City:

The user must enter data into all of the required fields and then click **Submit ACL Registration Request**. The MCS validates the data entered. If the submitted data is valid, the MCS redirects the MSA Authorized User to a new web page displaying a message that states an ACL registration request has been submitted for MSA Administrator approval.

Figure 11: Successful ACL registration request

Mitel Certificate Server

[Certificate Request](#)
[ACL Registration Request](#)
[Forgot Your Application Password](#)
[Change Your Email](#)
[Virtual Lab Request](#)

✓ The ACL registration request has been submitted and awaiting administrator approval.

Click [here](#) to submit another request

Application Registration Request Approval

Application registration approval is done by the MSA Administrator. The MSA Administrator logs in to the MCS and views a list of pending ACL registration requests. The MSA Administrator approves or denies each request based on the MSA Authorized User information provided in the ACL registration request. After approval, the MCS does the following:

1. Adds the user-provided company name, application name, MSA account number and application password to the MCS ACL. Once approved and added to the MCS ACL, these names and passwords cannot be changed.
2. E-mails the MSA Authorized User notifying approval using the e-mail address entered by the MSA Authorized User during the application registration.

Registration Request Denial

If the MSA Administrator denies the request, the MCS e-mails the MSA Authorized User notifying them of the denial, with the reason, using the e-mail address entered by the MSA Authorized User. The denial e-mail includes instructions for contacting MSA for more information.

Revoking Applications

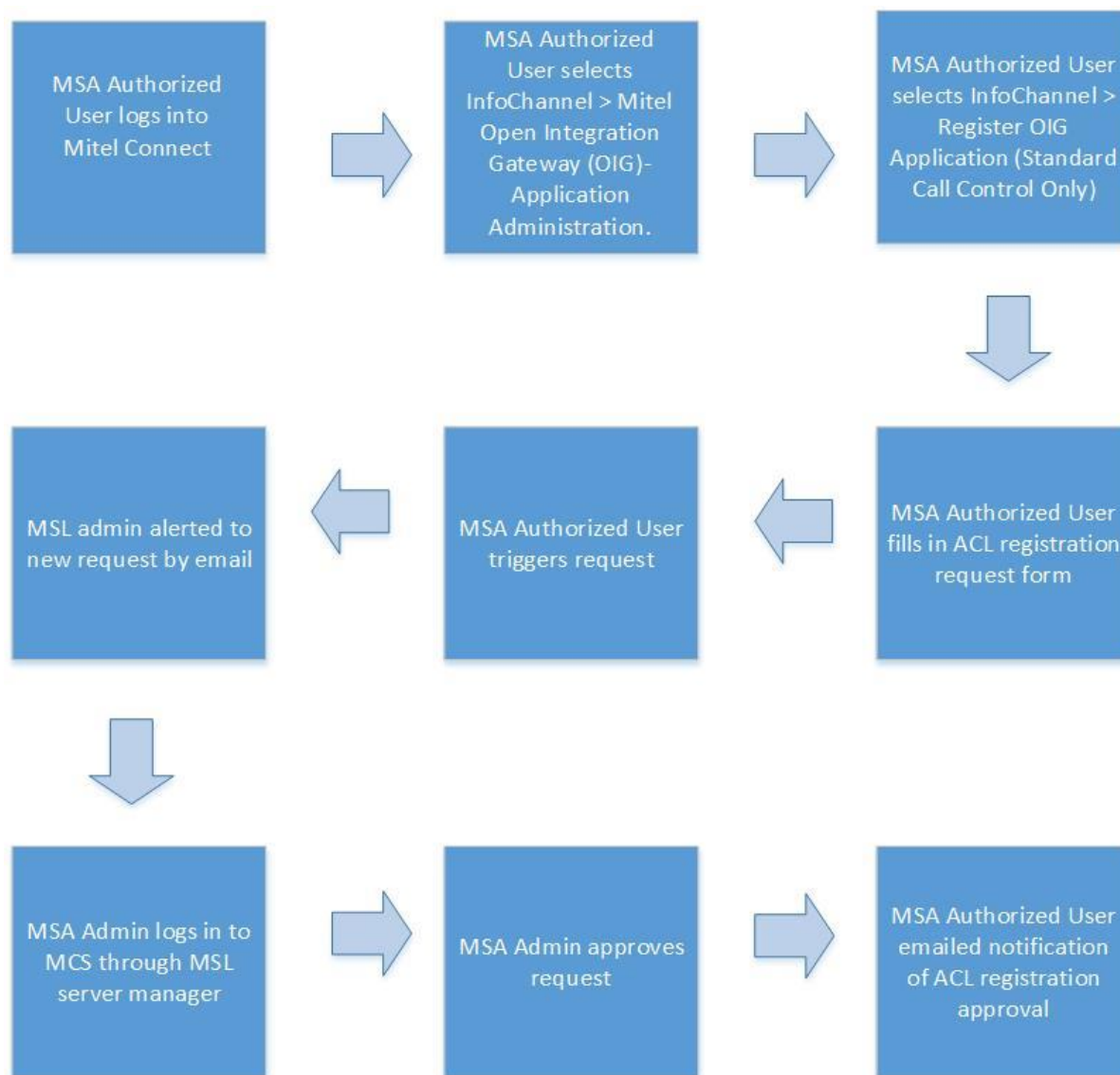
Revocation of applications from the ACL is done by the MSA Administrator. After an MSA–Authorized application has been registered in the MCS ACL, an MSA Administrator can decide to revoke the application. After an application has been revoked, the MCS does the following:

1. Updates the MCS ACL by tagging the application as revoked.
2. E-mails the MSA Authorized User notifying them of the revocation decision and the reason. The revocation e-mail includes instructions about contacting MSA for more information.

ACL Retrieval

The MCS ACL is retrieved by deployed Mitel OIG instances every four hours, or upon manual Mitel OIG Administrator request. Deployed Mitel OIG instances request the ACL through a web service offered by the MCS. Deployed Mitel OIG instances use the ACL to deny or approve communication requests from applications.

Figure 12: ACL registration request and approval flowchart



Mitel Certificate Request

MSA Authorized Users (MSA Members) must request a Mitel certificate when their applications require Advanced service operations from the Mitel OIG. A Mitel certificate request automatically includes an “add application to ACL” request, so a user does not need to submit two MCS requests to obtain access to a Mitel OIG.

Certificate Request Process

To access the MCS, an MSA Authorized User (MSA Member) logs in through MiAccess using their login credentials.

1. Log on to **MiAccess** (connect.mitel.com).

2. Select **InfoChannel** in the left sidebar.
3. Select **API and Interface Information** in the left sidebar.
4. Select **MiVoice Business** in the left sidebar.
5. Select **Mitel Open Integration Gateway (OIG) - Application Administration**. You will be directed to the Mitel Open Integration Gateway (OIG) Admin Portal.
6. Select **Request OIG Certificate (Standard and Advance Call Control)**.

An MCS web form is presented. Click the **ACL Registration Request** tab. An ACL registration request form is presented.



Note: DO NOT use special characters like comma, \$, #, @, and so on, in any of the fields, while registering applications with the Mitel Certificate Server (MCS).

Figure 13: Certificate request

Mitel Certificate Server

Certificate Request | ACL Registration Request | Forgot Your Application Password | Change Your Email | Virtual Lab Request

Please fill in the form to submit your certificate request. All fields are required.

Application Data

Application Name:

Company Name:

Application Password:

Confirm Application Password:

MSA Authorized User Data

Email:

MSA Account Number:

Phone:

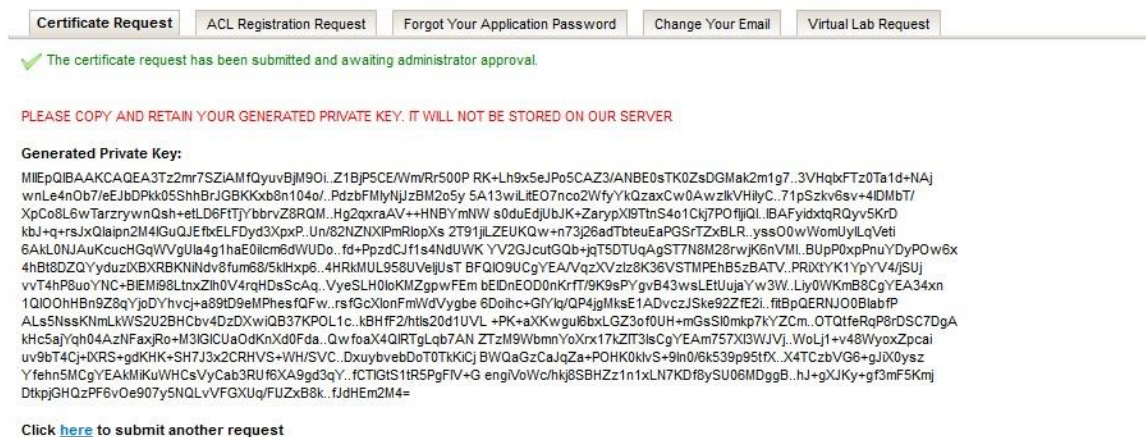
Country:

State/Province:

City:

The MSA Authorized User must enter data in all the required fields on the MCS web form, then click **Submit Certificate Request**. If the submitted data is valid, the MCS redirects the MSA Authorized User to another web form, which displays the following:

1. A message stating that a certificate request has been submitted and is awaiting MSA Administrator approval.
2. A message stating that the displayed MSA Authorized User private key must be copied before leaving this form. The MSA Authorized User private key that is displayed is destroyed when the web form is closed -- it is lost if it is not copied. If the private key is lost, then the pending certificate will be invalid; an application must have the matching private key for a Mitel certificate. If the private key is lost, then another certificate request will have to be submitted.
3. The private key for the requested Mitel certificate.

Figure 14: Successful certificate request submission**Mitel Certificate Server**


The screenshot shows the Mitel Certificate Server interface. At the top, there are five tabs: "Certificate Request" (selected), "ACL Registration Request", "Forgot Your Application Password", "Change Your Email", and "Virtual Lab Request". Below the tabs, a green checkmark icon is followed by the text: "The certificate request has been submitted and awaiting administrator approval." Below this, a red text box contains the instruction: "PLEASE COPY AND RETAIN YOUR GENERATED PRIVATE KEY. IT WILL NOT BE STORED ON OUR SERVER". Underneath, the "Generated Private Key:" is displayed, followed by a long, multi-line string of alphanumeric characters representing the private key. At the bottom, there is a link that says "Click [here](#) to submit another request".

The MSA Authorized User must copy the private key and secure it in a safe location. The private key must be added to the application named in the Mitel certificate request. The application must use the private key to encrypt data, as part of Mitel OIG login. The MCS does not store a copy of the generated private key. After copying the private key, the MSA Authorized User can exit the web browser session.

If the certificate request is approved, the MCS e-mails the Mitel certificate to the MSA Authorized User.

Certificate Request Approval

Mitel certificate request approval can be accomplished manually by the MSA Administrator. The MSA Administrator logs in to the MCS to view a list of pending certificate requests. The MSA Administrator approves or denies each request based on the information entered by the MSA Authorized User. After approval, the MCS does the following:

1. Generates a Mitel certificate that includes the MSA Authorized User public key that matches the provided application private key. The certificate expiry date is set to 25 years.
2. Digitally signs the Mitel certificate using a Mitel private key.
3. E-mails the MSA Authorized User the Mitel certificate, using the e-mail address entered by the MSA Authorized User during the certificate request.
4. Adds the MSA Authorized User application to the MCS ACL.

Certificate Request Denial

The MSA Administrator can deny a certificate request when reviewing the list of pending certificate requests. The MSA Administrator decides based on MSA Authorized User information. Once denied, the MCS e-mails the MSA Authorized User the denial and reason using the e-mail address provided by the MSA Authorized User. The denial e-mail includes instructions for contacting MSA.

Regenerating a Certificate for an Application

If an MSA member loses an application private key, the user must request another certificate. This additional request is different than the initial certificate request. The application registration in the ACL does not change; a new certificate is generated. The MSA member logs in through MiAccess using an MSA Authorized User account. The MSA Authorized User is presented with the MSA web portal. The web portal provides web links to a **Certificate Request** tab (see Figure 8). The MSA Authorized User selects this tab. The MSA Authorized User must enter data in all the required fields on the MCS web form, then click **Submit**. If the submitted data is valid, the MCS redirects the MSA Authorized User to another web form displaying the following:



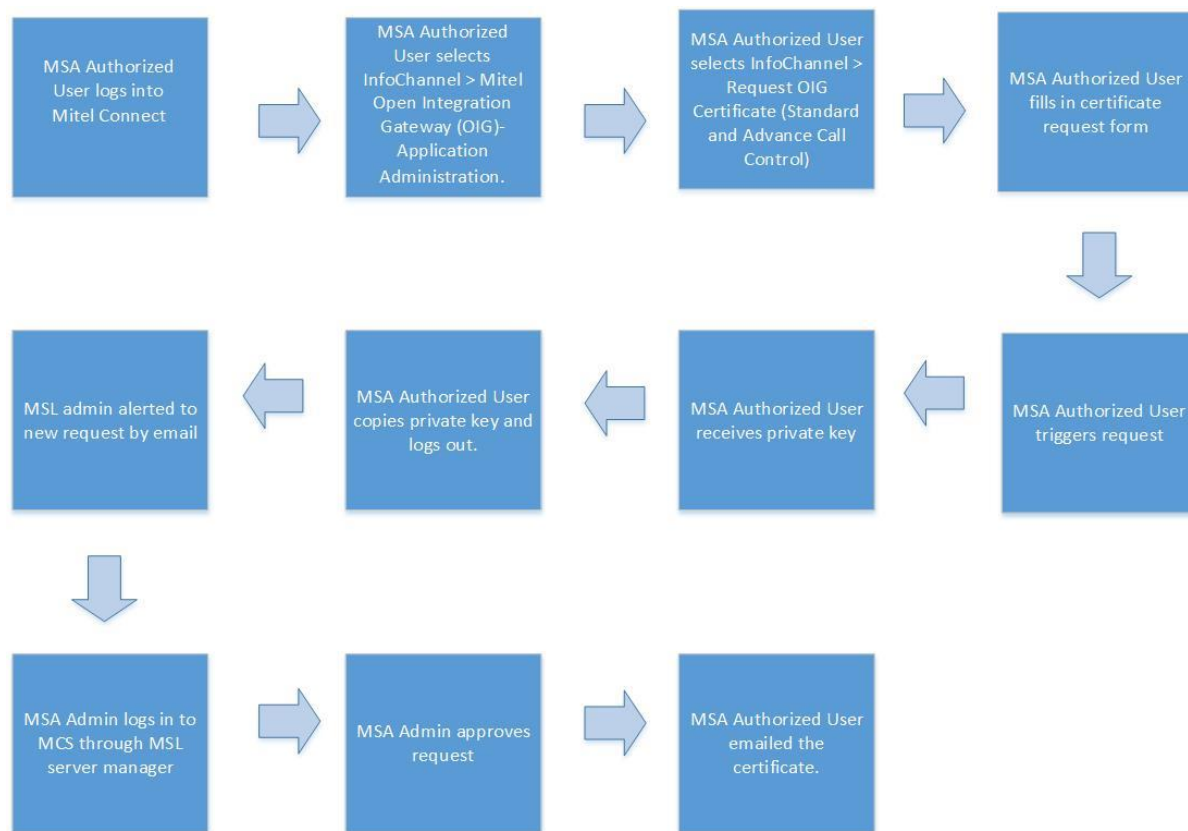
Note: The data entered must be exactly the same information that was entered during the application registration process. The company name, application name, and application password must be identical to those in the initial application registration.

1. A message that states a certificate regeneration request has been submitted and is awaiting MSA Administrator approval. This means that another certificate is being requested but the MCS ACL will remain the same (i.e., Company Name, Application Name, and application password do not change). If the user enters another application password, the password will be ignored. The existing application password in the ACL must be used by the application when logging in to a Mitel OIG (when the initial Company name, Application name, and application password are approved and added to the MCS ACL - the names and password CANNOT be changed).
2. A message that states the displayed MSA Authorized User private key must be copied before leaving this form. The MSA Authorized User private key displayed will be lost if not copied. If the private key is lost, then the pending certificate will be invalid and another certificate request will have to be submitted.
3. The private key associated with the additional Mitel certificate request.

The MSA Authorized User must copy the private key and secure it in a safe location. The private key must be added to the application named in the Mitel certificate request. The application will be required to use the private key to encrypt data as part of Mitel OIG login. The MCS does not store a copy of the generated private key. After copying the private key, the MSA Authorized User can exit the web browser session.

The MCS notifies (by e-mail) the MSA Administrator of the pending certificate request. If the MSA Administrator approves the certificate request, the MCS e-mails the Mitel certificate to the MSA Authorized User.

Figure 15: Certificate request and approval flowchart



Glossary

ACD	Automatic Call Distribution
ACL	Access Control List
AMC	Applications Management Center (licensing server)
API	Application Programming Interface
CCS	Call Control Service
COS	Class of Service
DLL	Dynamic Link Library
DMZ	De-Militarized Zone
DNS	Domain Name Server
ICP	IP Communications Platform
IP	Internet Protocol
IVR	Interactive Voice Response
LAN	Local Area Network
MCS	Mitel Certificate Server
MiCC	MiContact Center
MOL	Mitel OnLine
MSA	Mitel Solutions Alliance (Mitel developer partner program)
MSL	Mitel Standard Linux (operating system)
MSP	Media Service Provider
Mitel OIG	Open Integration Gateway
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
SDS	System Data Synchronization: A Mitel data sharing feature that allows changes to be made easily throughout a network of nodes, including MiVoice Business, MiCollab, and Mitel OIG.
TDM	Time Division Multiplexing
VOIP	Voice over IP
vLAN	Virtual Local Area Network
WAN	Wide Area Network
WSDL	Web Service Description Language

