# MiCloud Management Portal Engineering Guidelines

NOVEMBER 2017

RELEASE 6.0

**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 particular 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.



TRADEMARKS



MiCloud Management Portal
Engineering Guidelines
Release 6.0
November 2017

# Table of Contents

# 1 About this Document

## 1.1 Overview

This document provides engineering guidelines to assist in the planning and installation of MiCloud Management Portal. 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 4.0, Mitel, 2017.

[2] MiCloud Business Virtual for Service Providers, Deployment Guide, Mitel, 2017.

[3] MiCloud Business Multi-Instance for Service Providers, Deployment Guide, Mitel, 2017.

[4] MiCloud Business for Service Providers Help 4.0, Mitel, 2017, http://edocs.mitel.com/UG/en/MiCloud/4.0/Service_Provider_Portal_Help/Provision_Customers.html.

[5] MiCloud Management Portal Release Notes, R6.0, Mitel, 2017.

[6] Virtual Appliance Deployment, Solutions Guide, Mitel, 2016.

[7] Mitel Standard Linux Qualified Hardware List, Mitel, 2016.

[8] MiCollab Client for Mobile Resiliency Guide, Release 7.3, Mitel, 2017.

[9] MiCollab Client Engineering Guidelines, Release 7.3, Mitel, 2017.

[10] MiCloud Management Portal Engineering Guidelines (this document), Mitel, 2017.

For the latest versions of the above materials, please go to Mitel Connect at http://connect.mitel.com. You will need a valid user name and password to access this site.

# 2 System Overview

MiCloud Management Portal 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'[1] 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 (also called a bundle).

MiCloud Management Portal 6.0 is included as part of the MiCloud 4.0 release. MiCloud Management Portal could also be deployed independently outside of MiCloud. For a good understanding of MiCloud, please refer to reference documents [1], [2] and [3] in section 1.2 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

[1] Definition: https://www.techopedia.com/definition/1034/swivel-chair-interface

- Customer Administrator:
  - User Management
  - Assign DIDs
  - Call Rerouting
  - Call Groups (Hunt, Ring, Page, Pickup)
  - 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 MiVB data on behalf of the customer. Customers no longer need to configure their MiVBs directly.

Please note that the new Bidirection Synchronization feature does not work with MiVB platforms. When configuration changes are made directly to an MiVB 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 MiVB. These conditions should be avoided when possible.

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

MiCloud Management Portal can manage users on a MiCollab or a MiVB-X. MiCloud Management Portal can also manage NuPoint mailboxes for call groups on these platforms. The current user update capabilities for a MiCollab or a MiVB-X 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 MiVB-X.

MiCloud Management Portal 6.0 introduces Bidirection Synchronization and License data Synchronization. These features work with MiCollab and MiVB-X platforms to synchronize modifications to users made directly on the platforms. There are limitations to what can be synchronized. The details of this feature are found in [4].

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

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

- As DIDs are created in MiCloud Management Portal, these can be written to a 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 Gateways are treated as separate platform items, in that they are registered by administrators and then allocated to voice platforms (MiVB/MiCollab/MiVB-X) as required. A stand-alone MiVoice Border Gateway can be 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 MiVB-X platform can only be 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 will create a unified communications account on the assigned MiCollab Client Multi-Tenant server.

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

## 2.6 Features introduced in this release

A complete list of new features can be found in reference documents [4] and [5]. Important features that can impact this guidelines include:

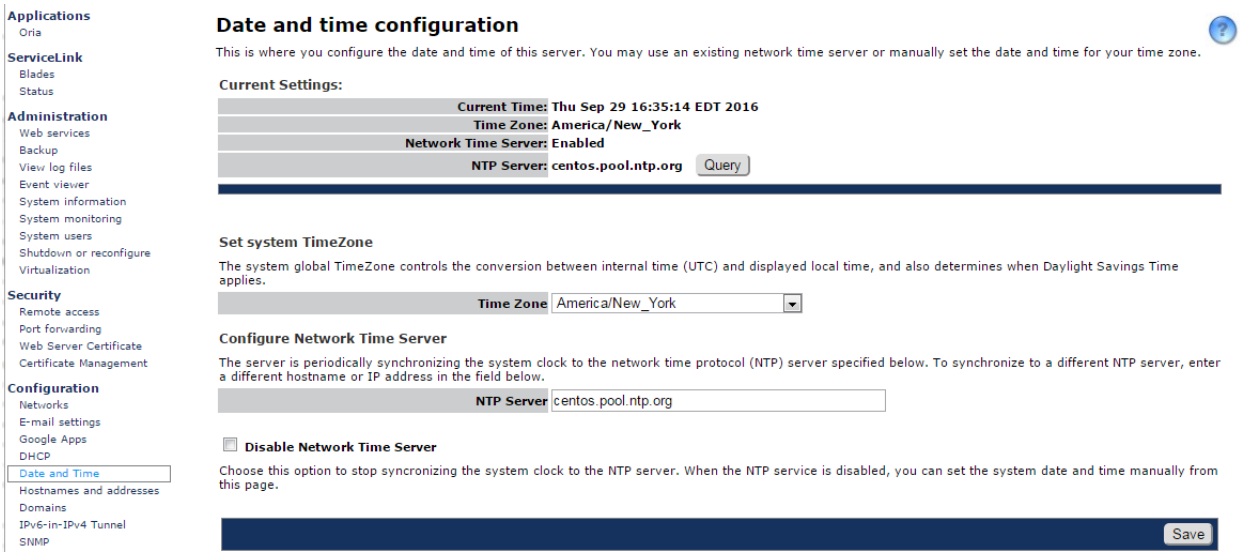
- Bidirection Synchronization
- License data Synchronization
- Enhanced license reporting
- Performance improvements in bulk import

# 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 OS on which MiCloud Management Portal runs and can be found when you log in to the server-manager address. The figure below shows the Date and Time menu.




## 3.2 Deployment Topologies

Reference document [1] gives a very good description of the different MiCloud deployment topologies. It is well worth reading that 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 diagram, any server instance (include the MiCloud Management Portal server) can be a physical or virtual computer.

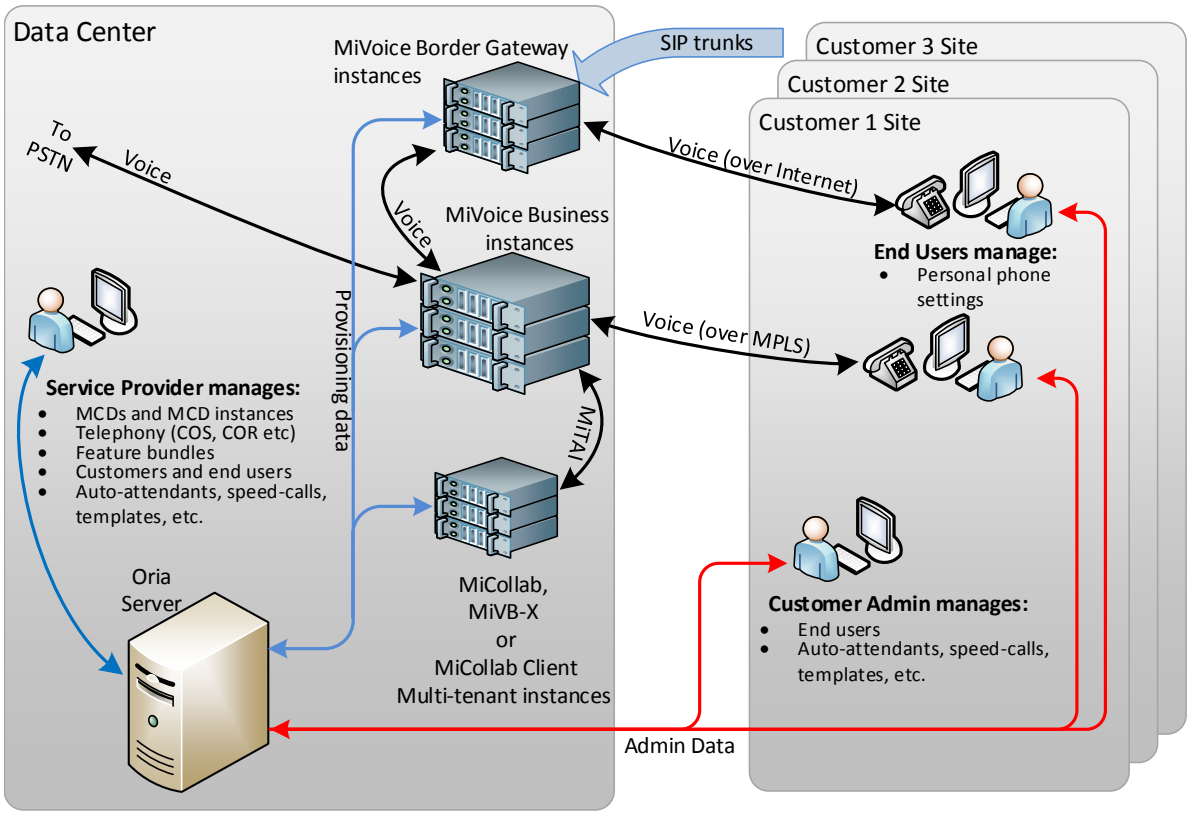



**Figure 1 Overview diagram.**

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

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

Other deployments are possible. For example, the platforms can be 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 can be located anywhere there is an Internet connection.

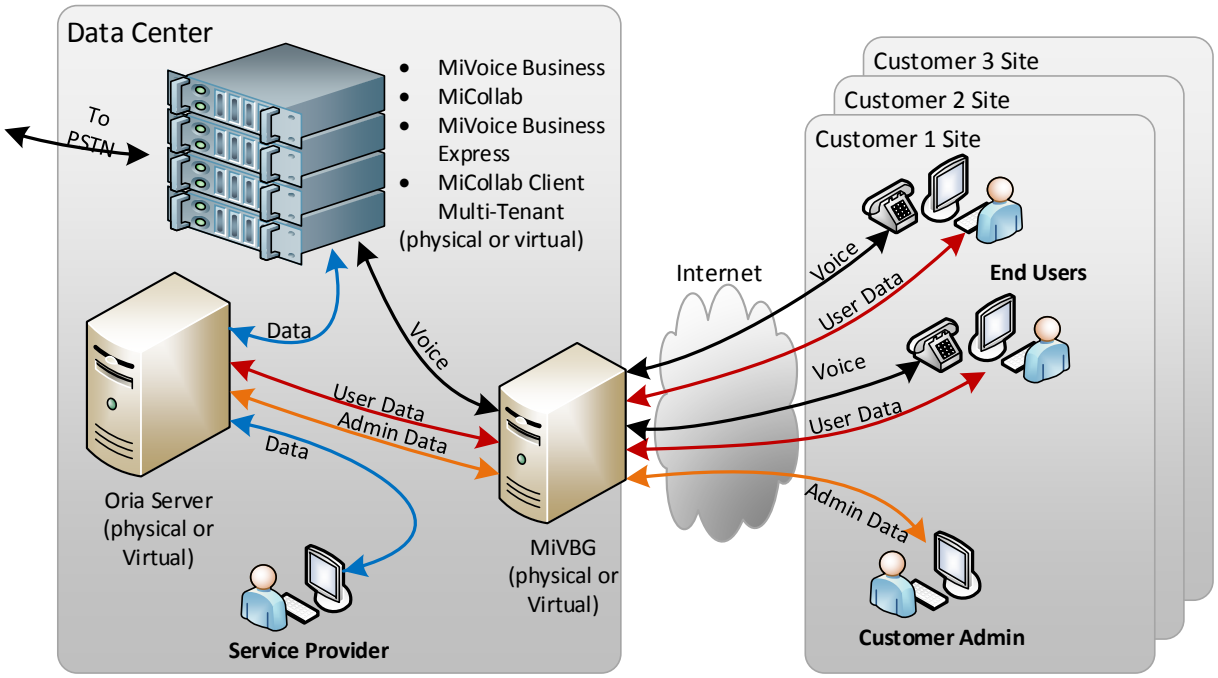



Figure 2 An example of Internet-based deployment topology.

The recommended solution for the gateway component is the MiVoice Border Gateway, which has been specifically designed for Teleworker applications. With the MiCollab and MiVoice Business Express platforms, the provider can choose 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 a lot 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 actually describes an "Extranet", however the term "VPN" will be 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.

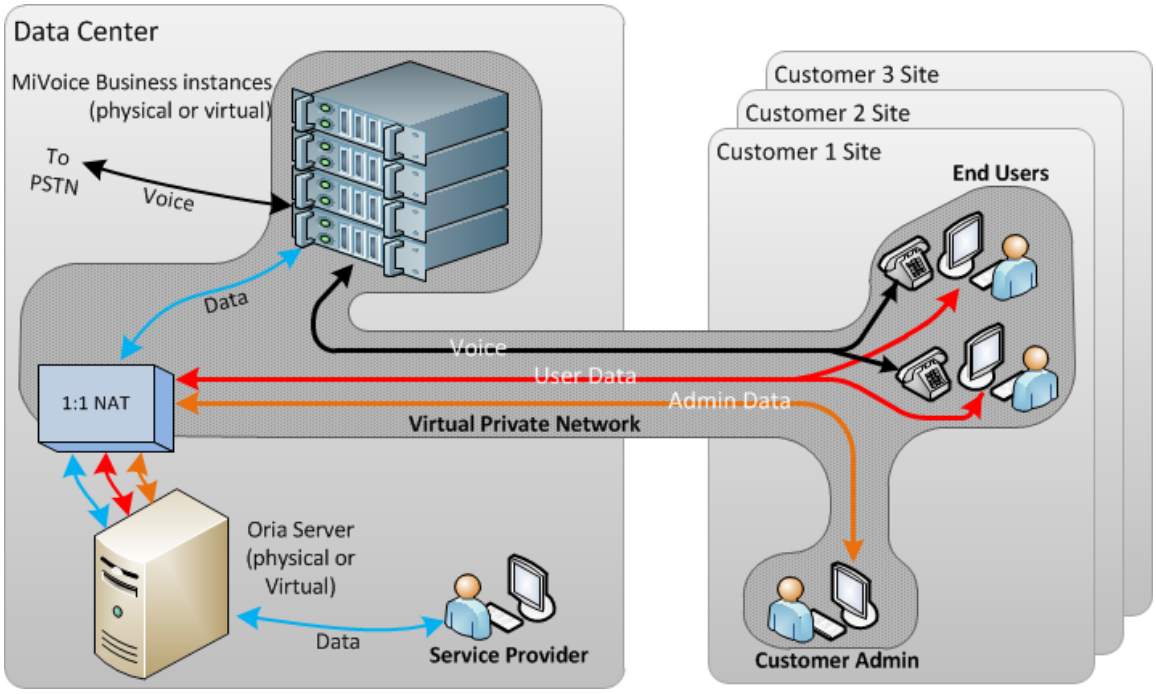



Figure 3 VPN deployment topology

## 3.3 Deployment Considerations

### Cost

Cost is always 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. MiVoice Business licenses, in particular 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 will be borne by the data center and included in the cost structure of the provided service. However, a MiVoice Border Gateway can support thousands of connections so a single MiVoice Border Gateway can service 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. In particular, a high-performance MPLS link can be quite expensive. Normally these costs are recurring. If the VPN is hosted at the data center, then these costs 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 may experience 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 3rd 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 6.0 is part of the MiCloud 4.0 suite of products. The most up to date and complete list of compatible software versions for MiCloud 4.0 can be found in [5]. It is reproduced here for convenience.

| Application | Recommended Software Level Requirement |
|---|---|
| MiCloud Management Portal | 6.0 |
| MiVoice Business | 8.0 SP2 |
| MiVoice Business-Virtual | 8.0 SP2 |
| MiVoice Business Multi Instance | 2.0 SP1 |
| MiVoice Business-Express | 8.0 |
| MiCollab | 8.0 |
| MiCollab Next Gen Client | 8.0 |
| MiVoice Border Gateway | 10.0 SP1 |
| MiCloud Management Gateway | 5.0.6.0 |
| Mitel Open Integration Gateway | 4.0.29 |
| MiContact Center Business | 8.1 SP3 |
| MiVoice Call Recording | 9.1 SP2 |
| 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, please refer to reference document [5].

## 4.2 LAN/WAN Requirements

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

### 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 will be deployed. This IP address will be 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 1:1 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 will be discussed in sections 5.4 and 5.5.

## 4.3 Hardware and Software Requirements

### 4.3.1 Support for Virtual Environments

MiCloud Management Portal 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 to reference document [6].

### 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 | 10.5.19.0 (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***

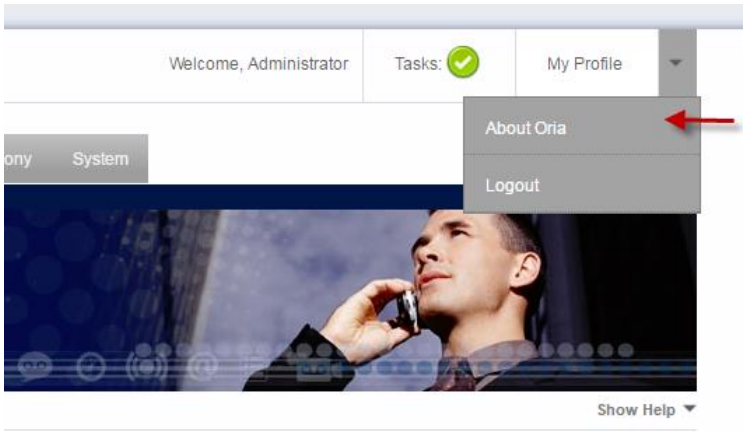
It is highly recommended that a dedicated physical server or dedicated virtual server instance be provided for the MiCloud Management Portal server. The *minimum* server requirements for MiCloud Management Portal can be found in reference documents [6] and [7]. Search for the key word MiCloud Management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

***Virtual Machine Requirements***

Normally, 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 has to 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 reference document [6].

### 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 to upgrade to the latest versions of browsers to avoid security issues. Minimum browser versions supported can be found in the *About MiCloud Management Portal* menu of the portal.



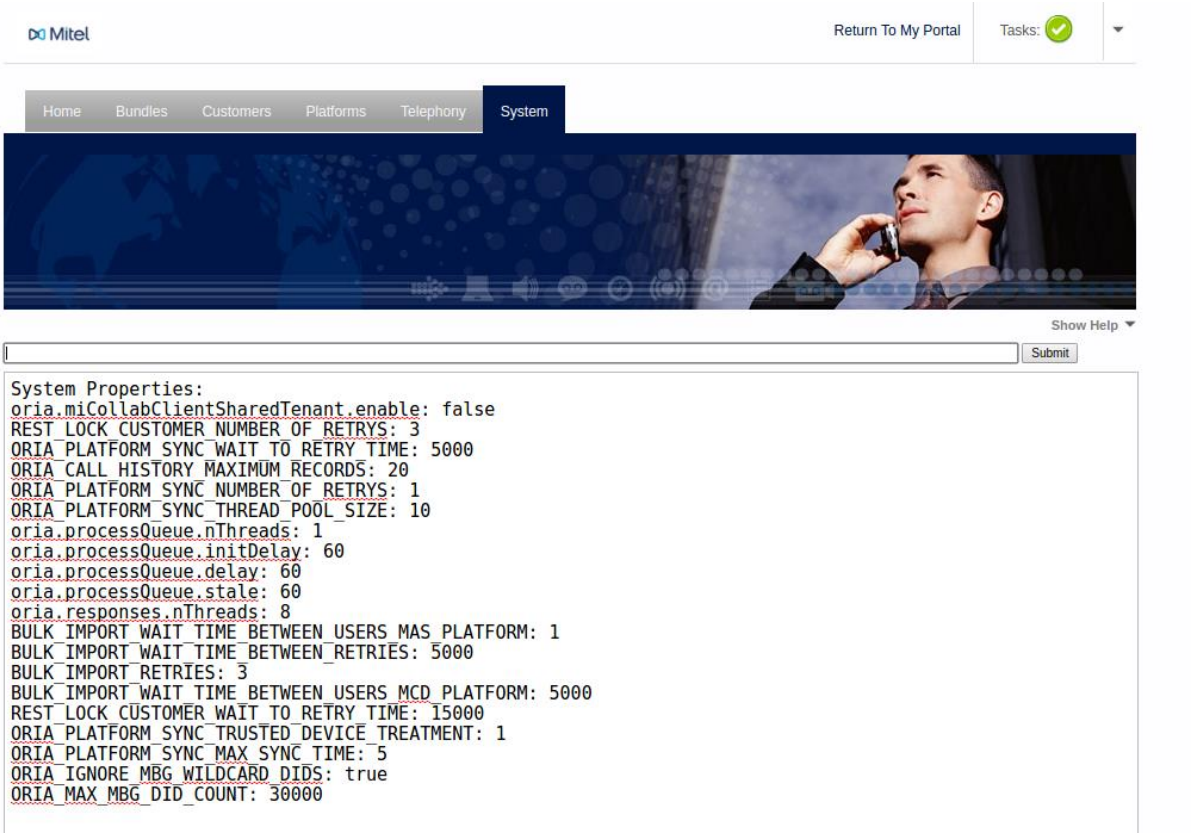

The customer administrator portal also runs on tablets that support Chrome, Firefox or IE/Edge.

Smartphones are not yet supported.

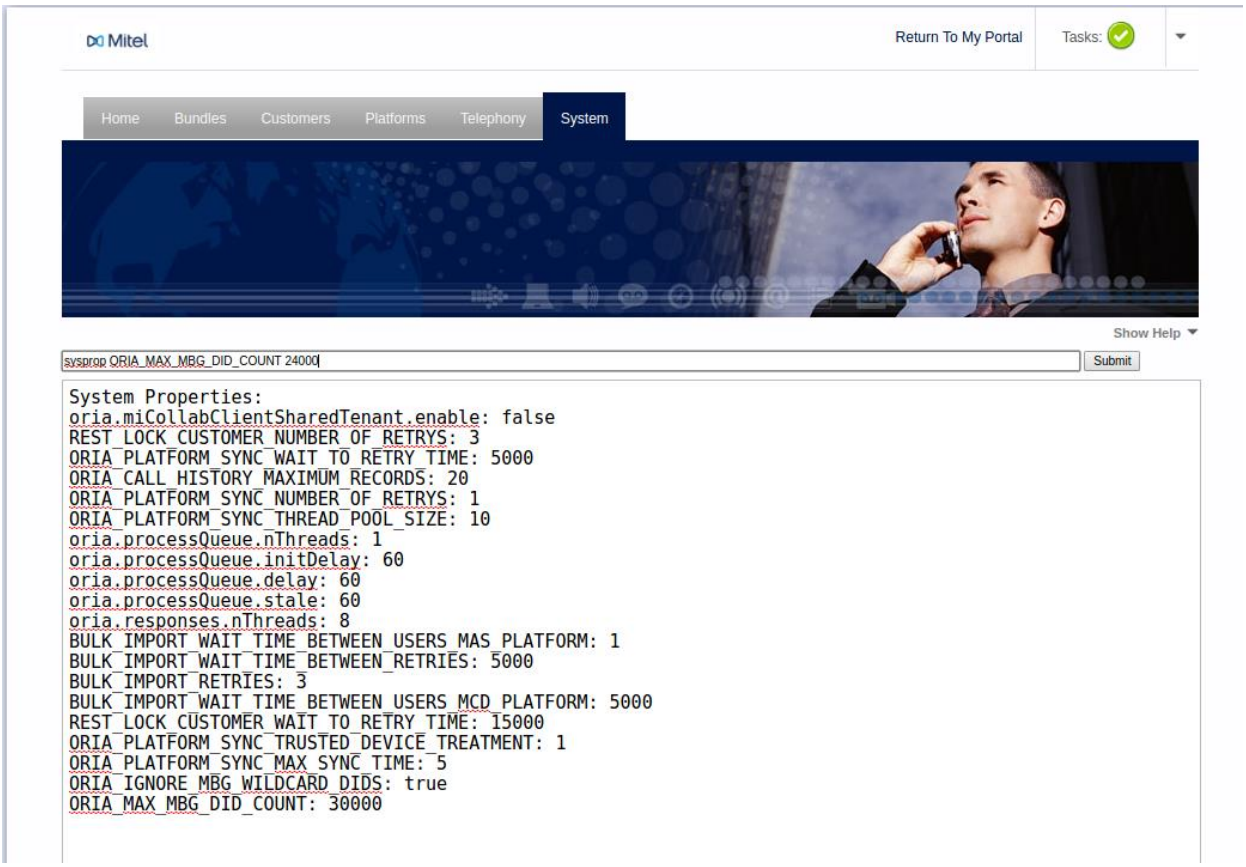
# 5 Configuration

## 5.1 System parameters and the sysprop maintenance commands

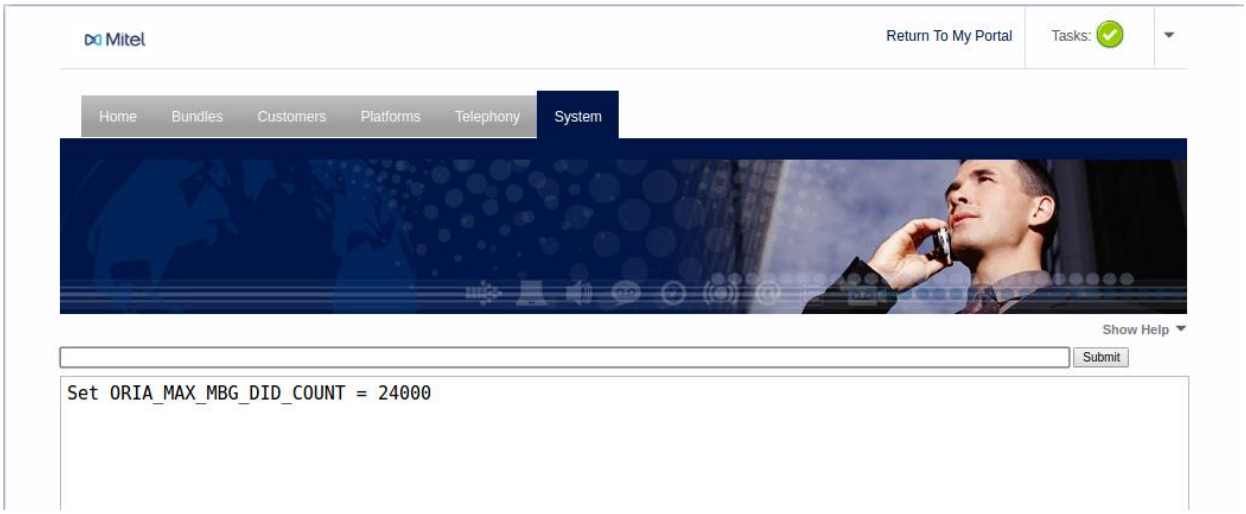
MiCloud Management Portal 6.0 makes modifying system parameters a lot easier by providing a maintenance command called *sysprop*. Without any parameter, the *sysprop* maintenance command shows a list existing system parameters and their values.



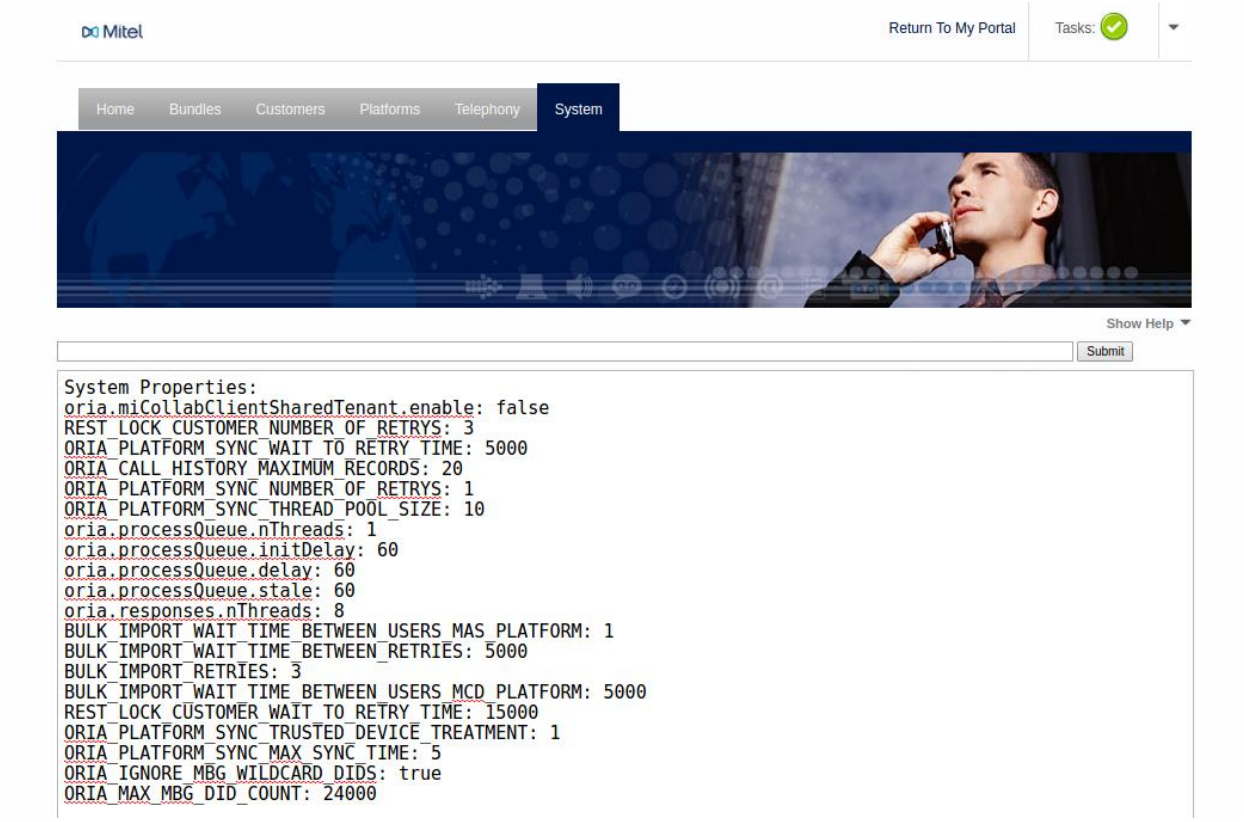

Here, we see that the parameter ORIA_MAX_MBG_DID_COUNT has been set to 30000. To set it to 24000, execute the *sysprop* command with the name of the parameter followed by its value like so:



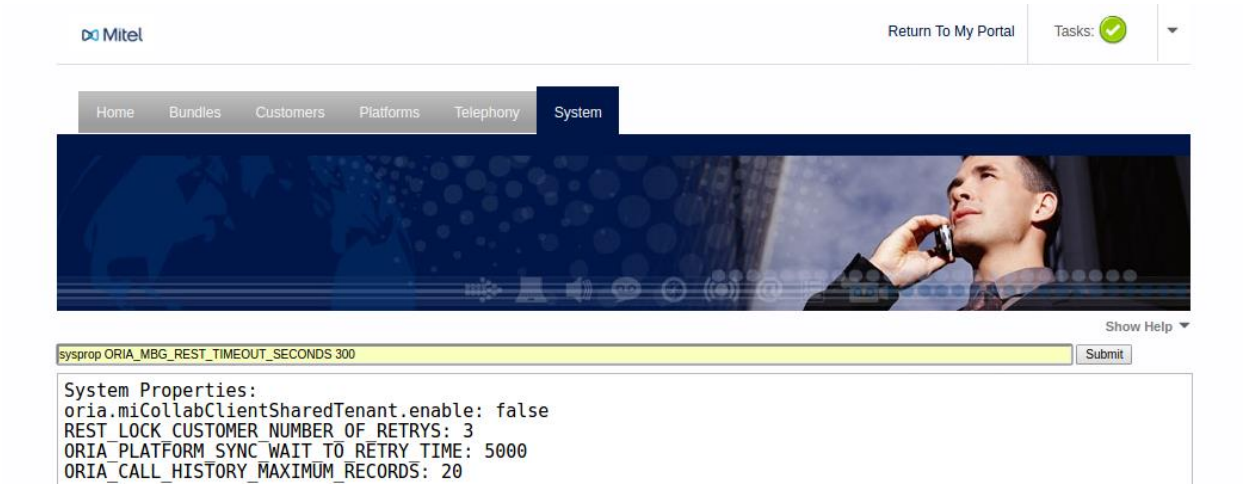

After you hit ENTER or click on the Submit button, the parameter is set to the specified value.



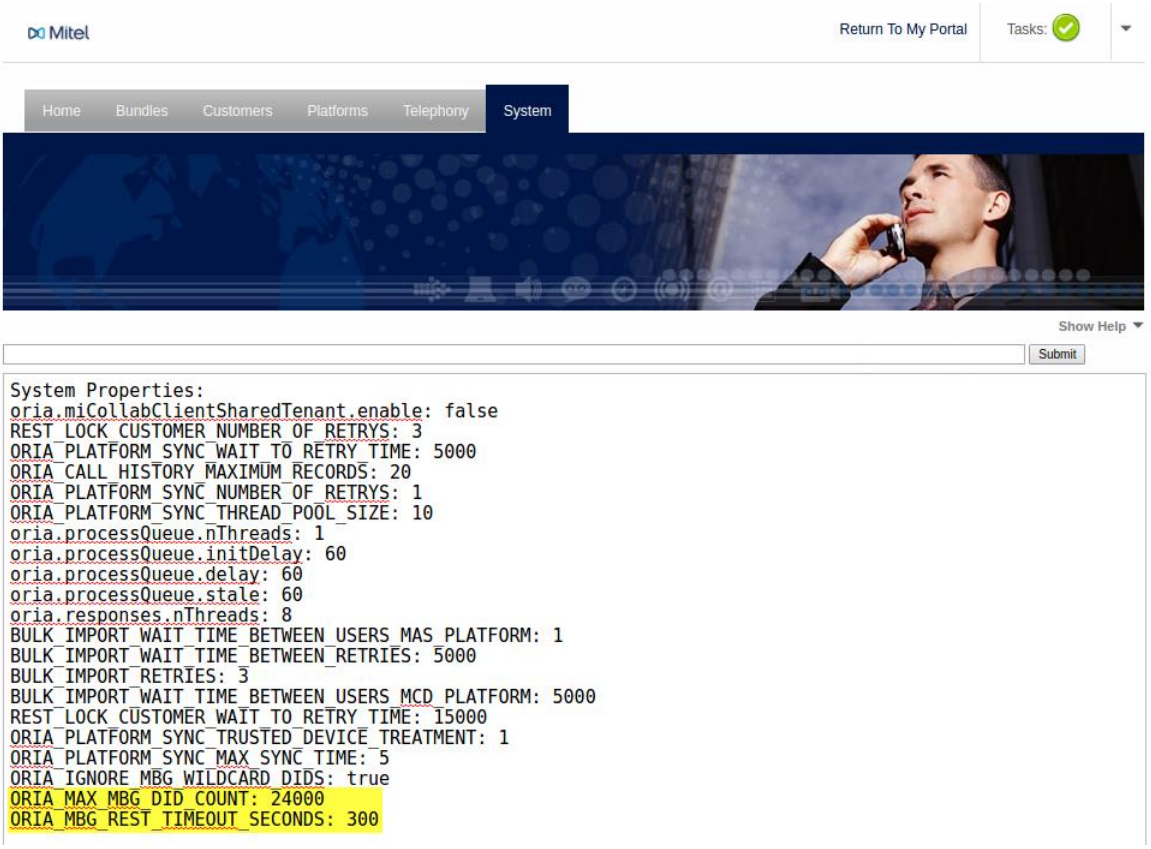

Executing *sysprop* again without any parameter confirms that the parameter was set correctly:




To set a parameter that currently doesn't exist, again execute the *sysprop* command with the name of the parameter and its value.




Now, both parameters are set correctly:




### 5.1.1 Some common system parameters

The *sysprop* command exposes a number of system parameters. Changing these parameters can change the behaviour of MiCloud Management Portal. As such, care must be exercised when using this command. Indeed, 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.<br><br>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 ORIA_MAX_MBG_DID_COUNT parameter.<br><br>If set to 'true' new MBG DID rules are written at the end of the rule list. |

| | | |
|---|---|---|
| | | 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. |
| ORIA_MAX_MBG_DID_COUNT | 20000 | The maximum number of DID rules that can be added when ORIA_IGNORE_MBG_WILDCARD_DIDS is set to 'true'. |
| ORIA_MBG_REST_TIMEOUT_SECONDS | 60 | Timeout when working with the MBG's REST interface. |

## 5.2 Port Usage

The following ports should be viewed with a help of a diagram such as Figure 2 and Figure 3.

| Port | Function | Platform | Usage |
|---|---|---|---|
| 53 | DNS | MiCloud Management Portal, MiVB, MiCollab, MiVB-X | Platforms need to resolve host names. Some platforms act as DNS servers. |
| 80 | http | MiCloud Management Portal, MiVB, MiCollab, MiVB-X | Users connect to any of these servers with their browsers. |
| | Management API | MiVB | MiCloud Management Portal uses this port to manage the MiVB |
| 25\|587 | SMTP | MiCloud Management Portal, MiVB, MiCollab, MiVB-X | The platforms can send emails to email servers. |
| 123 | NTP | MiCloud Management Portal, MiCollab, MiVB-X | MSL based platforms can use NTP to synchronize their clocks |
| 443 | https | MiCloud Management Portal, MiVB, MiCollab, MiVB-X | Users connect to any of these servers with their browsers. |
| | Management API | MiVB | MiCloud Management Portal uses this port to manage the MiVB |
| 10245-10250 | Management API | MiCollab | MiCloud Management Portal connects to this MiCollab's API to manage users |
| 10255-10260 | Management API | MiCollab | MiCloud Management Portal connects to this MiCollab's API to manage users |
| 35600 | Management API | Multi-tenant MiCollab Client Service (UCA) | MiCloud Management Portal connects to this UCA's API to manage accounts |

## 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:

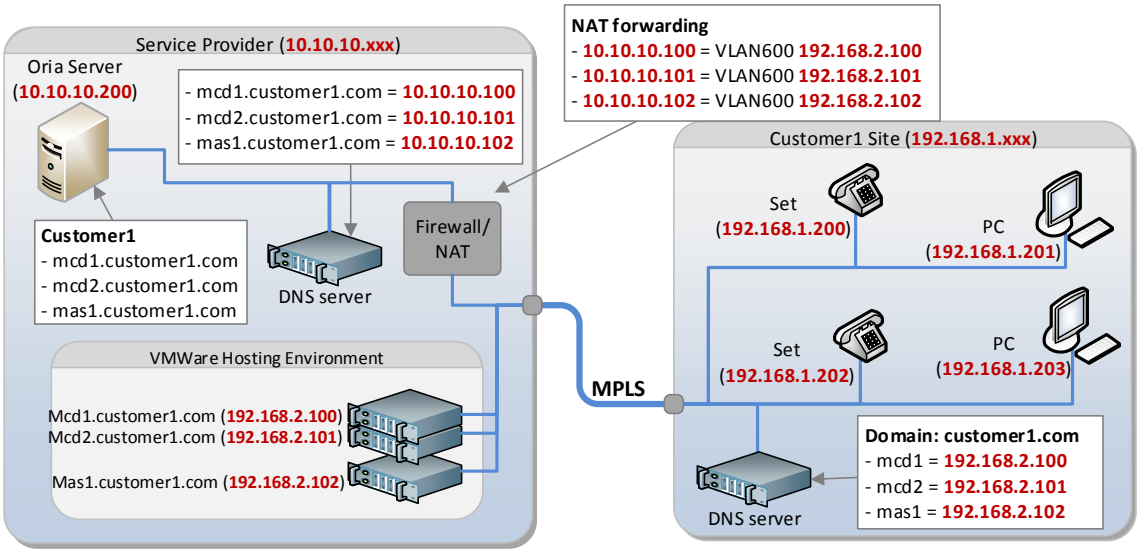
- The use of FQDN. Platform registration in MiCloud Management Portal are done using the FQDNs of the respective platforms
- With Flow Through Provisioning, the registration of MiVBs on MiCollab is done using IP addresses. Please refer to section 5.6 for details.
- The use of NAT between the SP's management 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 reference document [2].

## 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.

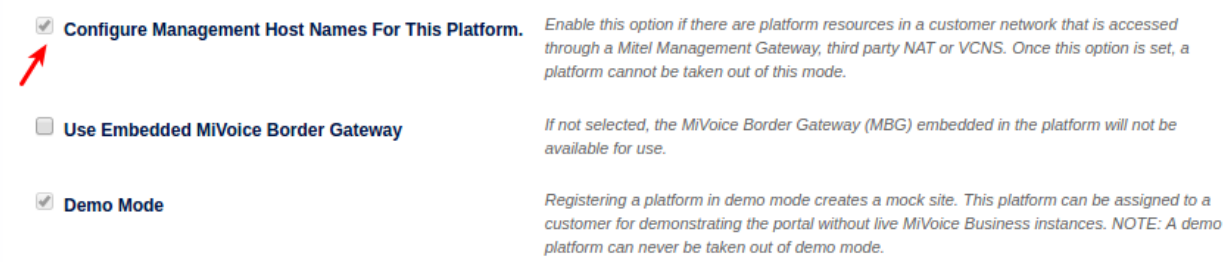
## 5.6 Working with MiCollab Flow Through Provisioning

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

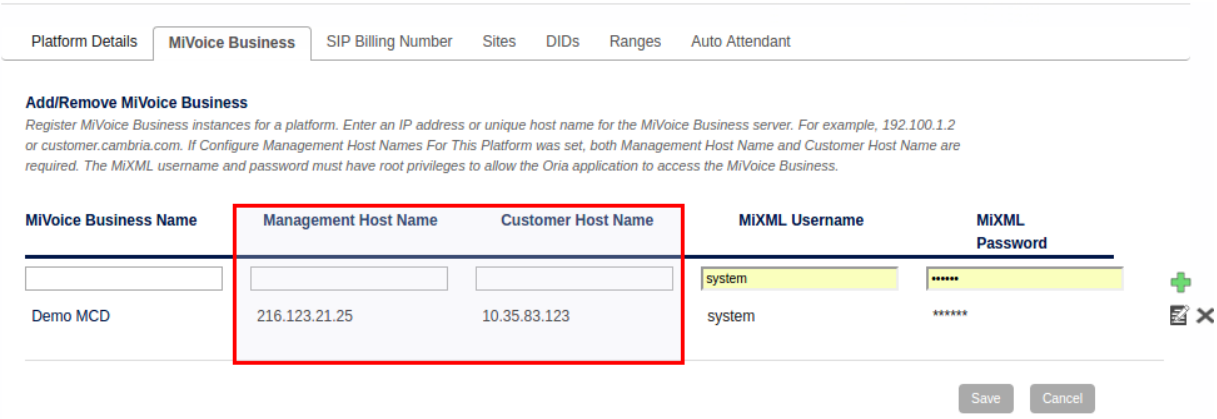
Basically, each platform IP address in the customer's VLAN must be paired with an IP address in the management network. In the example below, a MiVB platform whose address in the customer VLAN is 10.35.83.123 is paired with the address 216.123.21.25 in the SP's network. MiCloud Management Portal uses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

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*:




Then for each MiVB 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 MiVB.




## 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[2] MiVoice Border Gateway. Do not register two MiVoice Border Gateways from the same cluster.

[2] The exception is in the case of MiCollab Client resiliency. See ☞ in the last paragraph.

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.

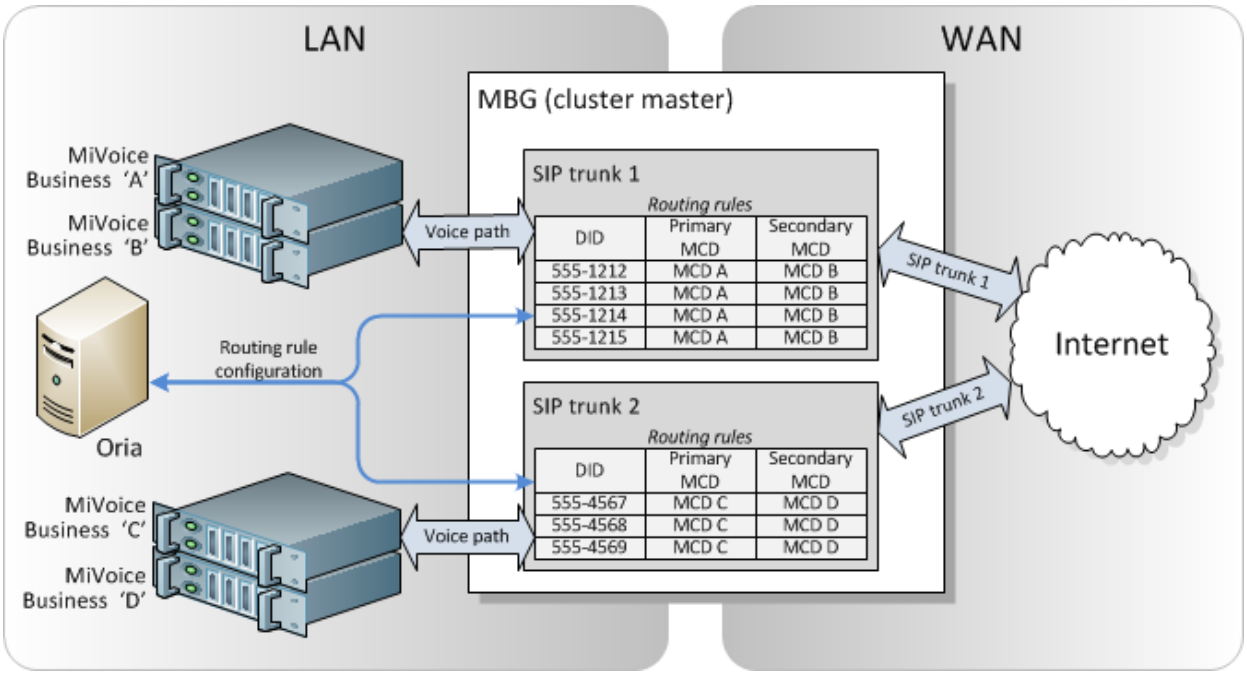
Once a set of MiVoice Border Gateways have been registered, they can be assigned to platforms for DID routing or device management functions. If the MiVoice Border Gateway is stand-alone (i.e. not embedded in a MiCollab or MiVoice Business Express server) then the same MiVoice Border Gateway can be assigned 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 reference document [8], section *Configure MiCloud Management Portal with FQDN/IP address of MiVoice Border Gateway*.

### 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:

- **ORIA_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 ORIA_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.

- **ORIA_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:

- Whether or not 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 whether or not 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-8.2.0.Final/standalone/deployments/MiCloud Management
PortalEar.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.

***NOTE***: When MiVoice Border Gateway DID rule and device settings are migrated from earlier releases of MiCloud Management Portal to release 3.3, this file is automatically updated with all the zones discovered during the importing of the Mitel phones from the MiVoice Border Gateways. For information about settings migration refer to section **Error! Reference source not found.**.

## 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

MiCloud Management Portal 6.0 introduces 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 ORIA_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[3] | 20 |

**Table 1 - User limits.**

MiCloud Management Portal call flows use MiVB'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 reference document [9] for engineering guidelines for this product.

[3] MiCloud Management Portal has been tested with 20 administrator users logged in and performing their management tasks.

# 7 Best Practices

Mitel recommends the following best practices.

## 7.1 Reassigning platforms

When platforms such as MiVBs are reassigned to new customers, some programming artifacts from previous customers may remain. This may cause unwanted behaviours for new customers. The best practice is to create new MiVB instances for new customers.

## 7.2 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 500 users per import. If more than 500 users are to be imported, the best practice is to import them in batches of 500.

# 8 Glossary

**ACD** **Automatic Call Distribution.** A package of advanced call processing features, relating to groups of agents who handle calls and agent supervisors.

**CESID** **Customer Emergency Services Identifier.** A means of correlating a user and a directory number to information stored in a physical location data base.

**COS** **Class of Service.** Defines the permissions an extension will have on a PBX or Centrex.

**CPN** **Calling Party Number.** What is used as the calling party number when making outgoing calls.

**CPU** **Central Processing Unit. T**he 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.

**DID** **Direct Inward Dialing.** IAlso 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.

**EMEM** **Embedded Mitel Express Messenger.** The built-in voice messaging system in an MiVoice Business software load.

**ESM** **Embedded System Manager.** The web-based management interface for the 3300 and MiVoice Business class of PBX.

**EHDU** **External Hot Desk User.** An off-premises hot-desk user.

**HDD** **hard Disk Drive.** A data storage device used for storing and retrieving digital information using rapidly rotating disks (platters) coated with magnetic material.

**IEEE** **Institute of Electrical and Electronics Engineers.** A technical professional society promoting the development and application of electrotechnology and allied sciences.

**IP** **Internet Protocol.** A protocol that specifies the format of data packets (also called datagrams) on a network, and the addressing scheme

**MiCollab** 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.

**MiCollab Client** This is one the the applications of the MiCollab product. It provides softphone clients, mobile clients functionality. Previously known as UCA.

**MiNET** 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.

**MiVB** MiVoice Business. Previously known as the 3300 or the MCD.

**MiVBG** **MiVoice Border Gateway.** 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.

**MiVB-X** MiVoice Business Express. Previously known as the vUCC.

**OVA** **Open Virtualization Archive.** An open standard for packaging and distributing virtual appliances or more generally software to be run in virtual machines.

| | |
|---|---|
| **PBX** | **Private Branch Exchange**. 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 |
| **RAM** | **Random Access Memory**. Volatile computer memory that holds instructions and data. |
| **SIP** | **Session Initiation Protocol**. A signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over IP networks. |
| **UC** | **Unified Communications**. 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. |
| **UCA** | **Unified Communications Advanced**. This is an obsolete acronym representing the MiCollab Client Service. |
| **VAR** | **Value Added Reseller**. A company that adds extra features to products it has bought before selling them on. |
| **VLAN** | **Virtual Local Area Network**. 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. |
| **VM** | **Voicemail**. A computerized system for answering and routing telephone calls. |
| **VPN** | **Virtual Private Network**. An extension of a private network across a public network, such as the Internet. |
| **VSP** | **Virtual Service Provider**. 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. |
| **VoIP** | **Voice Over IP**. A technology that allows telephone calls to be made over data networks using IP technology. |
| **XML** | **Extensible Markup Language.** A set of rules for encoding documents in a format that is both human-readable and machine-readable. |