Mitel Open Integration Gateway (OIG)

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

Software Release Notes
Release 4.2 SP1
May 2022

Table of Contents

About This Document

This RN (Release Note) is intended for Customer Service and Installation Personnel involved in the installation and maintenance of the Mitel Open Integration Gateway.

These Product Release Notes cover product specific information focused on premise installations. Much of the information contained here also can apply to Cloud deployments. If deploying OIG in a cloud environment, please be sure to **also** consult the appropriate MiCloud Business for Service Provider Release Notes.

Release Notes for Mitel Open Integration Gateway Release 4.2 SP1

This document describes the following areas related to Open Integration Gateway 4.2.62.0

- Product enhancements and functional changes

- Where to find the latest information

- Product areas improved in this release

- Known Issues

We strongly recommend you review the instructions found in the *Open Integration Gateway 4.2 SP1 Installation and Administration Guide* and the hardware and software requirements found in the *Open Integration Gateway 4.2 SP1 Engineering Guide* before downloading, installing, or upgrading your software.

Product Enhancements and Functional Changes

The following table describes product enhancements and functional changes for Open Integration Gateway Version 4.2.62.0

Product or Feature	Description
Support for Dialed Digits information with ACD2PathEvent	With OIG 4.2 SP1 and MiVB 9.3, OIG has added DIALED_DIGITS information with ACD2_PATH event type to provide Original Dialed Digits information for incoming call on the monitored ACD Path, when event cause is ACD_CALL_REQUEST, ACD_CALL_QUEUED or ACD_REQUEUE_REQUEST.
Certificate Validation support of OIG for connection to MiVB	With OIG 4.2, there was an added security mechanism, where OIG will connect to MiVB only if it trusts the signing authority of the certificate presented by MiVB, else connection fails. By default, OIG trusts only Mitel self-signed certificate.
	With OIG 4.2 SP1, OIG Administrator can add the customized certificate to add the certificate chain of trust in OIG, so that OIG can successfully connect to a MiVB with a customized certificate.
AWS, Azure Support	Mitel OIG 4.2 SP1 Blade can be installed on MSL deployed in AWS or Azure Clouds.

Where to Find the Latest Information

You can access the most up-to-date versions of the following documents from **MiAccess** > **Document Center** > **Applications** > **Collaboration** > **Open Integration Gateway** and **MiVoice Integrations**.

- Technical Documentation
  - Mitel Open Integration Gateway Installation and Maintenance Guide
  - Mitel Open Integration Gateway Engineering Guidelines
  - Mitel Open Integration Gateway Developer Guide – Fundamentals
  - Mitel Open Integration Gateway Developer Guide – Session Management Service
  - Mitel Open Integration Gateway Developer Guide – Call Control Service
  - Mitel Open Integration Gateway Developer Guide – Data Access Service
- Integration Documentation:
  - MiVoice Integration for Google Administration Guide
  - MiVoice Integration for Salesforce Administration Guide
- User Documentation:
  - MiVoice Integration for Google Quick Reference
  - MiVoice Integration for Salesforce User Guide

Product Areas Improved in This Release

TRACKING NUMBER	DESCRIPTION
OIG-727	Log4j Vulnerability remediated by upgrading the Log4j library to version 2.17.0. This addresses Log4j Vulnerability CVE-2021-44228, therefore with this release, the mitigation is no longer required.
	This upgrade also resolves further Log4j Vulnerabilities CVE-2021-45046 and CVE-2021-45105 as well.
	For CVE-2021-44832, OIG does not offer the access to log4j properties file, nor we have JDBC configuration in Mitel OIG. Hence, OIG should not be impacted by Log4j Vulnerability CVE-2021-44832.
OIG-715 OIG-719	Security fix where the X-Frame Options is now set to SAMEORIGIN. With this change, MiVoice Integration for Salesforce 2.5.52.0 is compatible with OIG 4.2 SP1 and above.
MIVB-27842	Issue fixed with MiVB 9.2, where, if consultationCall() is invoked with "number" attribute having a blank string OIG will return result as "true" and soft hold will be initiated. Partial digits with "number" attribute would be considered as final destination.
MBG-667	With MBG 11.3 SP1, more URLs are allowed. Hence, Session and Call Control Services can be utilized by Third party OIG Applications, MSL Page and Mitel OIG page is accessible across MBG.

Known Issues

1. When a network element (NE) for MiVoice Business is removed from the OIG admin UI Network Element table and the MiVoice Business node is removed physically from the IP network, the OIG continues to try to re-connect to the NE.

   A restart of the OIG server is required to stop the reconnect attempts from OIG.

2. If the Application Name or Company Name of an Advanced Application has any special characters like comma, $, #, *, @ etc., then while trying to login in OIG, the application will receive a certificate error "*The certificate provided does not match the application credentials provided*".

   It is recommended not to use any special characters in any of the fields like Application Name, Company Name, Country, State/Province and City, while registering the application with MCS.

3. OIG Web Server Page will not open properly, and Call control services will not be accessible to third party application, when accessed across MBG Web Proxy.