

# MiCloud Management Portal Engineering Guidelines

JULY 2020

RELEASE 6.1



## **Notice**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

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

## **Trademarks**

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto: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>.

© Copyright 2020, Mitel Networks Corporation

All rights reserved

MiCloud Management Portal  
Engineering Guidelines  
Release 6.1  
July 2020

## Table of Contents

<b>1</b>	<b>About this Document .....</b>	<b>1</b>
1.1	Overview .....	1
1.2	References .....	1
<b>2</b>	<b>System Overview .....</b>	<b>3</b>
2.1	Multi-Tiered Management .....	3
2.2	MiCloud Management Portal and MiVoice Business (MiVB) Relationship .....	4
2.3	MiCloud Management Portal and MiCollab/MiVoice Business Express (MiCollab/MiVB-X) Relationship .....	4
2.4	MiCloud Management Portal and MiVoice Border Gateway (MiVBG) Relationship .....	5
2.5	MiCloud Management Portal and MiCollab Client Multi-Tenant Relationship .....	5
2.6	Features introduced in this release .....	5
<b>3</b>	<b>Network and Element Requirements .....</b>	<b>6</b>
3.1	Date and Time Settings .....	6
3.2	Deployment Topologies .....	6
3.2.1	Internet-Based Deployment .....	7
3.2.2	Virtual Private Network (VPN) Deployment .....	9
3.3	Deployment Considerations .....	10
<b>4</b>	<b>System Requirements .....</b>	<b>11</b>
4.1	Application Requirements .....	11
4.2	LAN/WAN Requirements .....	11
4.2.1	Static IP Address .....	11
4.2.2	DNS Servers .....	12
4.2.3	NAT .....	12
4.3	Hardware and Software Requirements .....	12
4.3.1	Support for Virtual Environments .....	12
4.3.2	MiCloud Management Portal Server Requirements .....	12
4.3.3	Browser Requirements .....	13
<b>5</b>	<b>Configuration .....</b>	<b>14</b>
5.1	System parameters and the sysprop maintenance commands .....	14
5.1.1	Some common system parameters .....	17
5.2	Port Usage .....	18
5.3	VLAN Support using Split DNS .....	20
5.4	NAT with Mitel Management Gateway (MMG) .....	21
5.5	NAT with VMware vCloud Networking and Security .....	21
5.6	Working with MiCollab Flow Through Provisioning .....	22
5.7	MiVoice Border Gateway Configuration .....	22
5.7.1	MiVoice Border Gateway Web Services .....	23
5.7.2	Registering MiVoice Border Gateway platforms .....	23
5.7.3	DID Routing .....	24
5.7.4	Mitel phone, SIP, and UC Device Management .....	25
5.7.5	Managing MiVoice Border Gateway Cluster Zones .....	26
5.8	MiCollab Client Multi-Tenant .....	27
5.8.1	MiCollab Client Multi-Tenant Web Services .....	27
5.8.2	Registering MiCollab Client Multi-Tenant platforms .....	27
5.9	Generic Ranges for System Generated Numbers .....	27
5.10	Platform Synchronization for Billing .....	27

<b>6</b>	<b>Performance Specifications</b>	<b>29</b>
6.1	MiVoice Border Gateway performance	29
6.2	MiCollab Client Multi-Tenant performance	29
6.3	Spectre and Meltdown mitigation impact	30
<b>7</b>	<b>Administrators</b>	<b>31</b>
7.1	Service provider administrators	31
7.2	Customer administrators	31
<b>8</b>	<b>Security</b>	<b>33</b>
8.1	Identity and Authentication	34
8.2	Access and Authorization	34
8.3	Audits and Logs	34
8.4	Network Settings	35
8.4.1	LAN 2 Settings	35
8.4.2	WAN Settings	35
8.4.3	Remote Access	35
8.5	Anti-Virus Protection	35
8.5.1	Use of Antivirus Software	35
8.6	Software Patch Management Policy	36
8.7	LAN Security	36
8.7.1	Network Access Security	36
8.7.2	Using VLANs to Assist with Security	36
8.8	Security Certificates	36
<b>9</b>	<b>Best Practices</b>	<b>37</b>
9.1	Reassigning platforms	37
9.2	Importing large number of users	37
<b>10</b>	<b>Glossary</b>	<b>38</b>

# 1 About this Document

## 1.1 Overview

This document provides guidelines for the engineers in planning and installation of MiCloud Management Portal (MMP). The guidelines describe specific areas of the product that need to be considered before installation. These guidelines should not be considered as a comprehensive list, but as useful reminders or pointers for consideration.

This document describes:

- Product functionality, enhancements, and functional changes
- Network and element requirements
- System requirements
- System configuration for providing services to customers
- Performance specifications

This document provides guidelines for service providers in cases of new customer provisioning only. Retrofitting existing customer installations to be managed by MiCloud Management Portal is not explicitly supported; however, it can be accomplished if required by Mitel Professional Services.

This document should be used by system engineers to:

- Determine the network and element requirements to ensure compatibility.
- Determine the platform requirements for MiCloud Management Portal installation.
- Collect customer site information and requirements.
- Analyze and record any special configuration information required at the site for optimal performance.

## 1.2 References

Documents referenced by the Engineering Guidelines include:

- [1] MiCloud Business Solution Blueprint, Release 4.2, Mitel, 2019
- [2] MiCloud Business Virtual, Deployment Guide, Release 4.2, Mitel, 2019
- [3] MiCloud Business Multi-Instance, Deployment Guide, Release 4.2, Mitel, 2019
- [4] MiCloud Business Service Providers Help, Release 4.2, Mitel, 2019
- [5] MiCloud Management Portal Release Notes, 2019
- [6] Virtual Appliance Deployment, Solutions Guide, Mitel, 2019
- [7] MSL Qualified Hardware List, Mitel, 2018

- [8] MiCollab Client for Mobile Resiliency Guide, Release 8.0, Mitel, 2017
- [9] MiCollab Client Engineering Guidelines, Release 8.0 SP2, Mitel, 2018
- [10] MiCloud Management Portal Engineering Guidelines (current document), Mitel, 2018

## 2 System Overview

MiCloud Management Portal, formerly known as Oria is a system management and customer self-service application for voice and unified communication services. The goal of MiCloud Management Portal is to cut down on the 'swivel chair'<sup>1</sup> administration operations and make it easier and more efficient for a service provider to offer and deploy services to their customers.

MiCloud Management Portal enables a service provider to manage and deploy hosted services to their customers. At the same time, MiCloud Management Portal allows the service provider to offer each of their customers an administration and self-service portal to make site specific moves, adds, changes, and deletes. Additionally, phone users that are created for a customer have access to a variety of phone features defined by their assigned feature set (called a bundle).

MiCloud Management Portal 6.1 is included as part of the MiCloud 4.1 release. MiCloud Management Portal could also be deployed independently outside of MiCloud. For a good understanding of MiCloud, refer to documents [1], [2] and [3] in References of this document.

### 2.1 Multi-Tiered Management

MiCloud Management Portal is a multi-tiered application that provides several levels of control. The various levels and their attendant capabilities are:

- Service Provider (SP):
  - Platform (MiVoice Business/MiCollab/MiVoice Business Express/MiVoice Border Gateway) management
  - Control of Customer Sites
  - Customer User Creation
  - Direct Inward Dialing (DID or DDI) Management
  - Customer Emergency Services Identification (CESID)
  - Dial Plans and Key Templates
  - Billing and Licensing Information
  - Service Definition and Bundling
  - Customer site parameters (Voicemail hunt group, mailbox ranges, etc.)
  - Reseller (Virtual Service Provider and Value-Added Reseller) creation and management.
- Virtual Service Provider (VSP):
  - All the features of Service Provider except reseller creation and management
- Value Added Reseller (VAR):
  - All the features of Virtual Service Provider except platform management
- Customer Administrator:
  - User Management
  - Assign DIDs
  - Call Rerouting
  - Call Groups (Hunt, Ring, Page, Pickup)

---

<sup>1</sup> Definition: <https://www.techopedia.com/definition/1034/swivel-chair-interface>

- Hot Desk Phones
- Twinning
- Voicemail
- Call Flow
- ACD
- Key Template
- Auto Attendant
- Business hours
- Music-On-Hold
- End User:
  - Voicemail PIN
  - Twinning Number
  - Call History
  - Phone Directory
  - Programmable Keys
  - Personal Profile
  - Password management

## 2.2 **MiCloud Management Portal and MiVoice Business (MiVB) Relationship**

The main purpose of MiCloud Management Portal is to allow service providers to deploy unified communications services to their customers and manage any customer issues. It also enables the customer to perform their own management and self-service operations. To do so, MiCloud Management Portal modifies MiVoice Business data on behalf of the customer. Customers no longer need to configure their MiVoice Businesses directly.

Please note that Bidirectional Synchronization feature does not work with MiVoice Business platforms. When configuration changes are made directly to an MiVoice Business via its management interfaces (i.e. outside of the MiCloud Management Portal framework) these changes can create discrepancies between MiCloud Management Portal's database and that of the MiVoice Business. These conditions should be avoided when possible.

## 2.3 **MiCloud Management Portal and MiCollab/MiVoice Business Express (MiCollab/MiVB-X) Relationship**

MiCloud Management Portal manage users on a MiCollab or a MiVoice Business Express. MiCloud Management Portal also manages NuPoint mailboxes for call groups on these platforms. The current user update capabilities for a MiCollab or a MiVoice Business Express platform include User Data, Phone Data and Features.

Call group mailboxes are not associated with users. MiCloud Management Portal creates them without creating users on MiCollab or MiVoice Business Express.

Bidirectional Synchronization and License Data Synchronization was introduced in MiCloud Management Portal 6.0. These features work with MiCollab and MiVoice Business Express platforms to synchronize modifications to users made directly on the platforms. These are limitations to what can be synchronized. The details of this feature are found in the document [4] in References.

## 2.4 **MiCloud Management Portal and MiVoice Border Gateway (MiVBG) Relationship**

MiCloud Management Portal interacts with MiVoice Border Gateway in the following scenarios:

- As DIDs are created in MiCloud Management Portal, these can be written to MiVoice Border Gateway as SIP trunk routing rules.
- As users are assigned SIP or Minet devices in MiCloud Management Portal, these can be written to the MiVoice Border Gateway.

MiVoice Border Gateway are treated as separate platform items, which are registered by administrators and then allocated to voice platforms (MiVoice Business /MiCollab/ MiVoice Business Express) as required. A stand-alone MiVoice Border Gateway is shared by multiple voice platforms in the services of DID call routing, proxying for MiCollab clients and handling Teleworker devices.

A MiVoice Border Gateway that is embedded in a MiCollab or MiVoice Business Express platform is used by its host platform.

## 2.5 **MiCloud Management Portal and MiCollab Client Multi-Tenant Relationship**

When an MiCloud Management Portal user is created with a bundle that has the MiCollab option, then MiCloud Management Portal creates a unified communications account on the assigned MiCollab Client Multi-Tenant server.

MiCollab Client Multi-Tenant is treated as separate platform item, which is registered by administrators and then allocated to voice platforms (MiVoice Business) as required. A single MiCollab Client Multi-Tenant is shared by multiple voice platforms.

## 2.6 **Features introduced in this release**

A complete list of new features are found in documents [4] and [5] in References, some of which are:

- ACD Path and Group Enhancements
- Bidirectional Sync of Groups

## 3 Network and Element Requirements

### 3.1 Date and Time Settings

For consistent operations, the clock of the MiCloud Management Portal server and those of the platforms should be set to the same time zone. Mitel recommends synchronizing with a networking time server to maintain accurate time.

The Date and Time setting is a function of the MSL Operating System (OS) on which MiCloud Management Portal runs and are found when you log in to the server-manager address. The following figure shows the Date and Time menu.

**Date and time configuration**

This is where you configure the date and time of this server. You may use an existing network time server or manually set the date and time for your time zone.

**Current Settings:**

Current Time:	Thu Sep 29 16:35:14 EDT 2016
Time Zone:	America/New_York
Network Time Server:	Enabled
NTP Server:	centos.pool.ntp.org <a href="#">Query</a>

**Set system TimeZone**

The system global TimeZone controls the conversion between internal time (UTC) and displayed local time, and also determines when Daylight Savings Time applies.

Time Zone:

**Configure Network Time Server**

The server is periodically synchronizing the system clock to the network time protocol (NTP) server specified below. To synchronize to a different NTP server, enter a different hostname or IP address in the field below.

NTP Server:

☐ **Disable Network Time Server**

Choose this option to stop synchronizing the system clock to the NTP server. When the NTP service is disabled, you can set the system date and time manually from this page.

[Save](#)

### 3.2 Deployment Topologies

Document [1] in References describes different MiCloud Management Portal deployment topologies. It is worth reading the Document [1] first before proceeding. This section redacts those deployment topologies into two main strategies. The goal here is to provide a quick overview.

MiCloud Management Portal is normally deployed in a hosted environment, where the only telephone equipment on the customer site is the end-user phone sets.

The goal of any deployment scenario is to:

1. Provide a data path from the customer site to the MiCloud Management Portal server for execution of site-specific administration functions such as local user management, group management, auto-attendant configuration, etc.
2. Provide a voice and data path from the customer site to the customer's assigned platforms.

The following illustration shows the logical relationships between the elements and roles in a hosted MiCloud Management Portal environment. Subsequent sections discuss alternative methods of implementing this. In the following diagram, any server instance (include the MiCloud Management Portal server) can be a physical or virtual computer.

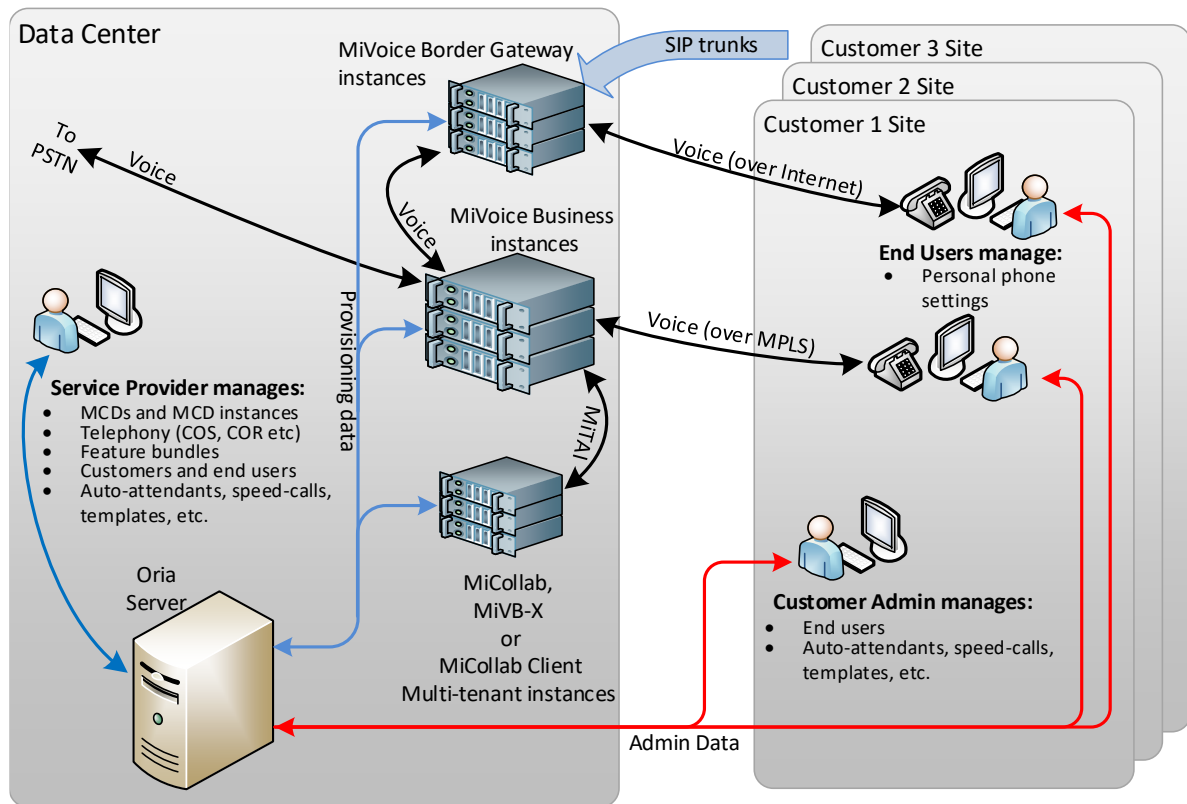


Figure 1 Overview diagram.

There are two basic strategies for user voice that are adopted while deploying an MiCloud Management Portal-managed system:

1. Internet-based, which requires a MiVoice Border Gateway to be the gateway for voice over the public Internet.
2. Virtual Private Network (VPN) which is *Internet Protocol* (IP) or *Multiprotocol Label Switching* (MPLS) based

Other deployments are possible. For example, the platforms are located at the customer site and managed by MiCloud Management Portal, but the networking requirements are significantly more complicated than a fully hosted environment. The following sections present the two main alternatives.

### 3.2.1 Internet-Based Deployment

In this type of deployment, voice and data travel from customer sites over the internet to the hosting data center. Voice and data arrive at a border gateway in the data center. The gate way then routes voice to the MiVoice Business instances and data to the MiCloud Management Portal server.

With this type of deployment, end users and customer admins are located anywhere there is an Internet connection.

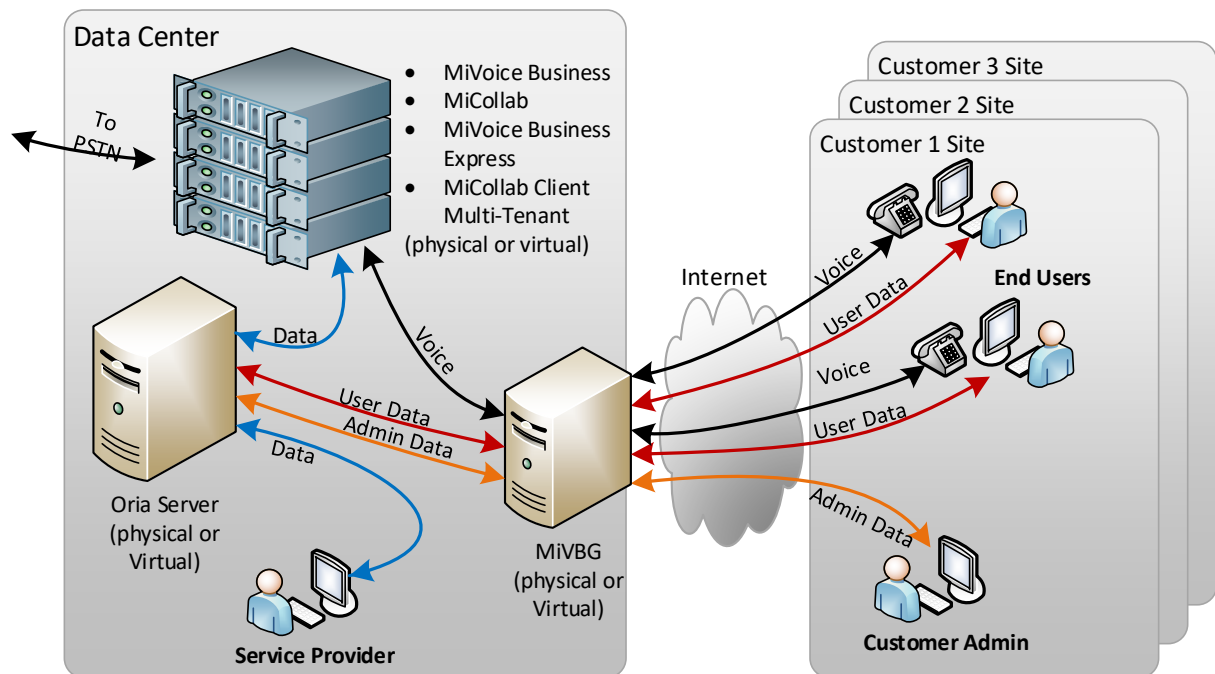


Figure 2 An example of Internet-based deployment topology.

The recommended solution for the gateway component is the MiVoice Border Gateway, which is specifically designed for Teleworker applications. With the MiCollab and MiVoice Business Express platforms, the provider chooses whether to use the embedded MiVoice Border Gateway or an external MiVoice Border Gateway for their needs. For information on configuring a MiVoice Border Gateway, refer to section 5.7 of this document.

MiCloud Management Portal makes it easier to employ MiVoice Border Gateways in solutions, as it has the ability to manage SIP trunk routing rules and client devices as part of the solution.

### 3.2.2 Virtual Private Network (VPN) Deployment

This alternative employs a VPN to extend the customer site network into the data center (or vice-versa) and providing a customer site with data access to the MiCloud Management Portal server and voice access to the assigned MiVoice Business instances.

**From the Wikipedia definition for Extranet:**

*“If all the sites in a VPN are owned by the same enterprise, the VPN is a corporate intranet. If the various sites in a VPN are owned by different enterprises, the VPN is an extranet. A site can be in more than one VPN; e.g. in an intranet and several extranets.”*

With that definition in mind, this alternative describes an “Extranet”, however the term “VPN” is used due to most people’s familiarity with it.

A VPN solution provides end users and admins with essentially local access to the MiCloud Management Portal server for data, and the MiVoice Business/MiCollab/MiVoice Business Express/MiCollab Client Multi-Tenant instances for voice and data. At the data center, service providers must manage the VPN policies carefully to allow customer access only to those elements assigned to the customer.

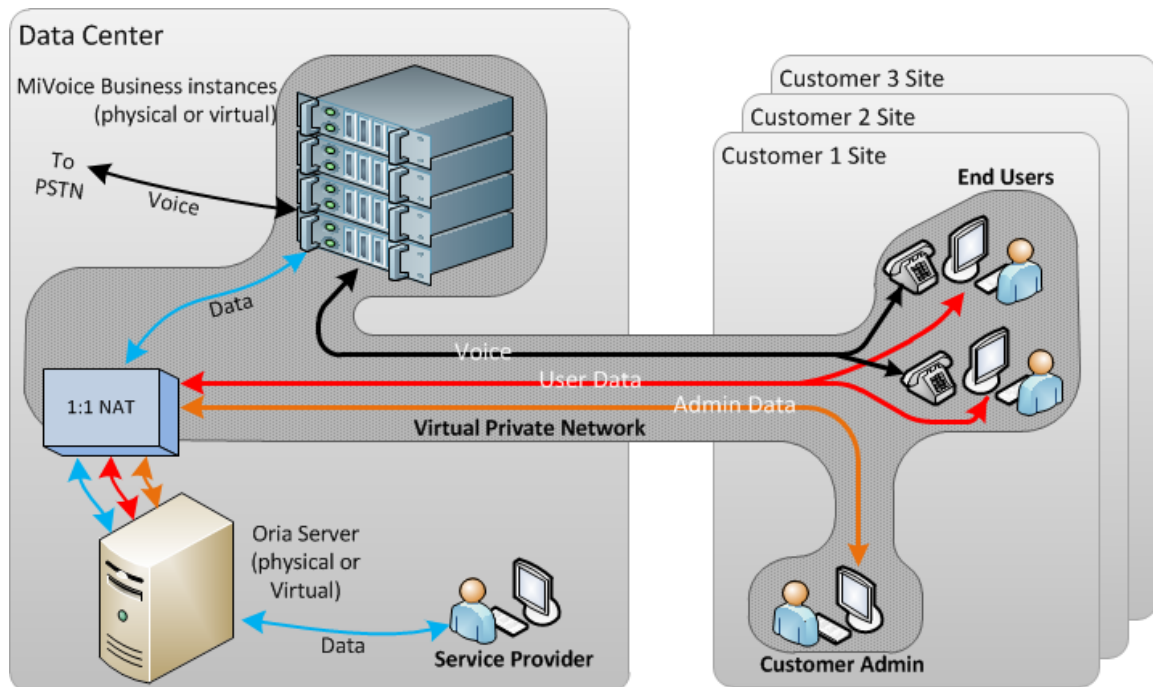


Figure 3 VPN deployment topology

### 3.3 Deployment Considerations

#### Cost

Cost is an important consideration when planning a deployment. The two alternative deployment topologies presented previously have different costs associated with them as well as common costs (i.e. in MiVoice Business licenses, user and voicemail licenses).

- The Internet-based/ MiVoice Border Gateway alternative requires a Teleworker license for each end user, as well as user and mailbox licenses. Furthermore, this solution requires the acquisition of the gateway hardware and software, whose costs is borne by the data center and included in the cost structure of the provided service. However, a MiVoice Border Gateway supports thousands of connections, so a single MiVoice Border Gateway services many customer sites. Refer to the MiVoice Border Gateway documentation for the current connection capacity.
- The VPN alternative incurs the cost of maintaining the VPN between the customer site and the data center. A high-performance MPLS link is quite expensive. Normally these costs are recurring. If the VPN is hosted at the data center, then the cost will be borne by the data center and included in the cost structure of the provided service.

#### Voice Quality

Due to the vagaries of the Internet, the Teleworker solution experiences reduced voice quality during times of high traffic on the Internet. On the other hand, the best voice quality is achieved via an MPLS VPN.

#### Vendor Count

The Teleworker option is an all-Mitel solution, whereas the VPN option requires the acquisition and maintenance of a 3<sup>rd</sup> party component, namely the VPN. If problems occur at the data center or at a customer site, with an all-Mitel solution, the service provider has fewer parties to deal with.

## 4 System Requirements

### 4.1 Application Requirements

MiCloud Management Portal 6.1 is part of the MiCloud 4.1 suite of products. The most up to date and complete list of compatible software versions for MiCloud 4.1 is found in the document [5] in References. It is reproduced here for convenience.

Application	Recommended Software Level Requirement
MiCloud Management Portal	6.1
MiVoice Business	8.0 SP3
MiVoice Business-Virtual	8.0 SP3
MiVoice Business Multi Instance	2.0 SP1
MiVoice Business-Express	8.0 SP2
MiCollab	8.0 SP2
MiCollab Next Gen Client	8.0.30X
MiVoice Border Gateway	10.0 SP2
MiCloud Management Gateway	5.0.6.0
Mitel Open Integration Gateway	4.0.37.0
MiContact Center Business	9.0
MiVoice Call Recording	9.1 SP4
Mitel Performance Analytics	2.2

To take advantage of the latest features, upgrade the platforms to the recommended versions stated above.

MiCloud Management Portal is compatible with older versions of Mitel platforms. For a list of backward compatible versions of Mitel platforms, refer to document [5] in References.

### 4.2 LAN/WAN Requirements

MiCloud Management Portal is deployed in several hosted topologies. Figure 2 and Figure 3 show two such topologies while document [1] in References describes more variations. Depending on the topology chosen, different network equipment and services are employed. Network design is a large subject and will not be covered in this Guide. Here major components specific to the needs of MiCloud Management Portal is discussed.

#### 4.2.1 Static IP Address

MiCloud Management Portal server requires a static IP address. Choose a static IP address that is routable on the network that MiCloud Management Portal is deployed. This IP address is required during installation or deployment of the MiCloud Management Portal server.

#### 4.2.2 DNS Servers

For VPN based deployments (Figure 3), where MiCloud Management Portal is in a different network than the customers' platforms, each network needs a separate DNS server to resolve FQDNs to local addresses. This is sometimes referred to as split DNS. Again, network design is a large subject and will not be covered here.

#### 4.2.3 NAT

For VPN based deployments (Figure 3), a NAT device is required for MiCloud Management Portal to communicate with the voice platforms and for customers to reach MiCloud Management Portal. NAT devices are discussed in sections 5.4 and 5.5.

### 4.3 Hardware and Software Requirements

#### 4.3.1 Support for Virtual Environments

MiCloud Management Web Portal is supported in virtualized environments. Product testing has been limited to VMware ESXi Servers. Supported versions of VMware are:

Application	Recommended Software Level Requirement
VMware ESXi	6.0, 6.5
VMware vCenter	6.0, 6.5

To learn more about deploying MiCloud Management Portal in a virtual environment (vMiCloud Management Portal), please refer document [6] in References.

#### 4.3.2 MiCloud Management Portal Server Requirements

##### **Software Requirements**

MiCloud Management Portal is a Linux based server application. It requires the following Linux operating system.

Software	Version
MSL	10.6.22.0 (64-bit)

If MiCloud Management Portal is deployed using the MiCloud Management Portal OVA, the correct MSL version is built into the OVA.

##### **Hardware Requirements**

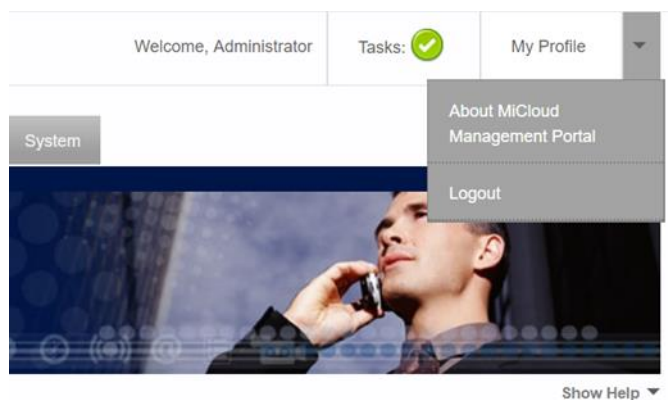
It is highly recommended that a dedicated physical server or dedicated virtual server instance be provided for the MiCloud Management Portal server. The *minimum* server requirements for MiCloud Management Portal is found in documents [6] and [7] in References. Search for the key word MiCloud Management Portal in those documents.

### Virtual Machine Requirements

Installation is done by importing the MiCloud Management Portal OVA file into a virtual environment. This is the simplest and quickest method of installing MiCloud Management Portal. It also ensures that all virtual machine settings are in accordance with Mitel recommendations. If MiCloud Management Portal must be installed manually in a virtual environment (i.e. starting with an MSL install and proceeding through a manual MiCloud Management Portal installation) then the installer must first configure the virtual machine to meet the requirements in document [6] in References.

#### 4.3.3 Browser Requirements

MiCloud Management Portal's service provider portal, customer administrator portal and end-user portal work with all three major browsers running on Windows. These are Mozilla Firefox, Microsoft Internet Explorer/Edge and Google Chrome. Mitel recommends upgrading to the latest versions of browsers to avoid security issues. Minimum browser versions supported are found in the *About MiCloud Management Portal* menu of the portal.

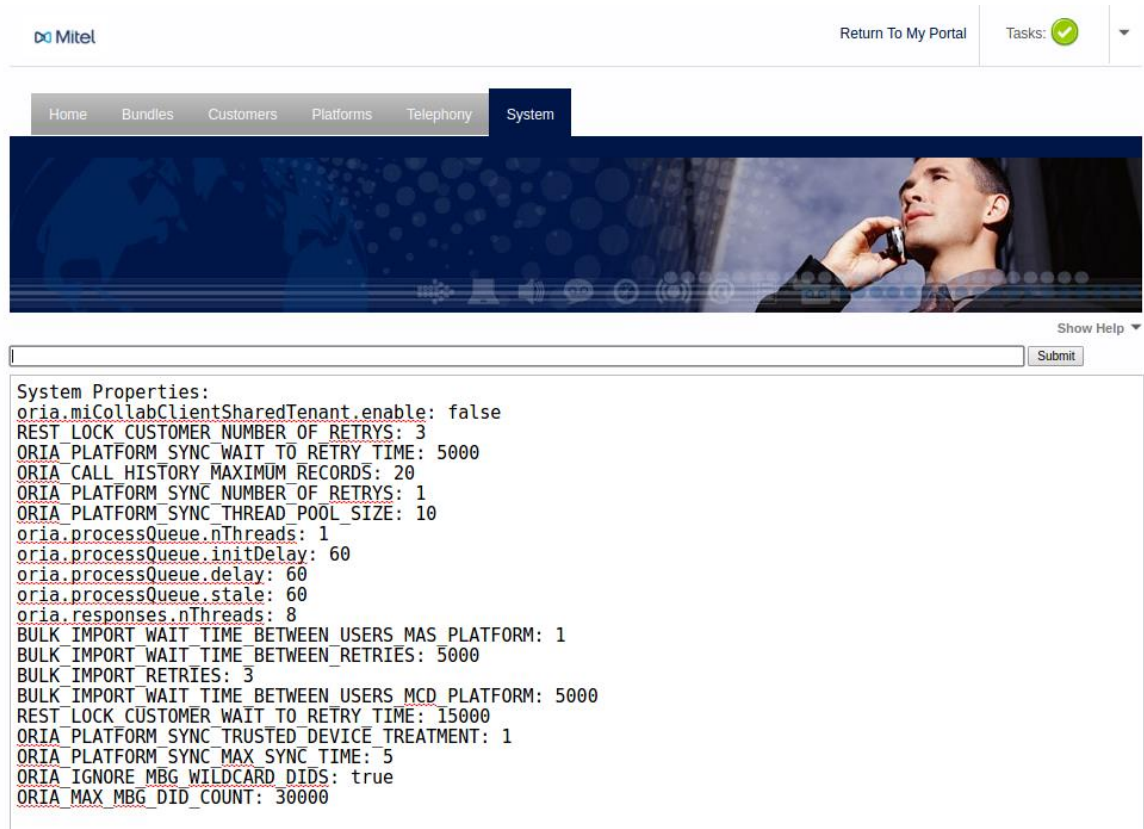


The customer administrator portal also runs on tablets that support Chrome, Firefox or IE/Edge. Smartphones are not yet supported.

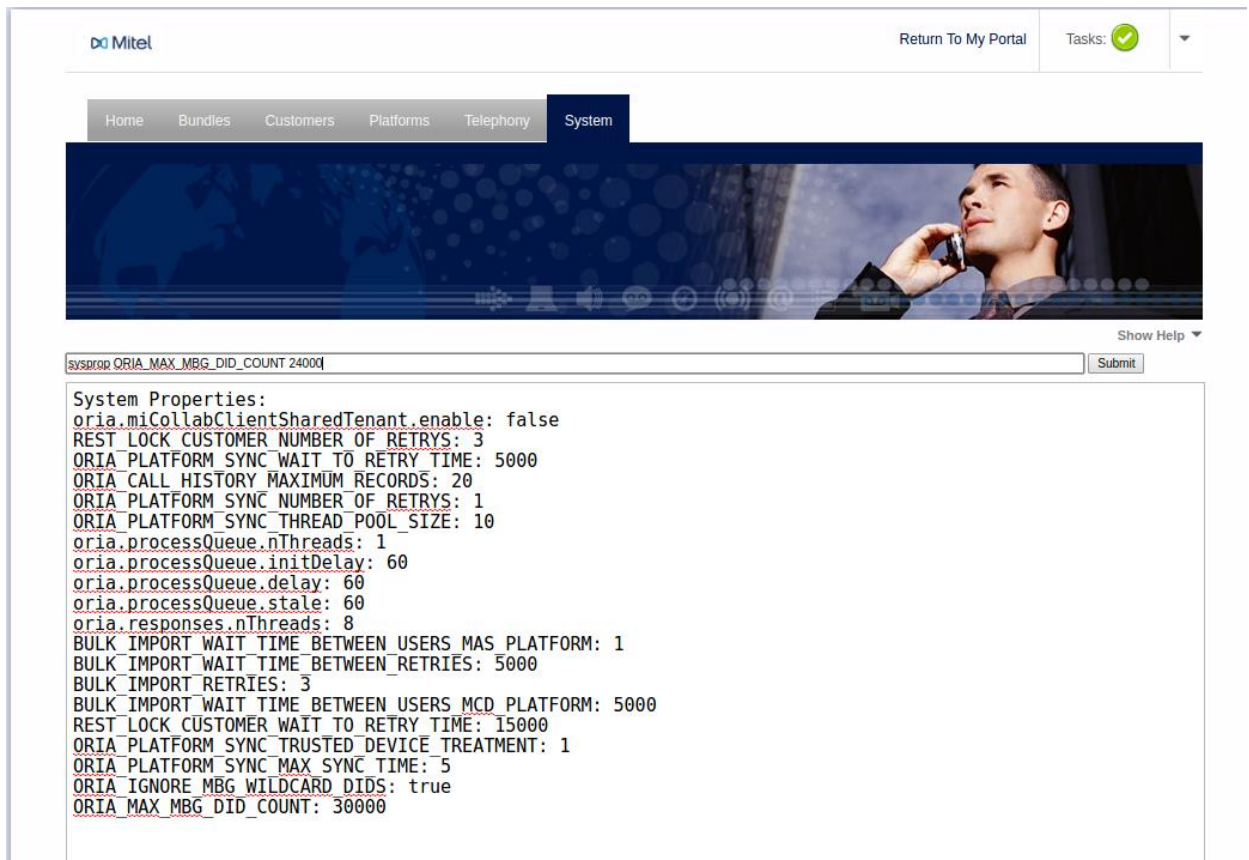
## 5 Configuration

### 5.1 System parameters and the sysprop maintenance commands

MiCloud Management Portal 6.1 makes modifying system parameters easier by providing a maintenance command called *sysprop*. Without any parameter, the *sysprop* maintenance command shows a list of existing system parameter and their values.



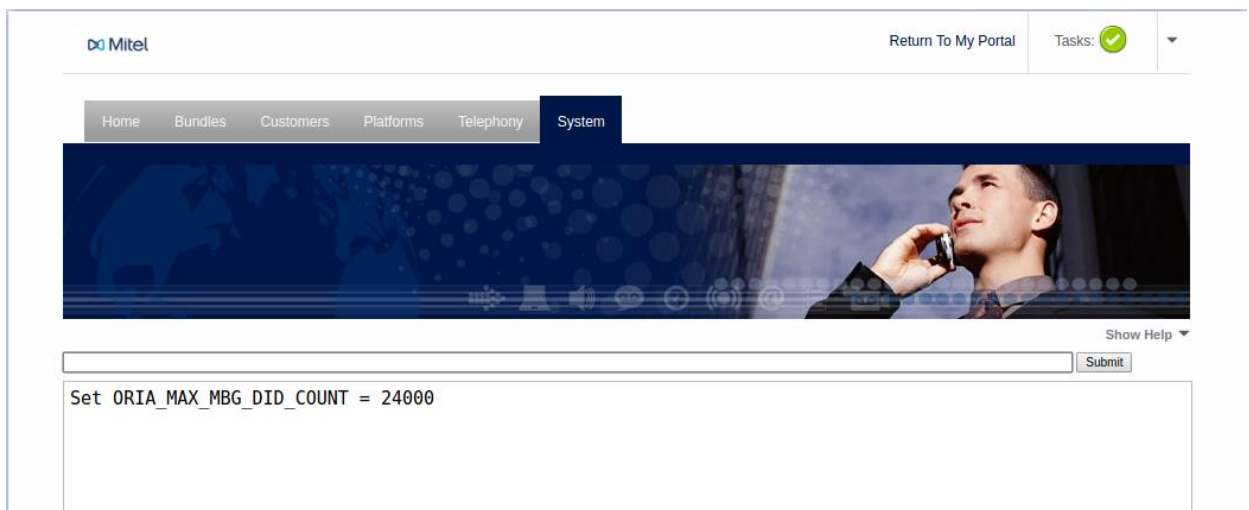
Here, we see that the parameter `ORIA_MAX_MBG_DID_COUNT` is set to 30000. To set it to 24000, execute the *sysprop* command with the name of the parameter followed by its value like so:



The screenshot shows the Mitel MiCloud Management Portal interface. At the top, there is a navigation bar with the Mitel logo, a "Return To My Portal" link, and a "Tasks" status indicator. Below the navigation bar, there is a menu with tabs for Home, Bundles, Customers, Platforms, Telephony, and System. The System tab is selected. A banner image of a man talking on a phone is displayed. Below the banner, there is a "Show Help" link. The main content area shows a command prompt with the command `sysprop ORIA_MAX_MBG_DID_COUNT 24000` entered. Below the command, there is a "Submit" button. The output of the command is displayed as a list of system properties:

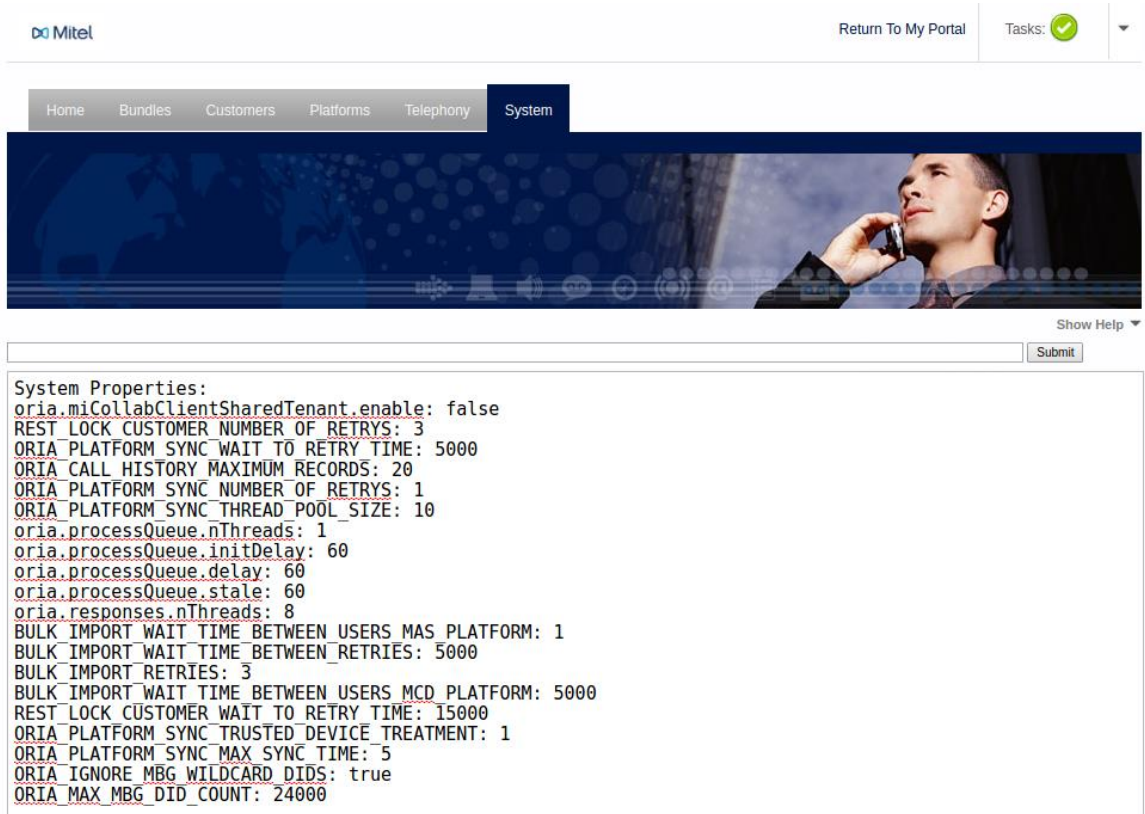
```
System Properties:
oria.miCollabClientSharedTenant.enable: false
REST_LOCK_CUSTOMER_NUMBER_OF_RETRIES: 3
ORIA_PLATFORM_SYNC_WAIT_TO_RETRY_TIME: 5000
ORIA_CALL_HISTORY_MAXIMUM_RECORDS: 20
ORIA_PLATFORM_SYNC_NUMBER_OF_RETRIES: 1
ORIA_PLATFORM_SYNC_THREAD_POOL_SIZE: 10
oria.processQueue.nThreads: 1
oria.processQueue.initDelay: 60
oria.processQueue.delay: 60
oria.processQueue.stale: 60
oria.responses.nThreads: 8
BULK_IMPORT_WAIT_TIME_BETWEEN_USERS_MAS_PLATFORM: 1
BULK_IMPORT_WAIT_TIME_BETWEEN_RETRIES: 5000
BULK_IMPORT_RETRIES: 3
BULK_IMPORT_WAIT_TIME_BETWEEN_USERS_MCD_PLATFORM: 5000
REST_LOCK_CUSTOMER_WAIT_TO_RETRY_TIME: 15000
ORIA_PLATFORM_SYNC_TRUSTED_DEVICE_TREATMENT: 1
ORIA_PLATFORM_SYNC_MAX_SYNC_TIME: 5
ORIA_IGNORE_MBG_WILDCARD_DIDS: true
ORIA_MAX_MBG_DID_COUNT: 30000
```

After you hit ENTER or click on the Submit button, the parameter is set to the specified value.



The screenshot shows the Mitel MiCloud Management Portal interface after the `sysprop` command has been executed. The command prompt now shows the confirmation message: `Set ORIA_MAX_MBG_DID_COUNT = 24000`. The "Submit" button is still visible. The rest of the interface, including the navigation bar, menu, and banner, remains the same as in the previous screenshot.

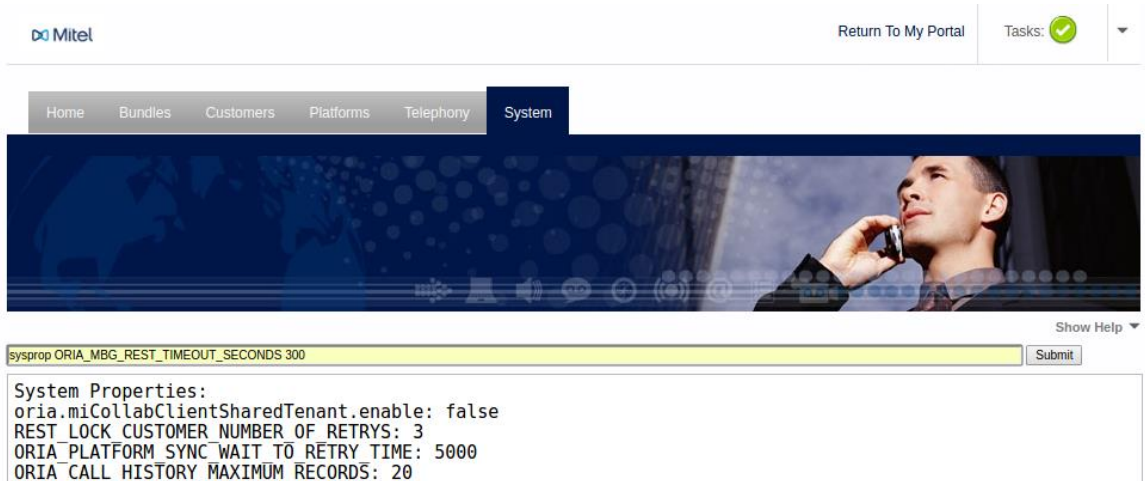
Executing `sysprop` again without any parameter confirms that the parameter was set correctly:



The screenshot shows the Mitel MiCloud Management Portal interface. At the top, there is a navigation bar with the Mitel logo, a "Return To My Portal" link, and a "Tasks" section with a green checkmark. Below the navigation bar is a menu with tabs: Home, Bundles, Customers, Platforms, Telephony, and System. The "System" tab is selected. The main content area features a banner image of a man talking on a mobile phone. Below the banner is a "Show Help" link and a "Submit" button. The central part of the page displays a list of system properties, each with a red underline indicating it is a link. The properties are as follows:

```
System Properties:
oria.miCollabClientSharedTenant.enable: false
REST_LOCK_CUSTOMER_NUMBER_OF_RETRYS: 3
ORIA_PLATFORM_SYNC_WAIT_TO_RETRY_TIME: 5000
ORIA_CALL_HISTORY_MAXIMUM_RECORDS: 20
ORIA_PLATFORM_SYNC_NUMBER_OF_RETRYS: 1
ORIA_PLATFORM_SYNC_THREAD_POOL_SIZE: 10
oria.processQueue.nThreads: 1
oria.processQueue.initDelay: 60
oria.processQueue.delay: 60
oria.processQueue.stale: 60
oria.responses.nThreads: 8
BULK_IMPORT_WAIT_TIME_BETWEEN_USERS_MAS_PLATFORM: 1
BULK_IMPORT_WAIT_TIME_BETWEEN_RETRIES: 5000
BULK_IMPORT_RETRIES: 3
BULK_IMPORT_WAIT_TIME_BETWEEN_USERS_MCD_PLATFORM: 5000
REST_LOCK_CUSTOMER_WAIT_TO_RETRY_TIME: 15000
ORIA_PLATFORM_SYNC_TRUSTED_DEVICE_TREATMENT: 1
ORIA_PLATFORM_SYNC_MAX_SYNC_TIME: 5
ORIA_IGNORE_MBG_WILDCARD_DIDS: true
ORIA_MAX_MBG_DID_COUNT: 24000
```

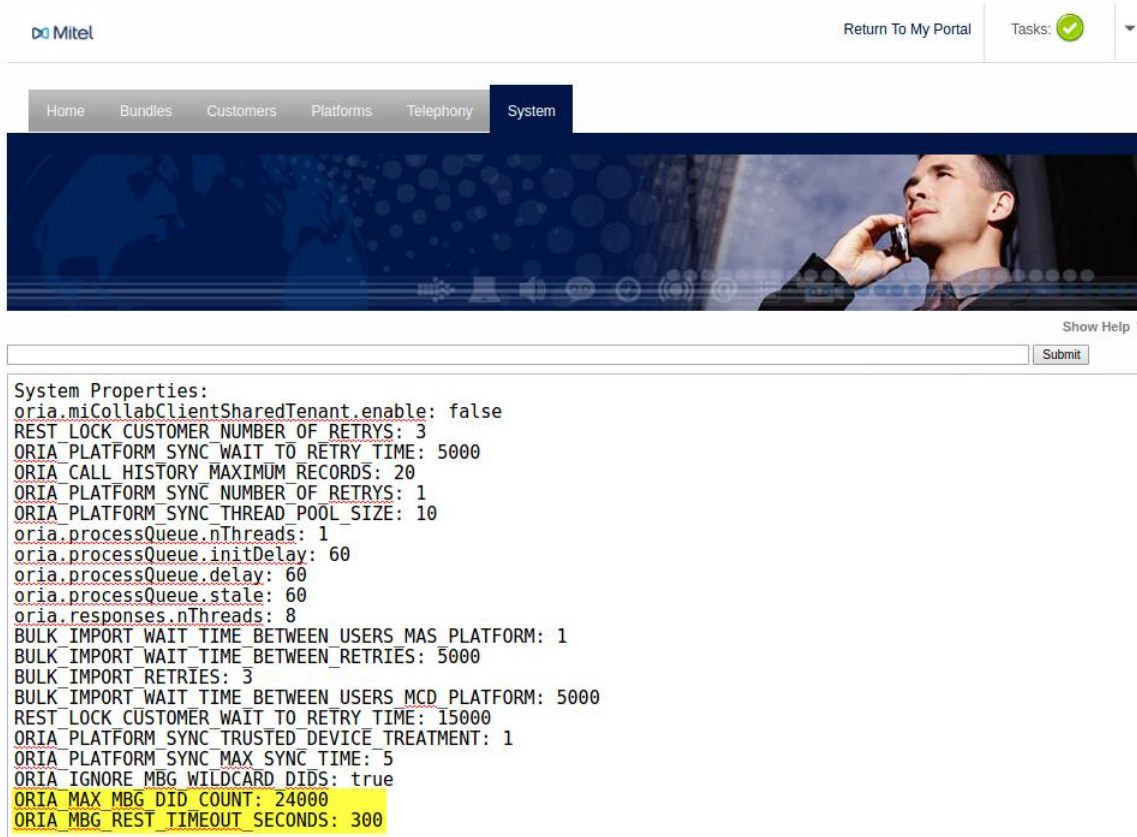
To set a parameter that currently does not exist, again execute the `sysprop` command with the name of the parameter and its value.



The screenshot shows the same Mitel MiCloud Management Portal interface as the previous one, but with a yellow highlight bar at the top of the main content area containing the command: `sysprop ORIA_MBG_REST_TIMEOUT_SECONDS 300`. Below the command bar is a "Submit" button. The system properties list is updated, showing only the properties that exist after the command execution:

```
System Properties:
oria.miCollabClientSharedTenant.enable: false
REST_LOCK_CUSTOMER_NUMBER_OF_RETRYS: 3
ORIA_PLATFORM_SYNC_WAIT_TO_RETRY_TIME: 5000
ORIA_CALL_HISTORY_MAXIMUM_RECORDS: 20
```

Now, both parameters are set correctly:



System Properties:

```

oria.miCollabClientSharedTenant.enable: false
REST LOCK CUSTOMER NUMBER OF RETRYs: 3
ORIA_PLATFORM_SYNC_WAIT_TO_RETRY_TIME: 5000
ORIA_CALL_HISTORY_MAXIMUM_RECORDS: 20
ORIA_PLATFORM_SYNC_NUMBER_OF_RETRYs: 1
ORIA_PLATFORM_SYNC_THREAD_POOL_SIZE: 10
oria.processQueue.nThreads: 1
oria.processQueue.initDelay: 60
oria.processQueue.delay: 60
oria.processQueue.stale: 60
oria.responses.nThreads: 8
BULK_IMPORT_WAIT_TIME BETWEEN USERS MAS PLATFORM: 1
BULK_IMPORT_WAIT_TIME BETWEEN RETRIES: 5000
BULK_IMPORT_RETRIES: 3
BULK_IMPORT_WAIT_TIME BETWEEN USERS MCD PLATFORM: 5000
REST LOCK CUSTOMER WAIT TO_RETRY_TIME: 15000
ORIA_PLATFORM_SYNC_TRUSTED_DEVICE_TREATMENT: 1
ORIA_PLATFORM_SYNC_MAX_SYNC_TIME: 5
ORIA_IGNORE_MBG_WILDCARD_DIDS: true
ORIA_MAX_MBG_DID_COUNT: 24000
ORIA_MBG_REST_TIMEOUT_SECONDS: 300

```

The `-d` option is used to delete a system property.

### 5.1.1 Some common system parameters

The `sysprop` command exposes system parameters. Changing these parameters changes the behaviour of MiCloud Management Portal. As such, care must be exercised when using this command. This command should only be used after consulting with Mitel MiCloud Management Portal Support.

The following table describes some of the system parameters that a site may wish to modify.

System Parameter	Default value	Description
ORIA_PLATFORM_SYNC_THREAD_POOL_SIZE	10	The number of concurrent threads that can synchronize MiCloud Management Portal with platforms for billing purposes. The default value (10) should be adequate for most sites.  If platform synchronization takes too long to complete and/or a site has hundreds of customers, this value can be increased. Note however that concurrent threads are expensive. If too much resources are dedicated to platform synchronization, other MiCloud Management Portal functions may be affected.
ORIA_CALL_HISTORY_MAXIMUM_RECORDS	20	The call history used in creating a device for a user.
ORIA_IGNORE_MBG_WILDCARD_DIDS	false	Works in conjunction with MICLOUD MANAGEMENT PORTAL_MAX_MBG_DID_COUNT parameter.

		<p>If set to 'true' new MBG DID rules are written at the end of the rule list.</p> <p>If set to 'false' new MBG DID rules have to be carefully inserted into the rule list above existing rules with wild cards that can supplant the new rules.</p>
ORIA_MAX_MBG_DID_COUNT	20000	The maximum number of DID rules that can be added when MICLOUD MANAGEMENT PORTAL_IGNORE_MBG_WILDCARD_DIDS is set to 'true'.
ORIA_MBG_REST_TIMEOUT_SECONDS	60	Timeout when working with the MBG's REST interface.
RAD_HUNTGROUPE_PHASE_TIMER	2	Phase timer value is used to program RAD hunt groups. The value is in seconds and applies to all customers. Range value: 1 to 99.
BIDIRECTIONAL_SYNC	true	To enable bidirectional sync: Sysprop BIDIRECTIONAL_SYNC true
BIDIRECTIONAL_SYNC	false	To disable bidirectional sync: Sysprop BIDIRECTIONAL_SYNC false
PORTAL_PASSWORD_MIN_LENGTH {value}	8	To modify minimum password length. Value is between 8-20.
REJECT_LAST_N_USED_PORTAL_PASSWORD	0	To restrict user to not to use previously used password. If value is zero, then no restriction. Maximum value is 10.

## 5.2 Port Usage

The following table list the ports MiCloud Management Portal listens on to serve its web portals.

Port	Function	Server	Note
80/443	Web portal	MiCloud Management Portal	<p>Users connect to MiCloud Management Portal.</p> <p>Port 80 redirects requests to secure port 443.</p>

The following table lists the ports of the various platform servers through which MiCloud Management Portal interacts.

Port	Function	Platform/Server	Usage
53	DNS	DNS Server	MiCloud Management Portal resolves host names.
443	Management API (MiXML)	MiVoice Business	MiCloud Management Portal uses this port to manage the MiVoice Business via its MiXML interface
10245-10250	Management API (Thrift)	MiCollab	MiCloud Management Portal connects to this MiCollab's API to manage users
10255-10260	Management API (Thrift)	MiCollab	MiCloud Management Portal connects to this MiCollab's API to manage users

Port	Function	Platform/Server	Usage
35600	Management API (REST)	Multi-tenant MiCollab Client Service (UCA)	MiCloud Management Portal connects to this UCA's API to manage accounts
443	Management API (REST)	MiVoice Border Gateway	MiCloud Management Portal connects to this MBG's API to manage devices and DIDs
443	Management API (REST)	MiVoice Border Gateway	MiCloud Management Portal connects to this MBG's API to manage devices and DIDs

Note, MiCloud Management Portal uses secure connections with all platform servers to protect data exchanges with them.

### 5.3 VLAN Support using Split DNS

With reference to section 3.2.2, each customer's VPN is a VLAN. The MiCloud Management Portal server is in a separate network; the service provider's (SP) network. Communication between the MiCloud Management Portal server and the platforms is facilitated by the NAT box in the figure.

Here are some details about this implementation:

- MiCloud Management Portal is deployed in the SP's management network.
- The platforms (MiCollab, MiVoice Business, MiVoice Business Express) to be provisioned by MiCloud Management Portal are deployed in an isolated VLAN for a given customer.

VLAN support in MiCloud Management Portal is accomplished through:

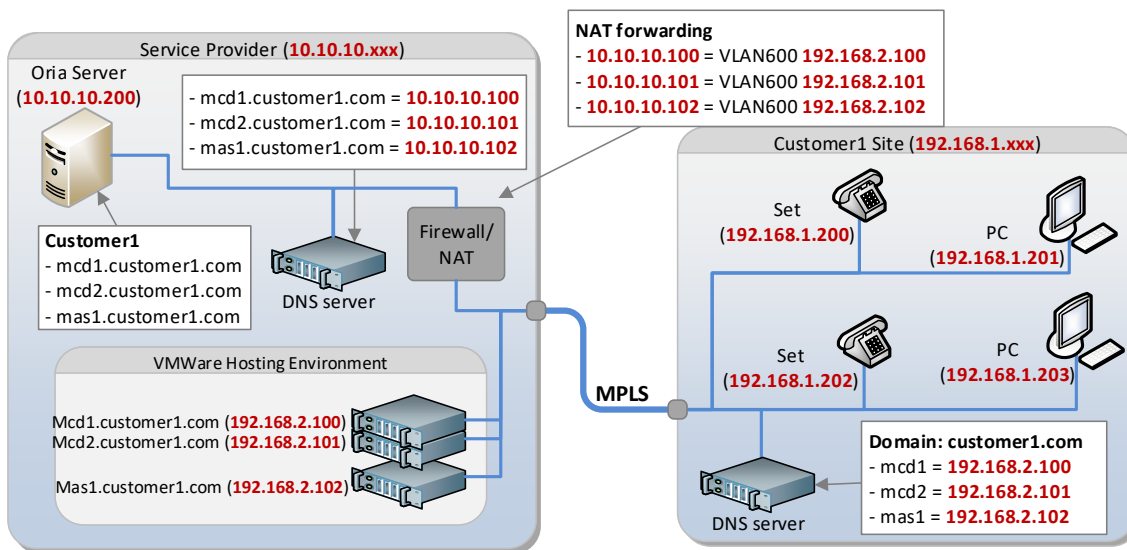
- The use of FQDN. Platform registration in MiCloud Management Portal are done using the FQDNs of the respective platforms
- With Flow Through Provisioning, the registration of MiVoice Businesses on MiCollab is done using IP addresses. Please refer to section 5.6 for details.
- The use of NAT between the SP's management network and the customer's VLAN.
- The use of a DNS in both the SP's management network and the customer's VLAN.

In the illustration below, all platforms for *custertomer1* are registered in MiCloud Management Portal using FQDNs, not IP addresses. In the SP's network, the DNS server translates the FQDNs of these platforms to IP addresses in the service provider address space (10.10.10.xxx).

On the customer site, the DNS server translates FQDNs of the same platforms to IP addresses in the customer's VLAN (192.168.2.xxx).

The use of different DNS servers resolving the same FQDN to different IP addresses, depending on which network the request originates from, is referred to as Split-DNS

In the hosting environment, IP addresses from the customer site are sufficient to reach the respective hosted platforms. However, IP addresses from the service provide need to be NATed from the service provider address space to the hosted VLAN addresses.



## 5.4 NAT with Mitel Management Gateway (MMG)

Mitel has a NAT product that can perform the necessary 1:1 NAT function represented by the NAT box in the figure above. Details of the MMG and how to configure it can be found in the section on *UCC Platform Deployment* of document [2] in References.

## 5.5 NAT with VMware vCloud Networking and Security

The NAT functionality can also be implemented using VMware vCloud Networking and Security product. For more information on vCloud Networking and Security, please refer to VMware's on-line materials on this product.

The following summarizes some considerations when installing and configuring vCloud Networking and Security:

- A provider needs to first create an IP reuse plan for the tenant spaces
- There are several options for edge deployment to support the 1:1 NAT function. For example:
  - vCloud deployment NAT from an Application network
  - vCloud deployment NAT from an Organization network
  - Direct vCenter deployment with port group backed networks

Providers need to evaluate the options for the best suitability.

- vEdge will deploy with a conflicting IP address on an interface. Make absolutely sure that no IP conflicts exist during vEdge deployment
- DNAT rules must be individual entries; range programming does not support true 1:1 NAT on the vEdge
- SNAT rules on the vEdge require a full vEdge reset after programming to take effect
- Split DNS must be used to support IP reuse between tenants

All Mitel vApps registered with MiCloud Management Portal must do so using a FQDN and not a straight IP to support the split DNS and NAT functionality.

## 5.6 Working with MiCollab Flow Through Provisioning

If a MiCollab platform has Flow Through Provisioning enabled, Management Host Names must be configured. More details on this can be found in References document [2], section *Upgrading MiCloud*.



Basically, each platform IP address in the customer's VLAN must be paired with an IP address in the management network. In the example below, a MiVoice Business platform whose address in the customer VLAN is 10.35.83.123 is paired with the address 216.123.21.25 in the SP's network. MiCloud Management Portal uses the address in the SP's network to talk to the MiVoice Business.

The following shows how to assign a management plane's IP address to a platform.

First, edit the platform and check the checkbox *Configure Management Host Names For This Platform*:

<input checked="" type="checkbox"/> <b>Configure Management Host Names for this Platform</b>	<i>Enable this option if there are platform resources in a customer network that is accessed through a Mitel Management Gateway, third party NAT or VCNS. Once this option is set, a platform cannot be taken out of this mode.</i>
<input type="checkbox"/> <b>Use Embedded MiVoice Border Gateway</b>	<i>If not selected, the MiVoice Border Gateway (MBG) embedded in the platform will not be available for use.</i>
<input type="checkbox"/> <b>License Reporting Only Mode</b>	<i>This platform will not be actively managed. It will only be registered for licence reporting purposes.</i>
<input type="checkbox"/> <b>Demo Mode</b>	<i>Registering a platform in demo mode creates a mock site. This platform can be assigned to a customer for demonstrating the portal without live MiVoice Business instances. NOTE: A demo platform can never be taken out of demo mode.</i>

Then for each MiVoice Business that is connected to this platform, a Management Host Name has to be provided. MiCloud Management Portal uses the Management Host Name address to communicate directly with the MiVoice Business.

Platform Details	MiVoice Business	SIP Billing Number	Sites	DIDs	Ranges	Auto Attendant
<b>Add/Remove MiVoice Business</b> <i>Register MiVoice Business instances for a platform. Enter an IP address or unique host name for the MiVoice Business server. For example, 192.100.1.2 or customer.cambria.com. If Configure Management Host Names For This Platform was set, both Management Host Name and Customer Host Name are required. The MiXML username and password must have root privileges to allow the Oria application to access the MiVoice Business.</i>						
MiVoice Business Name	Management Host Name	Customer Host Name	MiXML Username	MiXML Password		
Demo MCD	216.123.21.25	10.35.83.123	system	*****	 	
<div> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </div>						

## 5.7 MiVoice Border Gateway Configuration

MiCloud Management Portal includes support for managing DID rules and devices (Mitel phones, SIP, and UC clients) on a set of MiVoice Border Gateways assigned to a customer's MiVoice Business/MiCollab/MiVoice Business Express platform.

### 5.7.1 MiVoice Border Gateway Web Services

MiCloud Management Portal communicates with MiVoice Border Gateway servers via a web service interface that was introduced in MiVoice Border Gateway release 8.1. By default, the web services on the MiVoice Border Gateway are turned off. They must be explicitly turned on before the MiVoice Border Gateway is registered with MiCloud Management Portal. MiVoice Border Gateway releases prior to release 8.1 are not compatible with MiCloud Management Portal.

The web services are turned on by logging into the web admin console of the MiVoice Border Gateway server, locating and clicking on the *Web Services* category on the left, and clicking the *Start* button.

### 5.7.2 Registering MiVoice Border Gateway platforms

MiVoice Border Gateways must be registered with MiCloud Management Portal to be used for managing DID rules or for SIP and Mitel phones management. In cases where a cluster of MiVoice Border Gateways are used, only register the master<sup>2</sup> MiVoice Border Gateway. Do not register two MiVoice Border Gateways from the same cluster.

Who can register MiVoice Border Gateways?

- SPs can register MiVoice Border Gateways on behalf of VARs and Virtual Service Providers (VSP) through the *Login As* feature.
- VSPs can register MiVoice Border Gateways on their own by logging to their own portal.
- VARs cannot register MiVoice Border Gateways by logging in the portal.


Once a set of MiVoice Border Gateways have been registered, they can be assigned to platforms for DID routing or device management functions. If the MiVoice Border Gateway is stand-alone (i.e. not embedded in a MiCollab or MiVoice Business Express server) then the same MiVoice Border Gateway can be assigned to multiple platforms for both DID routing or device management.

Embedded MiVoice Border Gateways can be optionally automatically registered when the hosting MiCollab or MiVoice Business Express platform is registered. Those MiVoice Border Gateways are only available to the hosted platforms.



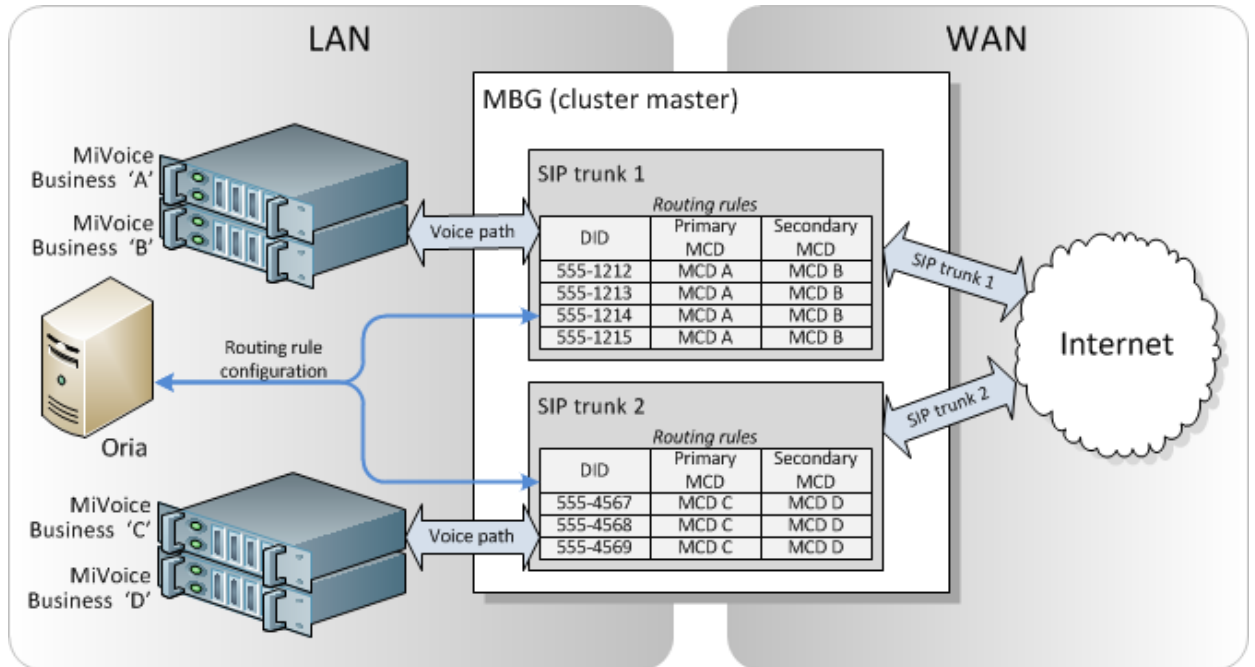
When MiCollab Client for Mobile for softphones are deployed and they are to be resilient the FQDN of the MiVoice Border Gateway cluster is used in place of the master MiVoice Border Gateway when a MiVoice Border Gateway cluster is registered. A thorough treatment of this subject is given in References document [8], section *Configure MiCloud Management Portal with FQDN/IP address of MiVoice Border Gateway*.

---

<sup>2</sup> The exception is in the case of MiCollab Client cy. See  in the last paragraph.

### 5.7.3 DID Routing

MiCloud Management Portal can maintain the DID routing rules for each SIP trunk on MiVoice Border Gateways. The following illustration shows a simplified configuration for discussion purposes:



The following are considerations when deploying MiVoice Border Gateways for DID routing under MiCloud Management Portal control.

- MiCloud Management Portal is responsible for managing routing rules for all SIP trunks on the MiVoice Border Gateway. The DIDs in the routing rule tables on the MiVoice Border Gateway correspond to DIDS set up in MiCloud Management Portal. For DIDs that are routed by the MiVoice Border Gateway, it is important that the correct SIP trunk be selected in MiCloud Management Portal when specifying DIDs for a platform. In the illustration above, DIDs 555-1212 to 555-1214 are associated with SIP trunk 1, and of course will not work at all if written to the routing rule table of SIP trunk 2.
- MiCloud Management Portal does not use DID rule wildcards (N, X, and \*). All DID rules are written as explicit phone numbers.
- Each platform group can have multiple MiVoice Border Gateways assigned for routing DIDs. Also, the same MiVoice Border Gateway can be assigned to several platform groups. In the illustration above, the pair **MiVoice Business A&B** can be in a different platform group than the pair **MiVoice Business C&D**, and thus the same MiVoice Border Gateway will be used by two customers for SIP DID routing.

The same MiVoice Border Gateway can be shared between SP, VSP and VAR however it should be registered separately for SP, VSP and VAR

- MiCloud Management Portal maintains some MiVoice Border Gateway state information required for the management of DID rules. In particular, if DID rules with wildcards are put in by another entity other than MiCloud Management Portal, MiCloud Management Portal keeps track of where wildcards are being used in the DID rules, in order that new rules are written above the wildcards. This prevents the wildcards from overriding explicit DIDs that contain no wildcards.

It is important that a MiVoice Border Gateway is not assigned to more than one MiCloud Management Portal system. Otherwise the DID ordering may be adversely affected when two MiVoice Border Gateways do near-simultaneous MiVoice Border Gateway DID rule assignments.

For the same reason, once MiCloud Management Portal is managing the DID rules on the set of MiVoice Border Gateways, it is highly recommended that DID rules are not edited via the MiVoice Border Gateway admin interface.

- MiCloud Management Portal does not support SIP trunk configuration on the MiVoice Border Gateway. All SIP trunks must be pre-provisioned on MiVoice Border Gateways before registering the MiVoice Border Gateways with MiCloud Management Portal. In the illustration above, SIP trunk 1 and SIP trunk 2 are configured via the MiVoice Border Gateway administration web interface, except for the actual DID routing rules.

There are 2 system parameters in MiCloud Management Portal that affect how the DID rule creation functions on the MiVoice Border Gateway:

- **MICLOUD MANAGEMENT PORTAL\_MAX\_MBG\_DID\_COUNT**

The MiVoice Border Gateway does not enforce any limits on the number of DID rules that can be assigned to a SIP trunk. This has caused problems in the past, when the number of DID rules approached about 20,000. The property MICLOUD MANAGEMENT PORTAL\_MAX\_MBG\_DID\_COUNT limits the number of DID rules per SIP trunk on all MiVoice Border Gateways managed by the MiCloud Management Portal server.

It is recommended to not let the number of DID rules per MiVoice Border Gateway SIP trunk exceed about 24000.

- **MICLOUD MANAGEMENT PORTAL\_MBG\_REST\_TIMEOUT\_SECONDS**

On heavily loaded systems, adding DID rules to MiVoice Border Gateway SIP trunks can take longer than the MiVoice Border Gateway interface allows. This causes client timeouts in MiCloud Management Portal, which appear as failures when in fact the DID rules are eventually successfully written to the database.

The default value for the timeout is 60 seconds. If DID rule creation results in timeouts, then the value can be increased. This number can be arbitrarily large; however, it will also affect the length of time before a disconnected server is detected.

It is recommended that the timeout should not exceed about 400 seconds.

Section 5.1 describes how to modify these and other system parameters.

#### 5.7.4 Mitel phone, SIP, and UC Device Management

MiCloud Management Portal release 3.3 introduced the concept of *sites*, which replaces the *phone systems* of previous releases. Whereas a phone system simply identified a primary and secondary MiVoice Business, a site adds to this the following:

- If to associate the platform device MiVoice Border Gateway to this site, and if so specify the following:
  - The MiVoice Border Gateway cluster zone
  - The MiVoice Border Gateway installer password.

- An optional default CESID, MiVoice Business zone and CPN

So essentially a site dictates if a Mitel phone, SIP, or UC set is registered on a MiVoice Border Gateway and which cluster zone it is assigned to. When properly set up, this insulates the customer administrator from having to know about or deal with MiVoice Border Gateways. Furthermore, it provides a way to automatically assign a default CESID and CPN simply by selecting a site for a user.

The following are considerations when deploying MiVoice Border Gateways for device management under MiCloud Management Portal control.

- MiVoice Border Gateways must be registered with MiCloud Management Portal in order to be used for device management.
- Each platform group can have a separate MiVoice Border Gateway assigned for each type of device (Mitel phones, SIP, and UC clients) or the devices can all be assigned to the same MiVoice Border Gateway. However, the same MiVoice Border Gateway can be assigned to several platform groups and thus is used by several customers.
- It is recommended that one or more MiVoice Border Gateways are used exclusively for the routing of SIP devices.

#### 5.7.5 Managing MiVoice Border Gateway Cluster Zones

MiCloud Management Portal requires a cluster zone specification when adding a Mitel phone to the MiVoice Border Gateway. However, at this time MiCloud Management Portal is not able to extract the cluster zone names from the MiVoice Border Gateway via the web services interface. Therefore, whenever a cluster zone is created on a managed MiVoice Border Gateway, the zone name must also be manually added to a XML file on the MiVoice Management Portal server. As long as the cluster zones on the MiVoice Border Gateway and in the XML file are manually synchronized, administrators will be able to correctly assign a MiVoice Border Gateway cluster zone when creating sites.

The file that contains MiVoice Border Gateway clusters zones can be found at the following location on the MiCloud Management Portal server:

```
/opt/dist_jboss/wildfly-  
10.1.0.Final/standalone/deployments/OriaEar.ear/KonosPortal.war/mbgZones.xml
```

It is helpful, but not essential, to have a bit of an understanding of XML when editing this file. Existing entries can be used as models when making manual updates. The general format to specify a set of zones for a MiVoice Border Gateway in this file is as follows:

```
<mbgCluster host="mymbg.mydomain.com">  
  <zone>Downtown</zone>  
  <zone>Uptown</zone>  
  <zone>Midtown</zone>  
</mbgCluster>
```

- The MiVoice Border Gateway is identified by its IP address or hostname, always in quotes, after the text **host=**
- Each zone is specified on its own line, between the text **<zone>** and **</zone>**
- The line containing **</mbgCluster>** is essential and must be included.
- Each MiVoice Border Gateway requires its own section, modeled on the above fragment.

Future releases of the MiVoice Border Gateway will provide a mechanism to extract the set of cluster zones from the server itself, making the XML file unnecessary.

## 5.8 MiCollab Client Multi-Tenant

MiCloud Management Portal includes support for managing MiCollab Client Multi-Tenant to a service provider's MiVoice Business platform.

### 5.8.1 MiCollab Client Multi-Tenant Web Services

MiCloud Management Portal communicates with MiCollab Client Multi-Tenant via a web service. By default, the web services on the MiCollab Client Multi-Tenant is turned on port 35600 and it is ready for MiCloud Management Portal to create tenants on MiCollab Client Multi-Tenant.

### 5.8.2 Registering MiCollab Client Multi-Tenant platforms

MiCollab Client Multi-Tenant must be registered with MiCloud Management Portal to be used for device and feature management.

MiCollab Client Multi-Tenant is not clustered. Multiple tenants are managed within the same server.

Who can register MiCollab Client Multi-Tenant servers?

- SPs can register MiCollab Client Multi-Tenant on behalf of VARs and VSPs through the *Login As* feature.
- VSPs can register MiCollab Client Multi-Tenant on their own by logging to their own portal.
- VARs cannot register MiCollab Client Multi-Tenant by logging in the portal.

MiCloud Management Portal allows a single MiCollab Client Multi-Tenant to be shared between several platforms (i.e. customers). The Tenant Id of the MiCollab Client Multi-Tenant however needs to be unique for each platform.

Once MiCloud Management Portal is configured to manage MiCollab Client Multi-Tenant, it is highly recommended that MiCollab Client Multi-Tenant is not managed directly via the MiCollab Client Multi-Tenant admin interface. Further, any default applications that may or may not be part MiCollab Client Multi-Tenant should not be directly used as well.

## 5.9 Generic Ranges for System Generated Numbers

The allowed minimum range of system generated numbers has been reduced from 200 to 50. Please note that if a lower range of numbers is used, there is a possibility that Call Flows and Auto Attendants may not be configured properly for Small Business.

## 5.10 Platform Synchronization for Billing

In the previous release i.e. MiCloud Management Portal 6.0 introduced the feature License Data Synchronization to maintain accurate billing data when changes are made directly on the platforms. This feature systematically reads information from all platform elements and reconciles the data with the information in the database of MiCloud Management Portal.

Synchronization takes time and consumes system resources. We recommend that to minimize impact, License data Synchronization should be scheduled to run during off-peak hours. The details of how to schedule synchronization and report generation are found in [4]. A site with many customers may wish to perform a manual sync to find out roughly how long it would take to do a sync. Depending on the number of customers, this may take several hours. The results are documented in the sync report, which is produced at the end of a successful sync. With this information, a synchronization can be scheduled to run automatically during off-peak hours.

If synchronization takes longer than required, a site with many customers may wish to adjust the number of synchronization threads, which may reduce the sync time. The number of synchronization threads is controlled by the system parameter MICLOUD MANAGEMENT PORTAL\_PLATFORM\_SYNC\_THREAD\_POOL\_SIZE. Refer to section 5.1.1 of this document for details.

## 6 Performance Specifications

Here are some performance limits of MiCloud Management Portal:

Limit	Value
Number of customers	1000
Number of end users	100,000
Number of end users per customer	5000
Concurrent administrator users <sup>3</sup>	80

Table 1 - User limits.

MiCloud Management Portal call flows use MiVoice Business's call rerouting resources to create call flow branches, as such call flow limits depend on the number of call rerouting resources available:

Limit	Value
Total number of branches (call rerouting resources available for call flows)	156
Number of branches per call flow	3
Number of call flows with 3 branches	52

Table 2 – Call flow limits.

### 6.1 MiVoice Border Gateway performance

A MiVoice Border Gateway can be shared amongst many MiCloud Management Portal customers so the number of DID rules and phones can be quite large. The higher the number of DID rules, the slower the MiVoice Border Gateway responds to MiCloud Management Portal. To keep response time reasonable, apply the operational limits detailed in section 5.7.3.

### 6.2 MiCollab Client Multi-Tenant performance

Here are some performance limits of a MiCollab Client Multi-Tenant server.

- Up to a maximum of 250 tenants.
- Up to a maximum of 25,000 devices in total.
- Up to a maximum of 12,500 users in total, with a single tenant not exceeding 5000 users at max 2 devices per user. The more users per tenant, the fewer tenants in total.

Refer to References document [9] for engineering guidelines for this product.

<sup>3</sup> MiCloud Management Portal has been tested with 20 administrator users logged in and performing their management tasks.

### **6.3 Spectre and Meltdown mitigation impact**

Inclusion of updates to mitigate the Spectre and Meltdown (Side Channel Analysis) vulnerabilities has an impact on the import time duration of the MiCloud Management Portal product. There is an additional delay of 2-3 seconds in the IO transactions per user (based on 3 phones per user), which scales linearly with increasing number of users. Measurements suggest a minor, but insignificant increase in CPU usage. This increase is minor when compared to the background activity.

Measurements with bulk import of 500 and 1000 users (3 phones per user) suggests the time increase is between 5 to 10% respectively. Increasing the quantity of users to larger numbers results in a time impact of up to 30%. Majority of the customer imports are based on smaller customer deployments, typically below 500 users, and therefore below 5% impact.

## 7 Administrators

### 7.1 Service provider administrators

MiCloud Management Portal is shipped with one default administrator account whose default login credentials are system/password. The password of this default administrator can be changed.

The default administrator account can create additional service provider administrator accounts with different operation profiles. Administrator roles can be implemented this way. Following is an example of operation profile.

Role Details Responsibilities

#### Select Responsibilities

To provide users with access to the system management features available through the portal, use the options below to select all that apply for this Operations Profile.

	Feature	Create	Modify	Delete	Login As	Description
<input checked="" type="checkbox"/>	Bundles	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	Provide control to create, modify and delete bundles that define the feature access for users.
<input checked="" type="checkbox"/>	Customers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enable user to create, modify or delete customers from the portal and view customer details.
<input checked="" type="checkbox"/>	Resellers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	You can create, modify or delete resellers that can be assigned groups of MiVoice Business for resale to customers. View the details of service provided to existing resellers.
<input checked="" type="checkbox"/>	Platform Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	Provide control to register MiVoice Business instances with the portal or view and modify the existing instances.
<input type="checkbox"/>	Brands	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	-	Provide access to create and modify the Brands assigned to customers.
<input checked="" type="checkbox"/>	Advanced	-	<input checked="" type="checkbox"/>	-	-	The Advanced feature allows a service provider user to configure the data center email server, setup the MiCloud Management Portal whitelist, and obtain MiCloud Management Portal server logs. Reseller users can only access MiCloud Management Portal server logs with this feature.
<input checked="" type="checkbox"/>	Background Task Results	-	<input checked="" type="checkbox"/>	-	-	The Background Task Results feature gives the results of the background operations
<input checked="" type="checkbox"/>	Phone Capabilities	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	Register Dialing Privileges (CORs) and Feature Profiles (COS) which set the phone features an assigned user can access.
<input checked="" type="checkbox"/>	Billing	-	-	-	-	Provide user with access to billing information including bundle usage details.
<input checked="" type="checkbox"/>	Default	-	<input checked="" type="checkbox"/>	-	-	The feature allows a service provider user to configure the default values for MiVoice Business.

### 7.2 Customer administrators

Service providers create customers, each with its own customer administrator user. These administrator users are assigned an administrator bundle whose permissions allow the users certain rights. Following are the permissions of one such administrator bundle.

Bundle Details

Features

### Select Features

To provide users with access to site administration features on the portal, select the applicable options from the list below.

	Feature	Create	Modify	Delete	Description
<input checked="" type="checkbox"/>	Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Provides access to the directory to create, modify and delete a customer's users.
<input checked="" type="checkbox"/>	Call Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enable user to create, add or remove users to Pickup Groups, Hunt Groups, and Ring Groups.
<input checked="" type="checkbox"/>	Hot Desk Phones	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Allows users to create, modify and delete hot desk devices
<input checked="" type="checkbox"/>	Key Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Manage and assign customer key templates.
<input checked="" type="checkbox"/>	Company Speed Dial	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enable user to create, modify and delete company wide speed dial numbers.
<input checked="" type="checkbox"/>	ACD Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The ACD Group feature allows you to create groups of users that can be placed in call paths such as those used by call center and support groups.
<input type="checkbox"/>	Advanced ACD Groups	-	-	-	Enable the user to have access to all the advanced acd features in ACD groups.
<input checked="" type="checkbox"/>	ACD Paths	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The ACD Path feature allows you to create, modify and delete ACD Paths that are used by call centers and support groups.
<input type="checkbox"/>	Advanced ACD Paths	-	-	-	Enable the user to have access to all the advanced acd features in ACD Paths.
<input type="checkbox"/>	ACD Music On Hold	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enable user to create, add or remove Music on Hold for ACD.
<input type="checkbox"/>	RAD Programming	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enable user to create, add or remove RAD greetings.

Further, additional customer administrators can be created by the first customer administrator. These additional administrators are assigned different administrator bundles to give them different roles.

## 8 Security

This section of the document is of interest to personnel who are responsible for ensuring the secure deployment and secure operation of the MiCloud Management Portal (MMP) system.

Security is an integral part of the MiCloud Management Portal system design; this document describes the MiCloud Management Portal security features in detail and provides recommendations as to how the administrator should configure the security features to ensure a secure MiCloud Management Portal deployment.

The MiCloud Management Portal security features are either enabled in the system by default, enabled during the installation/configuration phase of the system, or need to be enabled manually by the system administrator when the MiCloud Management Portal system is initialized.

The MiCloud Management Portal system security measures are mainly based on the following open standard technologies and access mechanisms:

- Transport Layer Security (TLS): TLS provides secure access to MiCloud Management Portal.
- Secure Shell (SSH): SSH provides secure console-based access to MiCloud Management Portal for additional configuration needs.
- To Configure identity and access management policies, ensure all the end user and administrator accounts, roles, permissions and passwords are secure.

Other mechanisms that can be employed to protect the MiCloud Management Portal system are based on the following:

- A securely designed corporate Local Area Network (LAN) infrastructure
- Configuration of internal and external public facing routers and firewalls

Further, MiCloud Management Portal as an application has security features that address identity, authentication, encryption, access and authorization.

In addition to the security recommendations described in this document, there are several general security aspects that must be covered and addressed by the system administrator and/or the Information Technology (IT) security officer.

Every organization must have defined IT security policy in place, defining goals, assets, trust levels, processes, incident handling procedure, etc. The security mechanisms available in MiCloud Management Portal must be covered by and deployed according to this policy.

An important security measure is to establish and maintain physical security. Only authorized personnel must have access to server locations, since many data-exposure attacks are mounted by having physical access to a host.

Further, the IT data infrastructure must be designed with security in mind. Security mechanisms and protocols must be enabled and all the components of the entire system must be configured, maintained and updated as necessary.

Documents for MiCloud Management Portal and other Mitel® products are available on the Mitel eDocs web site ([edocs.mitel.com](http://edocs.mitel.com)) with a Mitel Online account. You can get a list of documents in the section 1.2 References.

## 8.1 Identity and Authentication

To ensure privacy and maintain system integrity, access to MiCloud Management Portal is restricted by a login password to those users that are identified and authenticated.

The passwords are auto generated and sent via email to users directly to provide an added level of security.

Password rules are set in place for a secure password and the user session is terminated after an inactivity period.

### Recommendations:

- Strong password setting must be used.
- Make sure to change the default Service Provider Portal Admin account password on first time login.

Refer to *Installation and Administration Guide*, Release 4.1 for Service Provider Admin accounts.

## 8.2 Access and Authorization

For privacy, all personal data processing is protected with role (or bundle) based access and authorization controls.

For system integrity and reliability, including the controls that protect privacy, all system data processing, and all access to databases, files and operating systems, are protected with role based access and authorization controls. For details on administrator users, refer to section 7 Administrators.

MiCloud Management Portal provides third party client access to MiCloud Management Portal via REST APIs. These API follow similar access authorization as administrators.

### Recommendations:

- Create administrators for specific operations by selecting the required features during bundle creation.
- Temporary administrative roles must be created to support maintenance and/or troubleshooting activities. These administrators are deleted once the activities have completed.
- When a user is not in the service of the company, the administrator should delete the user from MiCloud Management Portal.
- Protect the admin credentials while using the client REST APIs.

## 8.3 Audits and Logs

MiCloud Management Portal system logs are comprehensive, by logging all the activities in the MiCloud Management Portal's portals.

## 8.4 Network Settings

The MSL platforms on which MiCloud Management Portal runs provide network interfaces and as a result they have security related network settings. These settings are discussed in this section. For details on Network Settings, refer to document [6] in References.

### 8.4.1 LAN 2 Settings

This LAN 2 is not configured and is disabled by default.

**Recommendation:** Unless required, it is recommended that the interface is disabled.

### 8.4.2 WAN Settings

The *WAN Settings* is disabled by default.

**Recommendation:** Unless required, it is recommended that the interface is disabled.

### 8.4.3 Remote Access

There is only Local LAN access available to the server. Portal access from the internet is via web proxy.

## 8.5 Anti-Virus Protection

MiCloud Management Portal software is installed on top of the Mitel Standard Linux (MSL) operating system. Compared to common operating systems, MSL provides a reduced attack surface. This reduced attack surface is the result of the following MSL characteristics:

- MSL does not support email
- MSL does not support internet Web browsing
- Users with write permissions are limited and access is strictly controlled
- Mitel has removed unnecessary files and packages from MSL
- Mitel has closed unnecessary IP Ports

In general, a platform that is both physically secure and installed in network that is securely designed and less prone to be infected when compared to a platform that lacks physical security and/or is installed in a network lacking security controls.

### 8.5.1 Use of Antivirus Software

The use of antivirus software is widely accepted in the IT industry for use on servers, end user mobile platforms and desktops. Mitel cannot guarantee that third party antivirus software will not affect the performance of the MiCloud Management Portal application, and Mitel does not offer any endorsements of antivirus software vendors, or evaluations of antivirus products.

If a customer requires technical support from Mitel related to antivirus software installed in a system, then Mitel requires the software to be removed before troubleshooting the problem.

## **8.6 Software Patch Management Policy**

It is necessary for the administrator to ensure that MiCloud Management Portal system is always updated and equipped with all critical patches to guarantee the highest level of security. Mitel has developed best practices for the management and installation of security patches released by the operating system vendors aiming to guarantee the highest level of security and the proper functioning of the system.

## **8.7 LAN Security**

MiCloud Management Portal and associated platforms communicate using the corporate LAN infrastructure, which is based on the IEEE 802.3 (Ethernet) standard.

LANs are usually a relatively open environment, and communications can be easily intercepted, eavesdropped, and hijacked, if counter measures are not taken when setting up the network.

### **8.7.1 Network Access Security**

It is recommended that the system administrator ensure that the L2 switch access control measures are properly configured and maintained.

### **8.7.2 Using VLANs to Assist with Security**

To make eavesdropping attacks or Denial of Service attacks more difficult, or less effective, traffic on the LAN should be grouped according to traffic types and trust levels. This can be achieved with the use of Virtual LANs.

## **8.8 Security Certificates**

The use of public certificates is recommended.

Refer to *MSL Installation and Administration Guide* to install Web Server Certificate.

## 9 Best Practices

Mitel recommends the following best practices.

### 9.1 Reassigning platforms

When platforms such as MiVoice Businesses are reassigned to new customers, some programming artifacts from previous customers may remain. This may cause unwanted behaviours for new customers.

Do not re-use the existing platforms for new customers since the information of the old customer is inadvertently exposed to the new customer. Delete the instance of the old customer and create a new instance for the new customer.

### 9.2 Importing large number of users

Importing users into the system is done through the MiCloud Management Portal Bulk Import Spreadsheet, which provides a blank template. The generated template has tabs for the different service bundles supported. The administrator then manually populates the spreadsheet, one bundle at a time. Currently, due to performance limitations, there is a limit of 2500 users per import. If more than 2500 users are to be imported, the best practice is to import them in batches of 2500.

## 10 Glossary

<b>ACD</b>	<b>Automatic Call Distribution.</b> A package of advanced call processing features, relating to groups of agents who handle calls and agent supervisors.
<b>CESID</b>	<b>Customer Emergency Services Identifier.</b> A means of correlating a user and a directory number to information stored in a physical location data base.
<b>COS</b>	<b>Class of Service.</b> Defines the permissions an extension will have on a PBX or Centrex.
<b>CPN</b>	<b>Calling Party Number.</b> What is used as the calling party number when making outgoing calls.
<b>CPU</b>	<b>Central Processing Unit.</b> The hardware within a computer that carries out the instructions of a computer program by performing the basic arithmetical, logical, and input/output operations of the system.
<b>DID</b>	<b>Direct Inward Dialing.</b> Also known as direct-dial-in or DDI. In DID service the telephone company provides one or more trunk lines to the customer for connection to the customer's PBX and allocates a range of telephone numbers to this line (or group of lines) and forwards all calls to such numbers via the trunk.
<b>EMEM</b>	<b>Embedded Mitel Express Messenger.</b> The built-in voice messaging system in an MiVoice Business software load.
<b>ESM</b>	<b>Embedded System Manager.</b> The web-based management interface for the 3300 and MiVoice Business class of PBX.
<b>EHDU</b>	<b>External Hot Desk User.</b> An off-premises hot-desk user.
<b>HDD</b>	<b>hard Disk Drive.</b> A data storage device used for storing and retrieving digital information using rapidly rotating disks (platters) coated with magnetic material.
<b>IEEE</b>	<b>Institute of Electrical and Electronics Engineers.</b> A technical professional society promoting the development and application of electrotechnology and allied sciences.
<b>IO</b>	<b>Input Output.</b> Input output operation.
<b>IP</b>	<b>Internet Protocol.</b> A protocol that specifies the format of data packets (also called datagrams) on a network, and the addressing scheme
<b>MMP</b>	MiCloud Management Portal is an application that allows to provision and administer customers and users. It includes a portal for the Service Provider and one for the Customer Administrator.
<b>MiCollab</b>	A Mitel product that provides unified communication features such as messaging, collaboration, softphone clients, mobile clients as well as border gateway. Previously known as MAS.
<b>MiCollab Client</b>	This is one the the applications of the MiCollab product. It provides softphone clients, mobile clients functionality. Previously known as UCA.
<b>MiNET</b>	A proprietary stimulus protocol that carries keystroke information from a telephone set to a call control server. It can also be used to carry information to the set for the control of simple text displays.
<b>MiVB</b>	MiVoice Business. Previously known as the 3300 or the MCD.
<b>MiVBG</b>	<b>MiVoice Border Gateway.</b> Previously known as the MBG. Mitel's platform for secure deployment of multiple services, including Teleworker, Sip trunking, secure call recording, web proxy, and remote management.
<b>MiVB-X</b>	MiVoice Business Express. Previously known as the vUCC.

<b>MSL</b>	Mitel Standard Linux
<b>OVA</b>	<b>Open Virtualization Archive.</b> An open standard for packaging and distributing virtual appliances or more generally software to be run in virtual machines.
<b>PBX</b>	<b>Private Branch Exchange.</b> A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines
<b>RAM</b>	<b>Random Access Memory.</b> Volatile computer memory that holds instructions and data.
<b>SIP</b>	<b>Session Initiation Protocol.</b> A signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over IP networks.
<b>UC</b>	<b>Unified Communications.</b> The integration of real-time communication services such as instant messaging , presence information, telephony (including IP telephony), video conferencing, data sharing, call control and speech recognition with non-real-time communication services such as voicemail, e-mail, SMS and fax.
<b>UCA</b>	<b>Unified Communications Advanced.</b> This is an obsolete acronym representing the MiCollab Client Service.
<b>VAR</b>	<b>Value Added Reseller.</b> A company that adds extra features to products it has bought before selling them on.
<b>VLAN</b>	<b>Virtual Local Area Network.</b> A single layer-2 network partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain.
<b>VM</b>	<b>Voicemail.</b> A computerized system for answering and routing telephone calls.
<b>VPN</b>	<b>Virtual Private Network.</b> An extension of a private network across a public network, such as the Internet.
<b>VSP</b>	<b>Virtual Service Provider.</b> A company that offers services under its own company or brand name, while actually using the equipment and facilities of another service provider to provide those services.
<b>VoIP</b>	<b>Voice Over IP.</b> A technology that allows telephone calls to be made over data networks using IP technology.
<b>XML</b>	<b>Extensible Markup Language.</b> A set of rules for encoding documents in a format that is both human-readable and machine-readable.



mitel.com

Copyright 2020, Mitel Networks Corporation. All Rights Reserved.  
The Mitel word and logo are trademarks of Mitel Networks Corporation.  
Any reference to third party trademarks are for reference only and Mitel makes no representation of the ownership of these marks.