MICLOUD MANAGEMENT PORTAL

Service Provider Portal Guide
Release 6.1
July 2020

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

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

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

MiCloud Management Portal

Service Provider Portal Guide

Release 6.1

July 2020

Table of Contents

Welcome

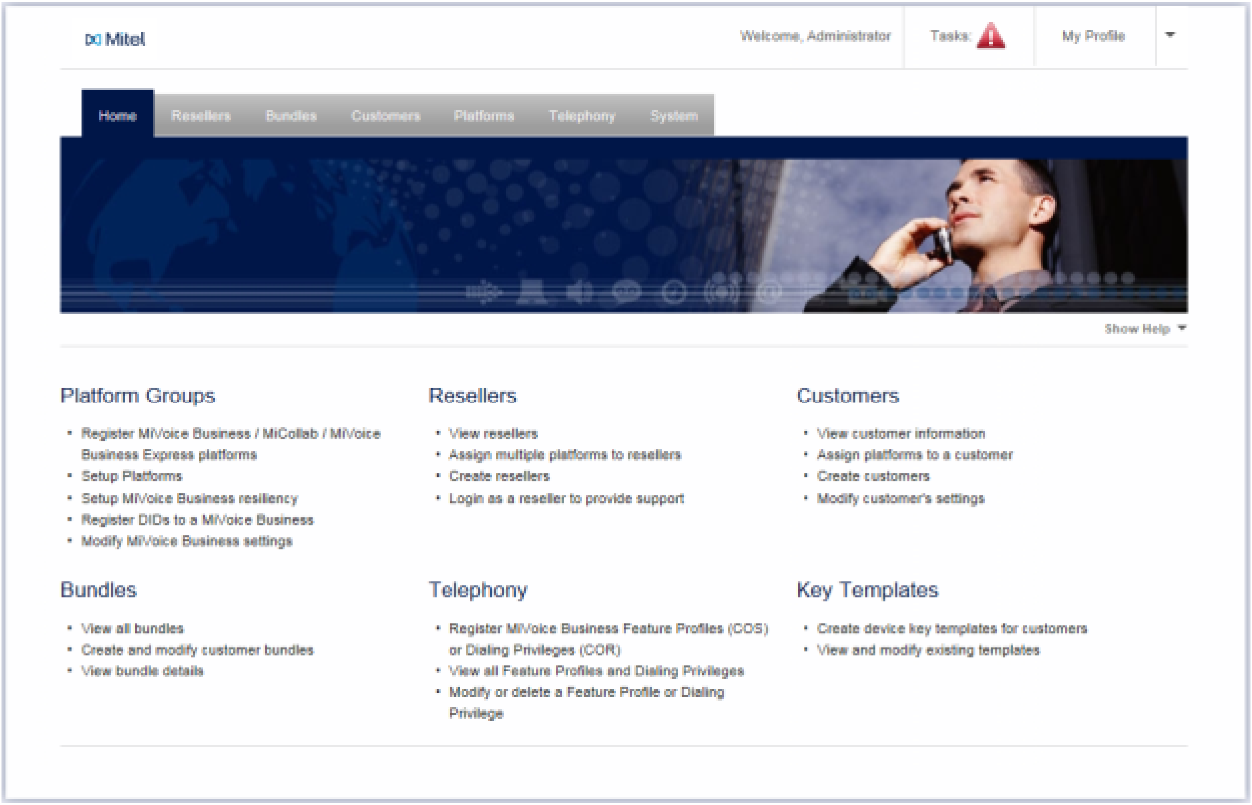
Provision and administer customers and users through MiCloud Management Portal, an application that allows you to deliver multi-customer communications services. MiCloud Management Portal includes a portal for the Service Provider and one for the Customer Administrator.

This is the Service Provider help; for Customer Administrator Portal help, see the MiCloud Management Portal documentation on Mitel Connect.

Service provider portal

The service provider portal allows you to provision customers and resellers.

A full Provision customers site map is included below.



Platform Groups

- Register MiVoice Business / MiCollab / MiVoice Business Express platforms
- Setup Platforms
- Setup MiVoice Business resiliency
- Register DIDs to a MiVoice Business
- Modify MiVoice Business settings

Resellers

- View resellers
- Assign multiple platforms to resellers
- Create resellers
- Login as a reseller to provide support

Customers

- View customer information
- Assign platforms to a customer
- Create customers
- Modify customer's settings

Bundles

- View all bundles
- Create and modify customer bundles
- View bundle details

Telephony

- Register MiVoice Business Feature Profiles (COS) or Dialing Privileges (COR)
- View all Feature Profiles and Dialing Privileges
- Modify or delete a Feature Profile or Dialing Privilege

Key Templates

- Create device key templates for customers
- View and modify existing templates

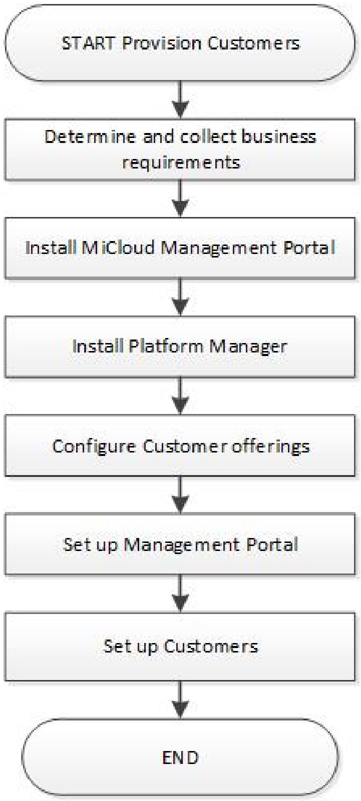
⚠ It is not recommended to register MXe server via MiCloud Management Portal.

⚠ MiCloud Business Multi-Instance Platform and MiVoice Business Express does not support MiCollab 9.0 and MiVoice Business 9.0 versions. The features ACD with SIP Softphone, 6970 Conference Phone, 6905 IP, and 6910 IP phones are not supported.

Provision customers site map

You can use the links in the table to navigate directly to the topic you need.

Important
There are several pre-configurations that you must perform on the MiVoice Business platform before you can provision it in Management Portal. Make sure that you read the Management Portal Engineering Guidelines before you configure the MiVoice Business platform in Management Portal.

	What's New
	Virtual service providers vs. value added resellers
 START Provision Customers Determine and collect business requirements Install MiCloud Management Portal Install Platform Manager Configure Customer offerings Set up Management Portal Set up Customers END	Determine and collect business requirements Install Management Portal Install Platform Manager Configure Customer Set up Management Portal Getting started - Set up customers
	Administer Customers
	Maintain Management Portal

What's New

ACD with SIP Softphone

ACD with SIP Softphone has been added to the Bundles to create as a Primary Phone. See Plan bundles for customers.

Support for 6905 IP and 6910 IP Phone Sets and 6970 Conference Phone

MiCloud Management Portal now supports 6905 IP and 6910 IP phone sets and 6970 conference phone. See Supported Phones and How Reporting Works.

Multiple MiCollab platforms within a network

Medium-Large Business (MLB) customers can create multiple instances of the MiCollab platform within a network. For example, a customer with over 5000 users, several large sites, and many retail outlets may want to set up one MiCollab platform for each business unit.

SSH File Transfer Protocol (SFTP) to upload Greeting Files

1. The greeting files are uploaded using SFTP for MiVoice Business 9.0 version and up. Greeting files are used in Music On Hold (MOH), ACD RAD Greetings, Auto Attendants, and General Mailbox.
2. To use SFTP, the following configurations are required:
    - Enable SSH in MiVoice Business MSL. See ACD Greetings and Music on Hold.
    - Configure Voice Admin Password in Management Portal. See Edit a Platform Group.

MiVoice Business 9.0 Time Zone Support

The Service Provider Administrator will set the Time Zone manually in MiVoice Business MSL when the MiVoice Business version is 9.0 or higher. See here.

Virtual service providers vs. value added resellers

Virtual service providers (VSPs): Have access to their own platform infrastructure directly through tools such as MiVoice Business System Adminstration Tool, and may also have access to a MiVoice Business, MiVoice Border Gateway, AMC licensing, and other infrastructures. With access to the infrastructure, they can register platforms and create customers in the portal.

Value Added Resellers (VARs): Do not normally have access to their own platform infrastructure. When VARs want to add a customer, they must contact the service provider and ask them to create a platform, register it in the portal, and make it accessible to a customer. After the customer is created, the VAR can then manage the customer.

Determine and collect business requirements

Before you install and set up Management Portal, complete an analysis of the potential customer base that hosted voice will be sold to. During the analysis, the goal is to discover the following:

- Target customers and type of end users
- Common phone features used by target users
- Expected dial plans
- Local dialing codes for each city where customers may exist

Design feature profiles and bundles

Upon producing the results for the customer analysis, it is necessary to determine how the various features are packaged into Feature Profiles and bundled with portal features to satisfy the majority of target users. Dialing privileges are also designed at this stage to include all potential customer locales and their various local dialing codes. This reduces lost time later when a default database update is required to include a new Dialing Privilege.

The following generic business requirements need to be set for all customers:

- Bundles/Feature Profiles
- Dialing Privileges
- Key Templates
- Brands

Install Management Portal

You can install Management Portal as a software blade on Mitel Standard Linux (MSL), or as a virtual appliance running on a virtual machine.

For information about the installation and setup of the voice platform (i.e. MiVoice Business Multi-Instance, MiVoice Business Virtual , MiVoice Business, MiVoice Border Gateway, etc.) or for proper network configuration, please refer to the appropriate Mitel product-specific documentation.

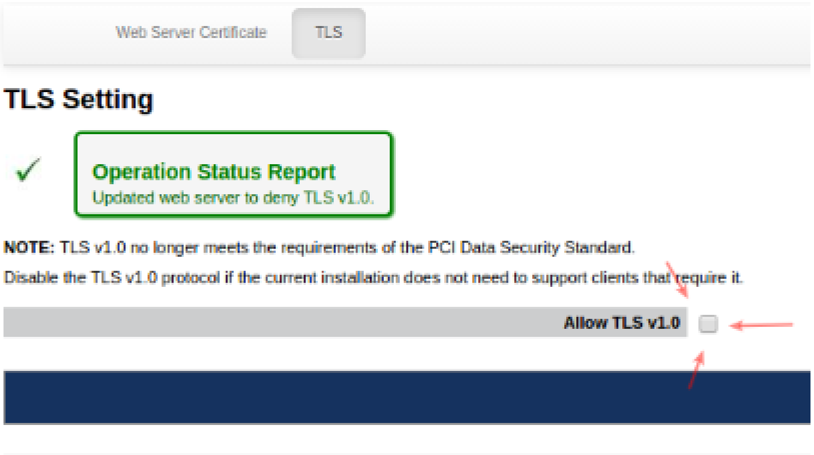
The procedures described here assume that all networking has been configured according to the Hosted Deployment model as described in the MiCloud Management Portal Engineering Guidelines. To ensure that MiCloud Management Portal operates properly, select an IP address that is available within the appropriate network or subnet to allow access to the appropriate voice platform.

Security

Important: TLS 1.0 has been found to be vulnerable to a number of security attacks. As such, Oria 5.3 disables support for TLS 1.0 by default. Mitel does not recommend using TLS v1.0. However, should you need to enable support for TLS v1.0, login to the MSL server manager for the server at:

[http://<address]http://<address of MiCloud Management Portal server>/server-manager,

go to **Security > Web Server > TLS** and select **Allow TLS v1.0**.



TLS Setting

✓ Operation Status Report

Updated web server to deny TLS v1.0.

NOTE: TLS v1.0 no longer meets the requirements of the PCI Data Security Standard.
Disable the TLS v1.0 protocol if the current installation does not need to support clients that require it.

Allow TLS v1.0 □

After MiCloud Management Portal is installed, you must configure the following parameters:

- Network Time Protocol (NTP)
- Keyboard/Time Zone/Locale (during the installation of MSL)
- HTTPS Web Certificate

Install on a physical server

The Management Portal software blade is installed from the blade panel in the MSL Server Manager. Install and activate the Management Portal software blade using the following steps:

- Logging in to the MSL Server Manager.
- Loading the software onto the MSL Server from the Management Portal CD, and then accessing the blade panel in the MSL Server Manager to install the Management Portal software blade.

Collect Site Information

The following table itemizes the information that is needed during installation and configuration. For efficient installation, it is recommended that you gather the following information beforehand.

- Administrator Password
- Domain Name of MSL Server
- System Name of MSL Server
- Gateway IP Address
- IP Address of your external NIC
- System IP Address for the Management Portal blade

To install Management Portal on a physical server:

1. Place the CD in the optical drive.
2. Log into MSL Server Manager using a supported browser with the user name 'admin' and the root password you gave when configuring the MSL server. The Server Manager is accessed by entering the following URL:*http://<www.hostname> OR <IP address of the MSL Server>/server-manager*.
3. Under **ServiceLink**, click **Blades**.
4. Click **Update List** to ensure an up-to-date listing of software blades.
5. Click **Install**. It may take a few minutes for the software to install.
6. Test the installation:
    a. Under Applications, click **Management Portal**.
    b. If Management Portal is not visible, refresh the browser.
    c. Click **Launch**.

Install on a virtual machine

Install Management Portal using the vSphere Client connected directly to the VMware ESX/ESXi 5.0, 5.1, 5.5, or 6.0 server or through the vCenter Server.

Install and activate the Management Portal virtual software using the following steps:

- Log in directly to the ESX/ESXi hosts or to the vCenter Server using the vSphere Client application.
- Deploy virtual Management Portal as a virtual machine and virtual application operating on VMware vSphere 5.0, 5.1, 5.5, 6.0, or 6.5.
- Power up the Virtual Machine and commissioning MSL/Management Portal.

Collect site requirements

The following information is required during the installation and configuration. For efficient installation, we recommend that you gather this information before you start.

- **Administrator password** - For password strength, choose a password that contains a mix of upper and lower case letters, numbers, and punctuation characters, and that is not a dictionary word.
- **Domain Name of MSL Server** - The domain on which the MSL server is installed, for example abc.com.
- **System Name of MSL Server** - Names must start with a letter; can contain letters, numbers, and hyphens. Also known as the host name.
- **MSL Server IP Address Subnet mask and Gateway IP address** - The MSL Server IP address will be the IP address for the Management Portal blade. An appropriate subnet mask for the MSL Server IP address. The IP address of the router.
- **vSphere Client application installed on a PC** - The vSphere Client is used to deploy Management Portal. The vSphere Client acts as a console to operate virtual machines and as an administration interface into the vCenter Server systems and ESX/ESXi hosts. Refer to the VMware website for detailed installation procedures and additional documentation.
- **(Optional) vCenter Server(s) installed on the network** - A service that acts as a central administrator for ESX/ESXi hosts connected on a network. This service directs action on the virtual machine and the hosts. The vCenter Server is the working core of vSphere. Refer to the VMware website for detailed installation procedures and additional documentation.
- **ESX/ESXi 5.0, 5.1, 5.5, or 6.0 installed on the server** - Use the latest software version as specified in the *Management Portal Engineering Guidelines*.

To install Management Portal on a virtual machine:

⚠ This installation procedure assumes that a VMware server has been installed and is running an ESX or ESXi operating system.

1. Install VMware vSphere client as follows:
    a. Open a web browser and enter the IP address of the VMware server.
    b. Click **Download vSphere Client** to download the client.
    c. Run and complete installation wizard.
2. Retrieve the latest Management Portal OVF template (Oria.ova file) from **Mitel Connect → Downloads**.
3. Open the vSphere client to connect to the virtual machine:
    a. Enter IP address of VMware server.
    b. Login as the root user.
4. Click **File → Deploy OVF Template. . . .** The Deploy OVF Template screen displays.
5. Select one of the following tasks:
    a. Deploy from file if the OVF template file was downloaded to the local computer or to a network share drive, then click **B rowse** to locate the file.
    b. Deploy from URL if the OVF template file is on the internet or accessible through a web browser; enter the URL of the location of the file.
6. Click **Next**. The OVF Template Details screen displays. Leave the default selections as is.
7. Click **Next**.
8. Click **Accept** to accept the license agreement and click **Next**.
9. Enter a meaningful name for the Management Portal virtual machine, or accept the default name. Click **Next**.
10. Click **Thick Provisioned Lazy Zeroed**. Click **Next**.
11. If the network defined in the OVF template doesn't match the name of the template on the host to which you are deploying virtual Management Portal, you are prompted to configure the network mapping. Contact your Data Center administrator for more details about which Network Mapping to use.
12. Click **Next**.
13. Review the information and click **Finish**.
    Note: This process may take up to 10 minutes to complete depending on network traffic and the performance of the server.
14. When the dialog indicating that the deployment is complete appears, click **Close**. Management Portal Virtual appears in the inventory list in the left side navigation pane.
15. Click the **Management Portal Virtual**.
16. After Management Portal Virtual has powered up, you can begin configuring the MSL server.

To configure the MSL server:

1. Open the virtual machine MSL Server Console in one of the following ways from within the vSphere Client:
    a. Right-click the newly created Management Portal virtual machine and select **Open Console**.
    b. Click the **Launch Virtual Machine Console** icon in the tool bar.
       Note: VMware Tools are pre-loaded as part of Management Portal Virtual.
    c. Click the **Console** tab in the main display window.
2. Click inside the MSL Server Console window to continue. If at any time you want to have the cursor available for other desktop activities, press the **CTRL+ALT**.
3. Follow the MSL server configuration procedures as described in the *MSL Installation and Administration Guide*.
4. When the MSL server configuration is complete, you may need to add a local network to MSL if you intend to access Management Portal Virtual from a different network from which it is installed.
    a. From the MSL Server Console window, select **9 - Manage Trusted Networks**.
    b. Click **Add** a new trusted network.
    c. In the **Network Address** field, enter the IPv4 or IPv6 address of the network to designate as "local".
    d. In the **Subnet mask** field, enter the dot-decimal subnet mask (for example, 255.0.0.0 if you intend to open up to the entire Class A subnet).
    e. In the **Router** field, enter the IP address of the router you will use to access the newly-added network.
    f. Click **Add**.
5. After the MSL server configuration is complete, you may need to add a local network to MSL if you intend to access Management Portal Virtual from a different network from which it is installed. The process includes adding a local network, subnet, and router to the Local Networks panel in the server manager as follows:
6. Log in using the admin user ID and root password created during the MSL server configuration.
    a. Using the arrow keys, select **11 - Access Server Manager**.
    b. Log in using the same administrator user ID and password as in **Step a**.

   c. Using the arrow keys scroll down to **Local Networks**.
   d. Use the down arrow key to select **Add Network**. Press **ENTER**.
   e. Use the down arrow key to enter the following information:
      i. Subnet Mask (for example, 255.0.0.0 if you intend to open up to the entire Class A subnet).
      ii. Router Address (for example, 192.168.1.x, the gateway IP provided during the MSL server configuration).
   f. Use the down arrow to select **Add** and press **ENTER**.
   g. Type **Q** to quit, then select **Exit** and **Yes**.
   h. Using the down arrow key, scroll to **Exit** from the MSL Server Console. Press **ENTER**.
   i. You are now ready to configure the Management Portal application.

7. Confirm the OVF memory and HDD configuration as follows:
   a. Right-click the newly created Management Portal virtual machine.
   b. Click **Edit Settings**.
   c. Under the **Hardware** tab, click **Memory** and set Memory Size to 6 GB.
   d. Under the **Hardware** tab, click **Hard Disk** and set Disk Provisioning to 50 GB.
   e. Under the **Hardware** tab, click **CPUs** and set Number of Virtual Sockets to 4.
   f. Click **OK**.
8. Complete the OVF configurations as follows:

1. Click **Power → Power On**.
2. Click the **Console** tab and wait for server to startup. Login as root user (use password provided by Mitel).
3. Select **Timezone Configuration** and set it based on your location. Click **OK**.
4. Select **Keyboard Configuration** and set it based on your preference. Click **OK**.
5. Select the **Network Configuration** option.
6. Select **Edit Devices → eth0**.
7. Uncheck the **Use DHCP** checkbox.
8. Enter the appropriate Static IP, Netmask, and Default gateway IP address.
9. Select **Edit DNS Configuration** and enter a Primary DNS server IP address.
10. Click **OK → Save → Save&Quit → Quit**.
11. Right-click the newly created **Management Portal** virtual machine.

- Click **Power → Shutdown Guest**.
- Right-click the **Management Portal** virtual machine.
- Click **Power → Reset**.

Install Platform Manager

To enable the Platform Manager features, install Management Portal File Server and Management Portal Platform Manager on a new server. Do not install them on the same server where Management Portal is installed .

Install the following software blades:

- Management Portal File Server
- Management Portal Platform Manager

The Management Portal software blade is installed from the blade panel in the MSL Server Manager.

To install File Server:

1. Place the CD that contains the MSL Management Portal File Server software blade in the optical drive.
2. Login into MSL Server Manager.
3. In the left-side panel under **ServiceLink**, click **Blades**.
4. Click **Update List** to ensure an up-to-date listing of software blades. If there is a report displayed from the last install, click **Clear this Report**.
5. In the **Current List of Blades** table, find the Management Portal **File Server** blade and click the **Install** link in the **Installation** column.
6. Accept the license agreement. It may take a few minutes for the software to install.
7. Click **CTRL+R** to refresh the page.
8. It takes few minutes for the application to start.
9. In the left-side panel under **Applications**, click Management Portal **File Server**.

For more information about Management Portal File Server, see File Server Help.

To install Platform Manager:

1. Place the CD that contains the MSL software in the optical drive.
2. Login into MSL Server Manager.
3. In the left-side panel under **ServiceLink**, click **Blades**.
4. Click **Update List** to ensure an up-to-date listing of software blades. If there is a report displayed from the last install, click **Clear this Report**.
5. In the **Current List of Blades** table, find the Management Portal **Platform Manager** blade and click the **Install** link in the **Installation** column.
6. Accept the license agreement. It may take a few minutes for the software to install.
7. Click **CTRL+R** to refresh the page.
8. It takes few minutes for the application to start.
9. In the left-side panel under **Applications**, click Management Portal **Platform Manager**.

For more information about Management Portal File Server, see Platform Manager Help.

Configure

Create a default MiVoice Business Platform database. Any operations performed in the portal will make direct changes to the tables within the MiVoice Business Platform database. For the portal to perform properly with each MiVoice Business Platform instance, configure the instances with the same default MiVoice Business Platform database.

Platform Manager can create platform instances from a blueprint. See Create a Platform Group using a Blueprint for more information.

Configure the default database

Before creating a customer and allowing a customer administrator to perform self-service operations, you need to setup a default MiVoice Business Platform database that can be applied to each MiVoice Business Platform instance.

The default MiVoice Business Platform database is based upon the information gathered during the system planning phase. It is a combination of configurations to satisfy system requirements for feature profiles (COS), bundles, dial plans, and default settings. The template is then applied to every MiVoice Business Platform instance to provide the same level of features and services to all customers.

⚠ **Note**
The Platform Manager installation includes some reference golden database files. You can find them on the Platform manager server, under the linux directory /opt/dist_oria-bim-setup/reference.

Prior to performing any configuration operations on the default MiVoice Business Platform database, it is necessary to ensure that all requirements have been satisfied and included in the default database. There are two parts of the default database that can be defined as follows:

- Fixed Defaults - Management Portal Default Configurations (these are fixed in Management Portal and cannot be changed)
- Flexible Defaults - Business Requirements Configurations

Fixed defaults

The fixed defaults refer to the settings that must be configured on the default MiVoice Business Platform database to ensure proper interaction between Management Portal and the MiVoice Business Platform.

When a user, hotdesk phone (IP device only), or call group is created using Management Portal, there are specific settings that Management Portal applies, and these must match those on the MiVoice Business Platform, to ensure it responds correctly (i.e. when a hunt group is created, Management Portal sets the Class of Service to COS 6).

See Fixed Defaults Table for the default values that Management Portal users. The values must be identical to the values configured on the default MiVoice Business database.

Flexible defaults

The flexible defaults refer to the settings that must be configured on the default MiVoice Business Platform database to ensure proper interaction between Management Portal and the MiVoice Business Platform instance corresponding to the bundle and dial plan assignments.

A bundle and dial plan are assigned to each newly created user. A bundle includes a Feature Profile, which is Management Portal's view of a Class of Service (COS). When a user is assigned a bundle, the COS number affiliated with the bundle gets assigned to the user on the MiVoice Business Platform.

Similarly, a dial plan in Management Portal corresponds to a Class of Restriction (COR) on the MiVoice Business Platform. When a user is assigned a dial plan, the COR that is registered to the dial plan gets assigned to the user on the MiVoice Business Platform.

To ensure that proper services (COS options and ARS routes) are available to an end user, it is essential to set the Flexible Defaults appropriately.

If any of the User features that affect the MiCollab Client are modified either through Management Portal or directly on the MiVoice Business System Administration Tool, then the changes will not be reflected on the MiCollab Client until it has been synchronized with those MiVoice Business instances affected.

Create the golden MiVoice Business database

To create the MiVoice Business database for the first time, it is necessary to use the fixed and flexible defaults listed above, and any other additional customer requirements that may arise. Once this information has been collected, the default database can be created and then applied to each MiVoice Business Platform instance, using one of the following methods:

- Platform Manager - If you are using Platform Manager, this is the easiest way to create golden database. See the Platform Manager Help for details.
- MiVoice Business Import Spreadsheets
- Configure an initial MiVoice Business, then Backup and Restore on other MiVoice Business instances

To create the Default Database using MiVoice Business Import Spreadsheet

1. Export the **3300ICPImportSpreadsheet.tar.gz** using the Embedded System Manager (ESM) from a form that has the Export button.
2. Unzip the file to get the **3300ICPImportSpreadsheet.tar** file.
3. Unzip the **3300ICPImportSpreadsheet.tar** to get the **3300ICPImportSpreadsheet.xls** file.

   ⚠ Ensure that the filename extension is ".xls". Filename extensions with ".xlxs" are not supported.

4. Open the spreadsheet, enable macros, and create the following spreadsheets for the default MiVoice Business database:
   a. Default CESID
   b. Class of Service Options
   c. VM Ports
   d. Station Attributes
   e. Hunt Groups
   f. Hunt Groups - Hunt Group Members
   g. Call Rerouting Always Alternative
   h. Call Rerouting
   i. Class of Restriction Groups
   j. Trunk configuration forms (eg. SIP Peer Profile, IP/XNET Trunk Profiles, and any additional forms that may be required)
   k. ARS Routes
   l. ARS Dialed Digits
   m. ARS Leading Digits
   n. ARS Digit Modification Plans
   o. Trunk Attributes
   p. Embedded UM Settings
   q. System Options
5. Enter the following appropriate information into spreadsheets:
   a. Required Management Portal defaults (voicemail, COS, COR, Default CESID, DID trunk).

      ⚠ Make sure your COS values are set up correctly. If you create a Ring Group with Voicemail and use it in a Call Flow, the call will route to Voicemail instead of the selected Overflow Point. This happens because the **COS Call Forward No Answer Timer** is set to 15 seconds while the default Overflow timer in the Ring Group is set to 20 seconds. The COS option will trigger before the Overflow Point thus routing the call to Voicemail.

   b. To enable Customer Administrators to create call flows that do not follow business hours, set the following COS values:
      i. Third Party Call Forward Follow Me Accept = Yes

        ii. Third Party Call Forward Follow Me Allow = Yes
        iii. Use Held Party Device for Call Re-routing = Yes
    c. Business requirements (COS - Feature Profiles, ARS - Dial Plans)
    d. Go to the Shared Options form and set "DPNSS/QSIG Diversion Enabled" to Yes.
6. For each sheet completed in Step 4 above, check the Data Format and Save For Import.
7. Use the output spreadsheet file to configure each MiVoice Business instance with this default database.
8. Follow these guidelines:
    - DID Configuration: Set the number of DID digits to absorb or insert for an incoming DID call (ensure that the DID trunk is set to absorb or insert all digits required to allow for ten digits to pass into the MiVoice Business instance).
    - Hardware Defaults: If the hardware defaults to not fit deployment requirements, refer to System Maintenance.
    - Call Rerouting: 6080 - 6099 will be used as pilot numbers in MiVoice Business.
    - Rows 20 - 39 (inclusive) in Call Rerouting Always and Call Rerouting 1st Alt forms are reserved for Management Portal. Any changes to Call Rerouting in Management Portal will change the values in these rows of these two forms.
    - Configuration Changes: Any changes to the default MiVoice Business database may require substantial reconfiguration of the Management Portal application to ensure that there are no discrepancies across the entire service offering.
    - Do not attempt to perform multiple loading tasks at the same time as the Import. Those tasks being loaded at the same time as the Import will fail. It will be necessary to retry those loading tasks independently.

To create an Initial MiVoice Business, then Backup and Restore on other MiVoice Business instances:

1. Use the MiVoice Business Embedded System Manager (ESM) to configure the initial MiVoice Business instance.
2. Test to ensure that the configuration was performed successfully.
3. Backup the MiVoice Business database.
4. Use the saved database backup file to configure each MiVoice Business with this default database.

Because Management Portal allows for programming Embedded Unified Messaging in user mailboxes, and Forward to Email in user mailboxes, the system programming requirements for these should be part of the default MiVoice Business database programming requirements.

Embedded Unified Messaging needs to be enabled on a system-wide MiVoice Business basis in the Embedded UM Settings form. For Forward Voicemail to Email, the SMTP server needs to be configured in the System Options form on the MiVoice Business instance(s).

To set up Embedded Unified Messaging:

1. Go to the Embedded UM Settings form on the MiVoice Business instance(s).
2. Program the following fields:
    a. Enable Embedded UM: Yes
    b. IMAP Server: The IP address of your IMAP server
    c. IMAP Server Connection Type: Either CLEARN, SSL, or STARTTLS
    d. IMAP Server Port: The port used by your IMAP server (typically 143)
    e. IMAP Server SSL Port: The port used by your IMAP server (typically 993)
3. Go to the **System Options** form.
4. Program the following fields:
    a. Email Server - The IP address of the SMTP server
    b. Email - Sender's Address - Enter an email address

Fixed Defaults Table

Use this table to plan and configure the default database.

> ⓘ There are several pre-configurations that you must perform on MiVoice Business before you can provision it using Management Portal. Make sure that you read the Management Portal Engineering Guidelines before configuring MiVoice Business in Management Portal.

Notes

- Index #1 in the Call Rerouting Always Alternatives and the Call Rerouting First Alternatives forms must be blank (or will be overwritten by Management Portal).
- Index #2 in the Call Rerouting Always and First Alternative #2 must be set to DN configured through the Management Portal.

Operation	Setting	Value	Description
COS Defaults	Hotdesk Phones	1/1/1	Day/Night1/Night2
	Standard Phones	Any	MiCW default is 11. Recommendation is to use COS 11 for the MiCollab environment
	Hunt Groups	6/6/6 (MiVoice) 25/25/25 (MiCollab)	Day/Night1/Night2 MiCW default value is 25.
	Ring Groups	6/6/6 (MiVoice) 26/26/26 (MiCollab)	Day/Night1/Night2 Will need to override the MiCW default value of 26.
	EHDU Extensions	11/11/11	Day/Night1/Night2 MiCW default value is 11.
COR Defaults	Hot Desk Phones	1/1/1	Day/Night1/Night2
DID Trunk Attributes	DID Digits to Absorb	Value that will generate a 7 digit number string.	Management Portal requires a 7 digit local number after the process of absorbing the DID digit string. For example, in North America, the digits to absorb will be 3 if the regional dialing plan is 10 digits and 0 if the regional dialing plan is 7 digits.
Voicemail (EMEM) Configuration	Voicemail COS	*Any	Enable options: - COV/ONS/E&M Voicemail Port - Message Waiting - Voicemail Softkey *Use any available COS for voicemail (ports/hunt group)
	Vmail Ports	*Any	Assign Voicemail COS *Create as many vmail ports as necessary
	Vmail Hunt Group	*Any	Assign: - Voicemail COS - Vmail ports *This is a configurable value (in the Settings tab when creating a Platform Group), and once assigned to a customer it cannot change.
	Call Rerouting First Alternative	2	Set as 'THIS' for all options to forward to voicemail hunt group (6000).
	Call Rerouting Always	2	Set as 'THIS' for all options to forward to voicemail hunt group (6000).
Voicemail (NuPoint) Configuration	Voicemail COS	Any	Use any available COS for voicemail. The MiCW default value is 82.
	Voicemail MWI COS	Any	Use any available COS for voicemail. The MiCW default value is 84.
	Voicemail Ports	Any	Assign Voicemail COS. Create as many voicemail ports as necessary. The MiCW default is to choose port numbers incrementally after the Voicemail Hunt Group number (eg. if the Voicemail Hunt Group number is 6000, the default is to start from 6001).
	Voicemail Hunt Group	6000 (MiCollab) 7000 (vUCC)	Assign: • Voicemail COS • Voicemail ports
	Call Rerouting First Alternative	2	Set as 'THIS' for all options to forward to voicemail hunt group (eg. 6000).
Speech Auto Attendant Configuration	Speech Auto Attendant COS	Any	Use any available COS for Speech Auto Attendant. The MiCW default value is 85.
Mitel Collaboration Advanced Configuration	Mitel Collaboration Advanced COS	Any	Use any available COS for MCA. The MiCW default value is 86.
Default CESID	Enable Automatic CESID	True	Allows user and hotdesk phone creation to occur successfully

Operation	Setting	Value	Description
Registration Access Code Configuration	Set Registration Access Code	Enter a string from 3 to 10 characters long to use when registering a new IP telephone. The access code followed by the DN constitutes the PIN and can include the characters # and/or *.	Is required for creating a MiCollab Client Tenant in a platform group. If not set (blank), Management Portal displays the error message "MCD does not have the registration code set" when you try to save the platform group.

Configure the server for the Welcome e-mail

You must configure SMTP on the MSL server to send Welcome messages from Management Portal.

To configure SMTP on the MSL server:

1. In the MSL server manager under Configuration, click E-mail Settings.
2. Configure the SMTP server as follows:
   a. Server to use for outbound SMTP: Enter the server hostname or IP address in this field.
   b. Destination Port for Outbound SMTP: Select a port for the SMTP. Available ports: SMTP Port 25 (use cleartext; default), SMTP port 587 (TLS encryption), and SMTP Port 465 (SSL encryption).

Register MiVoice Border Gateway

There are several pre-configurations that must be performed on the MiVoice Border Gateway (MBG) before it can be provisioned by Management Portal. It is important to read the Management Portal Engineering Guidelines first, before registering an MBG in Management Portal. If the network configuration includes a MiVoice Border Gateway (MBG) Cluster, it must be registered with the portal so that it can be assigned to a Platform Group. For proper registration, the MBG must exist and be reachable from Management Portal.

When registering an MBG, it must be based on the device types that are allowed to be programmed on the particular MBG:

- MiNet MBG
- SIP MBG
- MiCollab Client

Each Site can select an MBG for each device type and can allow 1 MiNet, 1 SIP, and 1 MiCollab Client device type, while each Platform Group can have multiple Sites with different combinations of MiNet, SIP, and MiCollab Client device MBGs.

PC MiNet Softphone phone types are programmed on the MiCollab Client device MBG; however, Management Portal does not allow a cluster zone to be specified.

DIDs can be assigned against one (or none) of a number of multiple MBG Clusters. For each DID range, an MBG Cluster and SIP Trunk can be selected.

DID Services can be assigned to a MiVoice Business platform or a MiVoice Border Gateway. DIDs are required in both the MBG SIP Trunks and MiVoice Business. The MBG needs DIDs to determine which MiVoice Business gets the call and the MiVoice Business needs them for DID Services.

Embedded MiVoice Border Gateway

Certain Platform Groups have an MBG embedded within that platform. The following platform types contain an Embedded MBG:

- MiCollab
- MiVoice Business Express

The Embedded MBG is categorized as follows, based on the type of device that can be programmed on it:

- MiNet Devices
- SIP Devices
- SIP Trunking (Routing Rules)

When creating a Site or registering a DID range for a MiCollab or MiCollab with Voice platform group, the Embedded MBG is included in the list of MBG Clusters, if it was registered. An Embedded MBG appears in the platform list to which it belongs.

When a user is created and assigned to a Site with an Embedded MBG, then the device is programmed on the Embedded MBG, if the Embedded MBG is assigned to the device type that was assigned to the user.

When a Hot Desk device is created and assigned to a Site with an Embedded MBG as the MiNet Device MBG, then the device will be programmed on the Embedded MBG.

When DIDs are registered for a MiCollab or MiCollab with Voice Platform Group, if the Embedded MBG is specified as the MBG, then the routing rules for those DIDs are programmed on the Embedded MBG. If another MBG cluster is specified, then the routing rules for those DIDs are programmed on that MBG.

If a MiCollab or MiCollab with Voice Platform type is not in use, you can delete it (it will also delete the Embedded MBG).

> ⚠ It is possible to register the same MBG twice by mistake, once with the IP address, and once with a Fully Qualified Domain Name (FQDN). Management Portal does not detect that the IP addresses are the same MBG. This does not cause any issues in Management Portal (other than it being treated as two separate MBGs) but may confuse the administrator. It is recommended that MBGs be registered in a consistent manner.

> ⚠ Ensure that Web Services have been enabled on the configured standalone MBG. Otherwise, communication between the MBG and Management Portal will fail.

To register an MBG Cluster and assign it to a Platform Group:

Registering an MBG cluster configures the DNS Server record on the DNS server to provide the MBG FQDN to the MBG cluster member hostname mapping.

1. From the **Platforms** tab, click the **MiVoice Border Gateways** tab.
2. Click **Register MiVoice Border Gateway Cluster**.

   > ⚠ If you register an MBG Cluster after adding users, the changes that you make to the Public Facing FQDNs are not updated in the MiCollab Client User Settings. To update the settings and send users the updated MBG information (SIP username, SIP password, and external FQDN), resend the Welcome email.

3. Enter details and then click **Submit**.

Make sure you enter the MSL Username and Password in the appropriated fields when registering the MBG. Otherwise, the registration will fail.

Re-enter the MSL Username and Password credentials when doing edit operations (such as when editing a Platform Group).

Extend the number of agent skill groups available in Management Portal

Each instance of MiVoice Business in Management Portal can have a maximum of 999 agent skill groups. However, in Management Portal, call flows use agent skill groups with ACD Paths and by default the MiVoice Business Multi-Instance configuration limits the number of agent skill groups to 64. You can increase this limit by changing the Extended Agent Skill Group setting in the License and Option Selection form.

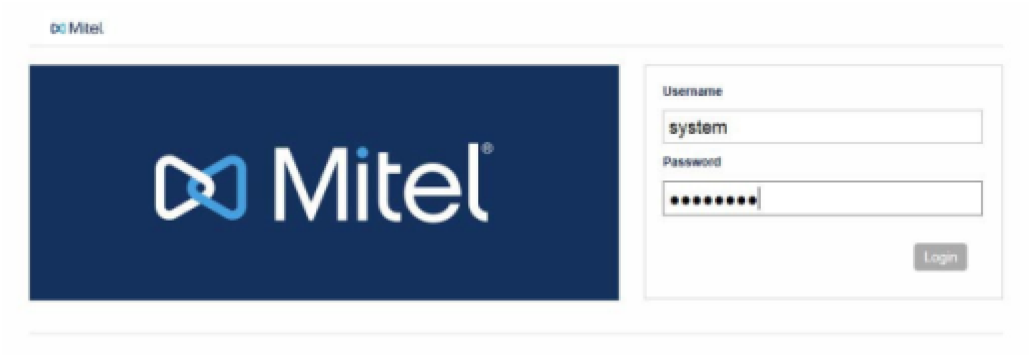
Set up Management Portal

Before provisioning customers, plan the bundles to be offered to customers and do a preliminary set up on the Management Portal.

Log in

Log into Management Portal with the default Username and Password:

- Username: **system**
- Password: **password**



Portal login formats

Here are the URL formats required for Management Portal:

Service Provider portal (Value Added Reseller/Virtual Service Provider)

- https://{address of MMP}/konos/login.do?id={web_id}

Service Provider portal

- https:// {address of MMP}/konos/sp/spLogin.do

Customer Administrator portal (Value Added Reseller/Virtual Service Provider/Service Provider)

- https:// {address of MMP}/customeradmin/{web id of customer}

End User portal

- https://{address of MMP} /konos/login.do?id= {web_id}

To configure timeout using maintenance command:

- Login to Service Provider portal or Customer Administration portal as mentioned above.
- Enter this URL in the same active service provider browser session (https://xx.xx.xx.xx/konos/commands.jsp) Replace xx.xx.xx.xx with the Management Portal server IP address or FQDN.

This will open up the Management Portal Service Provider maintenance command window.

- Enter the following command to update a single MiVoice Business and click **Submit**.

```
sysprop ORIA_PORTAL_TIMEOUT <value>
```

For example: sysprop ORIA_PORTAL_TIMEOUT 5. The *value* should be in minutes.

⚠ The default timeout is 15 minutes. Configured timeout will be effective from the next login.

Plan bundles for customers

To plan and determine the necessary bundle and feature requirements:

- Identify user types within potential customers and determine requirements for each user type.
- Design bundles with feature/phone type combinations that will satisfy your requirements of user types.

See tables for details:

- Table 1 Supported Phone Sets
- User Bundle Features by Service and License Type:
    - Table 2 MiCloud Business Virtual
    - Table 3 MiCloud Business Multi-Instance
- Phone Types by Service Type :
    - Basic IPT License
        - Table 4 Basic IPT MiCloud Business Virtual
        - Table 5 Basic IPT MiCloud Business Multi-Instance
    - Standard IPT License
        - Table 6 Standard IPT MiCloud Business Virtual
        - Table 7 Standard IPT MiCloud Business Multi-Instance
    - Entry UCC License
        - Table 8 Entry UCC MiCloud Business Virtual
        - Table 9 Entry UCC MiCloud Business Multi-Instance
    - Standard UCC License
        - Table 10 Standard UCC MiCloud Business Virtual
    - Premium UCC License
        - Table 11 Premium UCC MiCloud Business Virtual
    - Contact Center Agent
        - Table 12 Contact Center Agent MiCloud Business Virtual
        - Table 13 Contact Center Agent MiCloud Business Multi-Instance
    - Table 14 Management Portal Administrator Bundle Features

Considerations

- User Bundle phone features are dependent upon the service type and license type selected for the type of user.
- Up to three phone types per bundle can be configured, depending upon the service type and license type selected for the type of user for the bundle.

  ⚠ When you downgrade a user bundle from Management Portal, for example a user going from 3 phones down to 2, the MiCollab Client API will cause the user's status to be deleted and recreated. The user will need to log out of MiCollab Client, log in again and manually recreate their routing rules (set which devices will ring in different states).

- Phone types and feature profiles are also dependent upon the service type and license type selected for the type of user (see Table 2, "Phone Types by Service Type,")
- When selecting UCC user bundles, and creating MiCollab Client Service users through Management Portal, Management Portal will strip out any domain names from the username field before saving it to MiCollab. However, the user will receive a welcome email

from MiCollab Client Service with the login ID to be <username>.<Enterprise domain name>. It will be necessary to inform MiCollab Client Service users that they need only to log in with their user ID, not including the domain name.
- When MiCollab Client Service users have been created, and after being put in service, there is a subsequent change to a user or a service, that user will receive a logout request on their MiCollab Client application.
- When a MiCollab Client user changes their credentials in their MiCollab Client, and subsequently those credentials are changed within Management Portal, Management Portal will overwrite the credentials on the MiCollab Client for that user.
- If a MiCloud Business Multi-Instance user has been created (a SB Entry UCC Bundle) with Twinning, and the user's firstname, lastname, as well as their email address is edited via Management Portal, then their IMAP Account Login in the Voicemail tab must be changed manually in the Edit User form in the Management Portal customer admin portal if the Embedded UM Enabled option is selected.
- PC MiNet Softphone phone types are programmed on the MiCollab Client MBG.
- When users with MiCloud Business Virtual bundles are created, languages are set by default based on the MiCollab default language for applications such as MiCollab Client.
- When users with MiClould Business Mutli-Instance bundles are created, Management Portal can set the language for applications such as MiCollab Client because the MiCollab server is not involved in configuring those applications.
- Modifying a user with a bundle containing the Hot Desk or ACD feature to one with a non-Hot Desk or non-ACD feature is not permitted. Modifying a user with a bundle containing a non-Hot Desk or non-ACD feature to one with a Hot Desk or ACD feature is not permitted. Only changes between non-Hot Desk or non-ACD bundles, as well as bundles that contain the Hot Desk or ACD features are permitted.
- Users assigned bundles with Mobile Softphone, PC Softphone, Generic SIP, Hotdesk, or ACD Phone Types will not have their Call History display within their Management Portal page.
- Provide access to site administration features on the portal.
- Determine the Class Of Service (COS) numbers that will be used for each Feature Profile (determine Day/Night1/Night2 service).
- Record the Feature Profiles with COS numbers and feature combinations for each Feature Profile.

Tip
Part of designing a bundle is to design a Feature Profile that will define the phone set features that a bundle will provide to the assigned user. A Feature Profile is essentially registered as a Class of Service (including Day/Night1/Night2 time of day settings).

Table 1 Supported Phone Sets

6970 conference phone is deployed as a single device only with the following restriction till MiVoice Business starts supporting 6970:
- 6970 cannot be configured as a third device in MiCloud Management Portal, as it is considered as deskphone in MiCloud Management Portal.

Phone Type	Models
IP	5220, 5304, 5312, 5320, 5320e, 5324, 5330, 5330e, 5340, 5340e, 5360, 5215, 5235, 6920, 6930, 6940, 6970 (6970 is mapped to 6940 till MiVoice Business starts supporting 6970), 6905, 6910
SIP	5603, 5604, 5607, 5610, 5624
Dual Mode	5212, 5220, 5224
DECT	112
Open Phone	26, 27
SIP-DECT	612, 622, 632, 650

User Bundle Features by Service and License Type

Table 2 MiCloud Business Virtual

Service type	MiCloud Business Virtual					
Feature	Basic IPT	Standard IPT	Entry UCC	Standard UCC	Premium UCC	Contact Center Agent
Prime Phone	Y	Y	Y	Y	Y	Y
Second Phone	N	N	Y	Y	Y	N
Third Phone	N	N	Y	Y	Y	N
Fourth Phone	N	N	Y	Y	Y	N
Optional features						
Voicemail	N	Y	Y	Y	Y	Y
Voicemail to Email	N	N	N	N	N	N
Nupoint Class of Service	N	Y	Y	Y	Y	Y
Message Waiting	N	Y	Y	Y	Y	Y
Unified Messaging	N	N	Y	Y	Y	N
Standard Unified Messaging	N	N	Y	Y	Y	N
Advanced Unified Messaging	N	N	Y	Y	Y	N
AWV Conferencing	N	N	N	Y	Y	N
MiCollab Client Service	Y	Y	Y	Y	Y	Y
Chat	Y	Y	Y	Y	Y	Y
Lync/Skype For Business (SFB) Plugin ⚠ SFB Plugin is applicable only when MiCollab release is 8.1.1.11 or greater.	N	N	Y	Y	Y	N
MiCollab Console	Y	Y	Y	Y	Y	N
MiTeam	N	N	N	N	Y	N
Next Gen Mobile SIP Phone Settings	Y	Y	Y	Y	Y	Y
Enable Secure Transport	Y	Y	Y	Y	Y	Y
Compression	Y	Y	Y	Y	Y	Y

Table 3 MiCloud Business Multi-Instance

Service type	MiCloud Business Multi-Instance			
Feature	Basic IPT	Standard IPT	Entry UCC	Contact Center Agent
Prime Phone	Y	Y	Y	Y
Second Phone	N	N	Y	N
Third Phone	N	N	Y	N
Fourth Phone	N	N	Y	N
Optional features				
Voicemail	N	Y	Y	Y
Voicemail to Email	N	Y	Y	Y
Nupoint Class of Service	N	N	N	N
Message Waiting	N	N	N	N
Unified Messaging	N	N	N	N
Standard Unified Messaging	N	N	N	N
Advanced Unified Messaging	N	N	N	N

AWV Conferencing	N	N	N	N
MiCollab Client Service	Y	Y	Y	Y
Chat	Y	Y	Y	Y
Lync/Skype For Business (SFB) Plugin ⚠ SFB Plugin is applicable only when MiCollab release is 8.1.1.11 or greater.	N	N	Y	N
MiCollab Console	Y	Y	Y	N
MiTeam	N	N	Y	N
Next Gen Mobile SIP Phone Settings	Y	Y	Y	Y
Enable Secure Transport	Y	Y	Y	Y
Compression	Y	Y	Y	Y

Phone Types by Service Type

Table 4 Basic IPT License - MiCloud Business Virtual (MLB)

Service type	MiCloud Business Virtual (MLB)			
Phone type	PRIME	SECOND	THIRD	FOURTH
Deskphone	Y	NA	NA	NA
PC MiNet Softphone	Y	NA	NA	NA
PC SIP Softphone	Y	NA	NA	NA
Mobile SIP Softphone	Y	NA	NA	NA
Next Gen Mobile SIP Softphone	Y	NA	NA	NA
Hotdesk	Y	NA	NA	NA
ACD	Y	NA	NA	NA
ACD With Softphone	Y	NA	NA	NA
Generic SIP	Y	NA	NA	NA
MiVoice Conference Phone	Y	NA	NA	NA

Table 5 Basic IPT License - MiCloud Business Multi-Instance

Service type	MiCloud Business Multi-Instance			
Phone type	PRIME	SECOND	THIRD	FOURTH
Deskphone	Y	NA	NA	NA
PC MiNet Softphone	Y	NA	NA	NA
PC SIP Softphone	Y	NA	NA	NA
Mobile SIP Softphone	Y	NA	NA	NA
Next Gen Mobile SIP Softphone	Y	NA	NA	NA
Hotdesk	Y	NA	NA	NA
ACD	Y	NA	NA	NA
ACD With Softphone	Y	NA	NA	NA
Generic SIP	Y	NA	NA	NA
MiVoice Conference Phone	Y	NA	NA	NA

Table 6 Standard IPT License - MiCloud Business Virtual (MLB)

Service type	MiCloud Business Virtual (MLB)			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
Deskphone	Y	NA	NA	NA
PC MiNet Softphone	Y	NA	NA	NA
PC SIP Softphone	Y	NA	NA	NA
Mobile SIP Softphone	Y	NA	NA	NA
Next Gen Mobile SIP Softphone	Y	NA	NA	NA
Hotdesk	Y	NA	NA	NA
ACD	Y	NA	NA	NA
ACD With Softphone	Y	NA	NA	NA
Generic SIP	Y	NA	NA	NA
MiVoice Conference Phone	Y	N	N	N

Table 7 Standard IPT License - MiCloud Business Multi-Instance

Service type	MiCloud Business Multi-Instance			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
Deskphone	Y	NA	NA	NA
PC MiNet Softphone	Y	NA	NA	NA
PC SIP Softphone	Y	NA	NA	NA
Mobile SIP Softphone	Y	NA	NA	NA
Next Gen Mobile SIP Softphone	Y	NA	NA	NA
Hotdesk	Y	NA	NA	NA
ACD	Y	NA	NA	NA
ACD With Softphone	Y	NA	NA	NA
Generic SIP	Y	NA	NA	NA
MiVoice Conference Phone	Y	NA	NA	NA

Table 8 Entry UCC License - MiCloud Business Virtual (MLB)

Service type	MiCloud Business Virtual (MLB)			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
Deskphone	Y	N	N	N
External Phone	N	Y	N	N
PC MiNet Softphone	Y	N	Y	Y
PC SIP Softphone	Y	N	Y	Y
Mobile SIP Softphone	Y	N	Y	N
Next Gen Mobile SIP Softphone	Y	N	Y	Y
Hotdesk	Y	N	N	N
Generic SIP	Y	N	Y	Y
MiVoice Conference Phone	Y	N	Y	Y

Table 9 Entry UCC License - MiCloud Business Multi-Instance

Service type	MiCloud Business Multi-Instance			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
Deskphone	Y	N	N	N
External Phone	N	Y	N	N
PC MiNet Softphone	Y	Y	Y	Y
PC SIP Softphone	Y	Y	Y	Y
Mobile SIP Softphone	Y	Y	Y	N

Service type	MiCloud Business Multi-Instance			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
Next Gen Mobile SIP Softphone	Y	Y	Y	N
Hotdesk	Y	N	N	N
Generic SIP	Y	Y	Y	Y
MiVoice Conference Phone	Y	Y	Y	Y

Table 10 Standard UCC License - MiCloud Business Virtual (MLB)

Service type	MiCloud Business Virtual (MLB)			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
Deskphone	Y	N	N	N
External Phone	N	Y	N	N
PC MiNet Softphone	Y	N	Y	N
PC SIP Softphone	Y	N	Y	N
Mobile SIP Softphone	Y	N	Y	Y
Next Gen Mobile SIP Softphone	Y	N	Y	Y
Hotdesk	Y	N	N	N
Generic SIP	Y	N	Y	Y
MiVoice Conference Phone	Y	N	Y	Y

Table 11 Premium UCC License - MiCloud Business Virtual (MLB)

Service type	MiCloud Business Virtual (MLB)			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
Deskphone	Y	N	N	N
External Phone	N	Y	N	N
PC MiNet Softphone	Y	N	Y	Y
PC SIP Softphone	Y	N	Y	Y
Mobile SIP Softphone	Y	N	Y	N
Next Gen Mobile SIP Softphone	Y	N	Y	N
Hotdesk	Y	N	N	N
Generic SIP	Y	N	Y	Y
MiVoice Conference Phone	Y	N	Y	Y

Table 12 Contact Center Agent - MiCloud Business Virtual (MLB)

Service type	MiCloud Business Virtual (MLB)			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
ACD	Y	NA	NA	NA
ACD With Softphone	Y	NA	NA	NA
ACD With SIP Softphone	Y	NA	NA	NA

Table 13 Contact Center Agent - MiCloud Business Multi-Instance

Service type	MiCloud Business Multi-Instance			
Phone type	**PRIME**	**SECOND**	**THIRD**	**FOURTH**
ACD	Y	NA	NA	NA
ACD With Softphone	Y	NA	NA	NA
ACD With SIP Softphone	Y	NA	NA	NA

Table 14 Management Portal Administrator Bundle Features

Bundle type	Feature	Description
Administrator Bundle	ACD Groups	Allows you to create groups of users that can be placed in call paths such as those used by call centers and support groups.
	Advanced Settings	Allows you to modify business hours.
	Advanced ACD Groups	Provides access to all the advanced ACD features in ACD paths.
	ACD Paths	Allows you to create, modify, and delete ACD paths that are used by call centers and support groups.
	Advanced ACD Paths	Provides access to all the advanced ACD features in ACD paths.
	ACD Music On Hold	Allows you to create, add, or remove MOH for ACD.
	Auto Attendant	Allows you to create, modify and delete Auto Attendant call flows.
	Call Flows	Allows you to create, modify and delete company call flows.
	Call Groups	Allows you to create, add or remove users to Pickup Groups, Hunt Groups, and Ring Groups.
	Call Rerouting Destinations	Lets the system redirect calls to alternate answering points or devices.
	Company Speed Dial	Enable user to create, modify and delete company wide speed dial numbers.
	Email Capabilities	Enables the user to send information emails and reset passwords.
	General Mailbox	Allows the user to create, modify and delete general company mailboxes.
	Hot Desk Phones	Allows users to create, modify and delete hot desk devices.
	Key Templates	Lets you manage and assign key templates.
	Music On Hold	Lets you enable and upload embedded Music On Hold (MOH) for a site.
	Override Feature Profile	Lets you override Feature Profile settings when creating or modifying a user.
	Override Feature COS	Lets you override feature COS when creating or modifying a user.
	RAD Programming	Allows you to create, modify, and removed RAD greetings and MOH.
	Synchronize Platforms	Lets you initiate the Synchronize Platforms operation for a Customer.
	Users	Provides access to the directory to create, modify and delete a customer's users.
	Work Groups	Lets you program the Call Coverage Service number.

Create and change bundles

Bundles are groups of features, phone types, and devices that is assigned to one or more customers. You must create at least one user bundle before the customer administrator can create a user.

There are two types of Bundles that can be created in Management Portal:

- Administrator
- User

Administrator bundles typically provide access to other system management functions such as managing Call Groups, Hot Desk Phones, and Key Templates. User bundles are primarily based on the service and license types you choose. See Planning Bundles for Customers for details about user bundle services by license type.

Notes

When you downgrade a user bundle from Management Portal, for example a user going from 3 phones down to 2, the MiCollab Client API causes the user's status to be deleted and recreated. The user needs to log out of MiCollab Client, log in again and manually and recreate their routing rules (set which devices will ring in different states).

When you change a bundle that includes a teleworker set (registered to MiVoice Business), the configured MiVoice Business settings on the MiVoice Border Gateway revert to the default settings, and the teleworker set logs out. To fix this issue, manually change the MiVoice Business settings on the MiVoice Border Gateway back to the original configured MiVoice Business settings. The MAC address is not affected.

User bundle services and license types

The services available for user bundles are MiCloud Business Multi-Instance and MiCloud Business Virtual. Each MiCloud service provides a number of license types to choose from:

MiCloud Business Multi-Instance

- Basic IPT
- Standard IPT
- Entry UCC
- Contact Center Agent

MiCloud Business Virtual

- Basic IPT
- Standard IPT
- Entry UCC
- Standard UCC
- Premium UCC
- Contact Center Agent

Bundle optional features

The following optional features are available for phone users, depending on the service and license type you choose:

- Voicemail
- Voicemail To Email
- AWV Conferencing
- MiCollab Client Service
  - Chat
  - Lync Plugin/Skype For Business (SFB)

> ⚠ Skype For Business (SFB) details are mentioned in the welcome email notification when MiCollab release is 8.1.1.11 or greater.

  - MiCollab Console
  - MiTeam
- Next Gen Mobile SIP Phone Settings
  - Enable Secure Transport
- Compression
  - Wideband Audio
  - Compressed
  - Non Compressed

You can also configure the following Voicemail features:

- Voicemail
  - Attendant Extension
  - NuPoint Class of Service
    - Feature COS
    - Limits COS
  - Message Waiting
    - Message Waiting #1
    - Message Waiting #2
  - Unified Messaging
    - Standard Unified Messaging

- Advanced Unified Messaging

ACD in Customer Administrator Bundles

When Customer Administrator bundles are created, customer admins can be assigned permissions like Basic or Advanced Groups, Basic or Advanced Paths, ACD Music on Hold, and RAD Programming.

When you create Customer Administrator bundles, you decide what level of permissions you assign to your customer admins, Basic or Advanced Groups, Basic or Advanced Paths, ACD Music on Hold, and RAD Programming.

When you create a Customer Administrator bundle, Management Portal includes a default set of permissions. You can change these permissions for each Customer Administrator bundle. See Assign Customer Admin Features for ACD.

Create bundles

Create the bundles that you plan to assign to customers and administrators. To meet the demands of potential customers, design a variety of bundles, and then create them on the system.

> ⚠ **Note**
> Do not set the extension and mailbox length at the maximum if you plan to create a user with more than one phone. Implementing the following settings will prevent a customer administrator from creating a user with more than one phone:
>
> - Create bundle with more than one phone.
> - Create a customer with unrestricted extension length and set the MiVoice Business mailbox at maximum length (7).
> - Create a user with the maximum extension length (7).

To create a User bundle:

1. From the Management Portal service provider portal, click the **Bundles** tab.
2. Click **Create Bundle**.
3. Select **User Bundle** and click **Next**.
4. Under **Bundle Details**, enter a name, code, and description for the bundle.

   > ⚠ If you are deploying MiCollab Clients for Mobile users, you need to create a special User Bundle of type Next Gen Mobile SIP Softphone. See MiCollab Clients for Mobile.

5. Under **Phone User Features**, select the:
   Service and license type.
   Optional features - The optional features and profiles available depends on the selections. See Planning Bundles for Customers for information about the service and license types.
   Prime phone settings - Select the prime phone type and select one or more feature profiles for the bundle. When the phone type is set to none, the feature profile selection tool is disabled.
6. Under **Bundle Devices**, select one or more devices to include in the bundle.
7. Click **Submit**.
8. (optional) Upload any setup instructions that you want to include as an attachment in the Welcome Email.
9. Click **Save**.

Notes:

Sometimes failures may occur during a change bundle operation. It is now possible to rollback the change to its previous configuration. Should a failure occur during a Change Bundle operation, there will be a series of guided prompts in Management Portal to either correct the error or revert back to the previous bundle configuration.

The Management Portal MiCollab Bundle only enables the Advanced MiCollab Unified Messaging Telephone User Interface features. You must log into Server Manager and open the Nupoint Web Console to provision the end user’s Adv. UM Alias, and password (if required).

To create an Administrator bundle:

1. From the Management Portal service provider portal, click the **Bundles** tab.
2. Click **Create Bundle**.
3. Select **Administrator Bundle**.
4. Under **Bundle Details**, enter a name, code, and description for the bundle.
5. Under **Select Site Administration Features**, select the administration features for the bundle.
6. Click **Submit**.

Override feature and phone profiles in bundles

You can set permissions that allow a Customer Administrator to override the following bundle fields in Management Portal:

- Phone Feature Profiles
- FCOS

Feature profiles for phones

You can allow Customer Administrators to override phone feature profiles in a bundle. When using the override feature, the first feature profile you choose is the default.

To allow Customer Administrators to add or change the phone feature profile for users, select the *Override Feature Profile* option under the Site Administration Features section in the Administrator bundle.

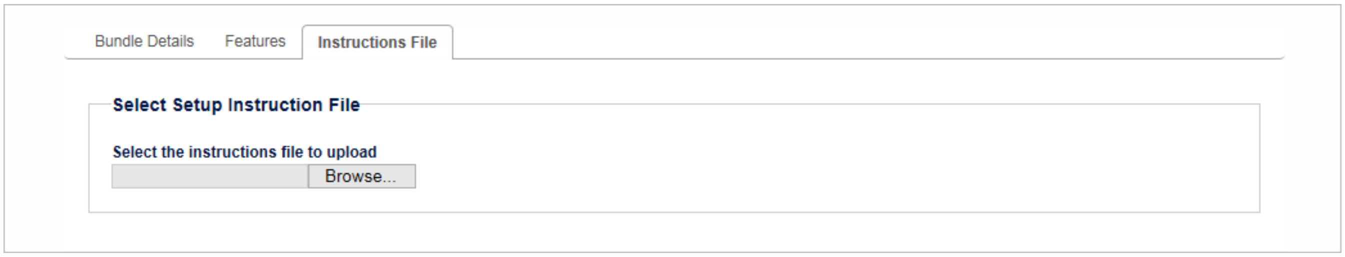
Feature profiles for voice mailboxes

You can select a feature profile for a user's voice mailbox in the Customer Administrator Advanced tab based on the list FCOS options available in MiCollab. The default feature profile is the one in the bundle assigned to the user. If the default feature profile for the bundle is not in the MiCollab list, it will not appear in feature profile list.

To allow Customer Administrators to add or change the phone feature profile for users, select the *Override FCOS Profile* option under the Site Administration Features section in your Administrator bundle.

Upload bundle setup instructions

When you create a bundle, you can choose to upload setup instructions for users. The instructions are sent as an attachment in the Welcome email and also made available (download) in the user portal My Services page. All document file formats are supported and there are no file size restrictions on the My Services page.



Select Setup Instruction File

Select the instructions file to upload

Register dialing privileges

Dialing Privileges correspond to Class of Restriction (COR) numbers that have been pre-configured to specific Automatic Route Selection (ARS) routes programmed on the default MiVoice Business database.

As a recommended guideline:

- Create and pre-configure all required Dialing Privileges on the default MiVoice Business database prior to customer creation.
- Design the Dialing Privileges based on predictions of where calls will come from and what type of outbound calling privileges will be required.
- Configure the Dialing Privileges to be the same on every MiVoice Business Platform that is managed using Management Portal. The goal is to create a shared set of dialing privileges that can be assigned to any customer provisioned using Management Portal and allow each customer to access the same routes. Due to this requirement, a Default MiVoice Business Platform Database must be created to include ARS programming that can be set for all MiVoice Business Platform instances.

To plan and determine the necessary dialing privilege requirements:

1. Determine cities, states/provinces, and countries in which service will be provided.
2. Gather all dialling patterns (local, long distance, international, etc.) that will be offered.
3. Determine all required Dialing Privileges to satisfy customer needs. (Capturing this information in a spreadsheet will make it easier to enter the information in Management Portal.)
4. Ensure design has been completed properly for default MiVoice Business Platform data- base configuration.

To register Dialing Privileges:

1. Log in to Management Portal.
2. Click the **Telephony** tab and select **Dialing Privileges**.
3. Click **Register Dialing Privilege**.

Create key templates

You can set up phone keys and default key templates from within the service provider portal and assign them to a customer during customer creation. After a template is assigned, changes made to it from the service provider portal are not applied to the template viewed by the Customer Administrator. The Customer Administrator sees the template as it was initially configured.

Service Providers can create Key Templates for Customer Administrators to use when setting up users instead of programming the keys manually.

Multi-Call key on Primary Phone

The Multi-Call key is programmed automatically on all SIP phones that are configured as primary phones. If the key template is already configured as a Multi-Call key, then the key template is used to create the Multi-Call key for the primary phone. If there is no key template or the key template does not have a Multi-Call key, Management Portal automatically adds the Multi-Call key on the next available key.

Multi-Call key on 2nd, 3rd and 4th phones

The Multi-Call key is programmed on the following SIP devices (UC Endpoints) automatically for the 2nd(SB path), 3rd or 4th phone.

- PC SIP Softphone
- Mobile SIP Softphone
- Next Gen Mobile SIP Softphone
- MiVoice Conference Phone

Because there is no key template (for 2nd, 3rd and 4th phones), Multi-Call key is automatically added by Management Portal. Multi-Call key is added to the 1st and 2nd key.

To create a key template:

1. From the **Telephony** tab, click **Key Templates**, then click **Create Template**.
2. (optional) In **Phone Layout**, select the phone layout to display. Leaving the setting at default displays all the possible phone keys.
3. Program each key by clicking it and setting the features. You can also apply the template to users who have one row of keys.
4. Click **Save**.

Create brands

Color schemes and images displayed throughout the portal can be created and modified to match a corporate brand or other desired customized brand. Multiple brands can be created on the system, which allows different service provider customers to have different portal branding schemes assigned to them.

The following modifiable branding options are available:

- Company Logo
- Login Page Image
- Portal Banner Image
- Favicon Image (Browser Tab)
- Navigation Bar Color
- Heading & Page Link Color

Use the brand creation wizard to create a customized brand that can be assigned to one or more customers. Users will see the images and colors associated with the brand assigned to their company while logged into the portal. When a change is made to a brand it is reflected across the system and any customers that were assigned the initial brand will see the changes when they log into the portal.

To create a Corporate Brand:

1. Collect the following information:
    a. URL for the following company pages:
    b. Company Website
    c. Terms of Use Page
    d. Privacy Policy Page
2. Image of the corporate logo:
    a. Recommended Dimensions: 60 pixels (height)
    b. Supported Formats: JPG / GIF / PNG
3. Design and create the following corporate images:
    a. b Login page
        i. Recommended Dimensions: 575 pixels X 230 pixels
        ii. Supported Formats: JPG / GIF / PNG
    b. c Portal banner
        i. Recommended Dimensions: 950 pixels X 150 pixels
        ii. Supported Formats: JPG / GIF / PNG
    c. d Favicon (browser tab)
        i. Recommended Dimensions: 17 pixels X 17 pixels
        ii. Supported Formats: ICO. An error message appears when the image is not in the correct format.
4. Determine color scheme for navigation bar and headings / page links. Color Code: HEX / RGB / HSB
5. Log in to Management Portal, click the System tab, select Brands, then click Create Brand.

Create Welcome e-mail

The Welcome e-mail is the e-mail message that new users receive when their account is created. Typically a Welcome e-mail contains welcome text and user login credentials. The Welcome e-mail is derived from the default e-mail template through customization. A service provider creates and edits e-mail templates in **System > Email Template**.

Management Portal displays the welcome e-mail in the receiver's language as long as that language is supported.

Note
If you need to stop welcome e-mail messages from being sent from MiCollab, you must disable the option from MiCollab.

The following flowcharts outline the steps required for setting up and generating the Welcome e-mail:

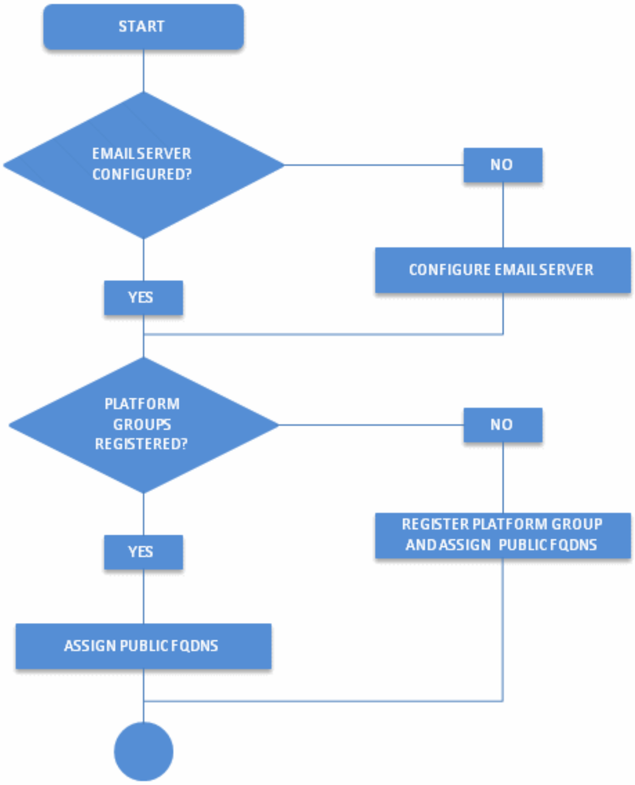


Figure 1: Register platform group and set up e-mail server

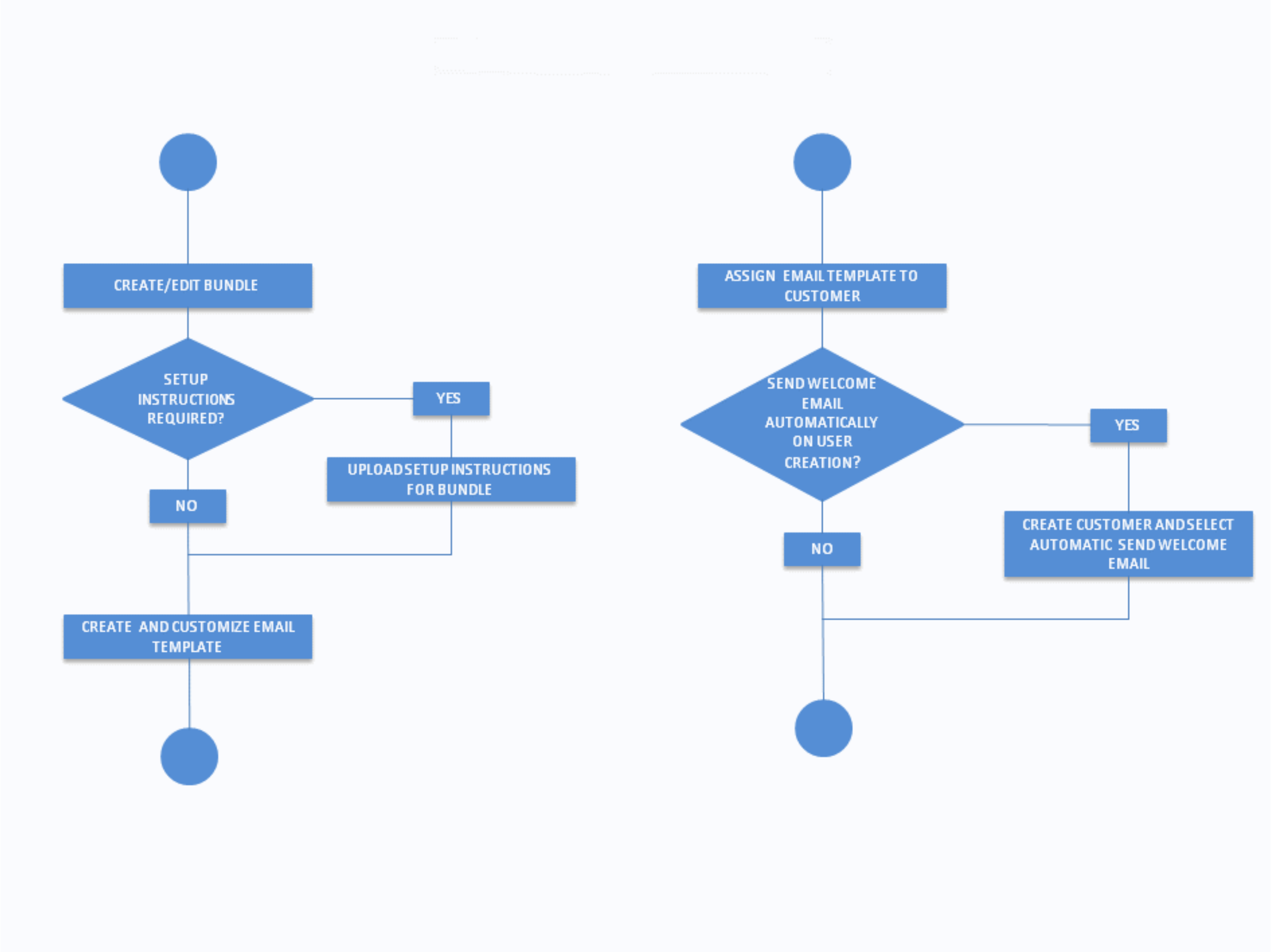

CREATE/EDIT BUNDLE
SETUP INSTRUCTIONS REQUIRED?
YES
UPLOAD SETUP INSTRUCTIONS FOR BUNDLE
NO
CREATE AND CUSTOMIZE EMAIL TEMPLATE
ASSIGN EMAIL TEMPLATE TO CUSTOMER
SEND WELCOME EMAIL AUTOMATICALLY ON USER CREATION?
YES
CREATE CUSTOMER AND SELECT AUTOMATIC SEND WELCOME EMAIL
NO

Figure 2: Create bundle and e-mail template

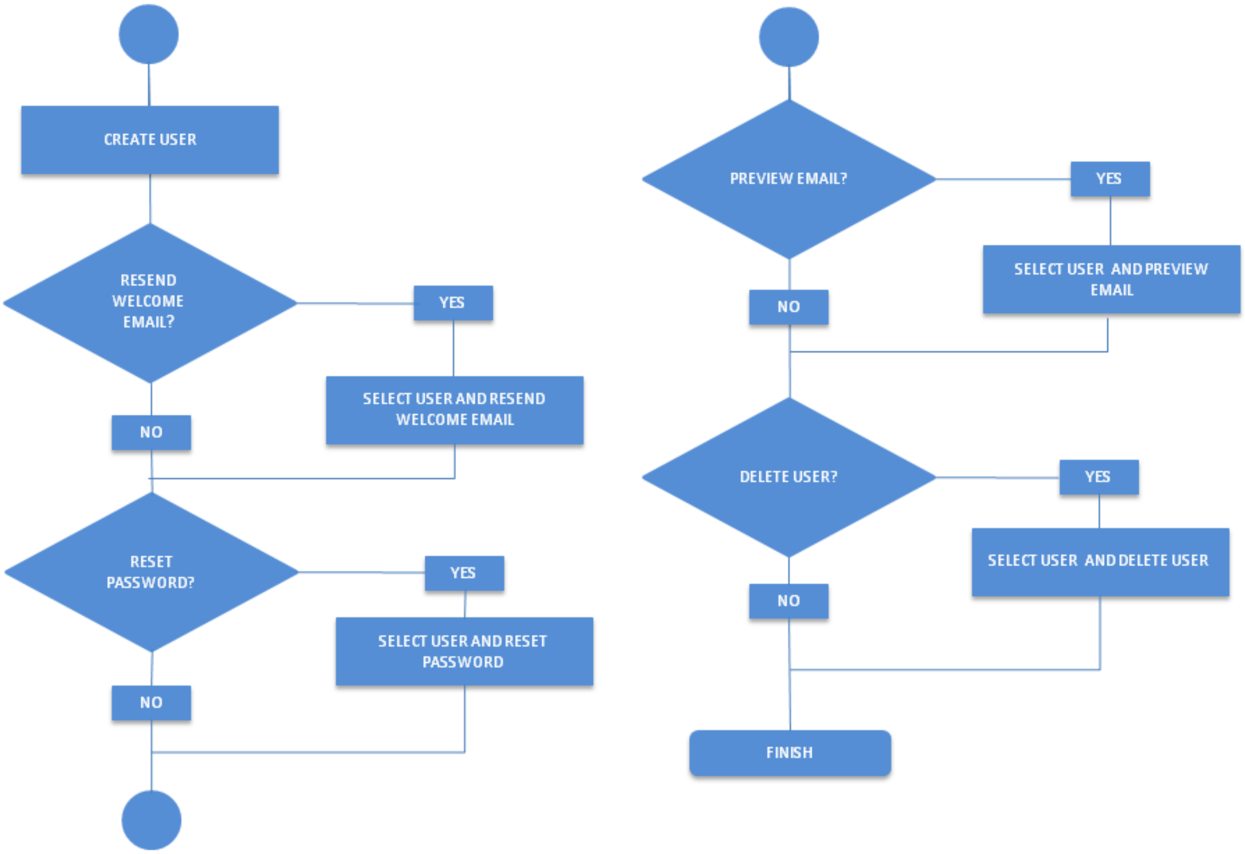

CREATE USER
RESEND WELCOME EMAIL?
YES
SELECT USER AND RESEND WELCOME EMAIL
NO
RESET PASSWORD?
YES
SELECT USER AND RESET PASSWORD
NO
PREVIEW EMAIL?
YES
SELECT USER AND PREVIEW EMAIL
NO
DELETE USER?
YES
SELECT USER AND DELETE USER
NO
FINISH

Figure 3: User Creation and Welcome e-mail

You can send a Welcome e-mail manually by selecting the user and then selecting the **Send Welcome Email** action. Or you may prefer to send the Welcome e-mail automatically to all users when they are created. Bulk Import supports the automatic sending of the Welcome e-mail on user creation. When users are added using Bulk Imports the Welcome e-mail is automatically sent to each user. Management Portal provides a default e-mail template with pre-populated content and all services enabled for both new installs and product upgrades. You cannot delete the default e-mail template.

Any setup instructions that you upload are sent with the Welcome e-mail and they are also accessible from the user's My Services page.

A Welcome e-mail can contain the following types of information:

- Customized content
- List of services the user has access to
- User name and password
- Links to services
- Links to application downloads

Language Support

The Subject, Greeting, and Footer text fields all support international text (UTF-8).

Default e-mail template content and options

The default e-mail template contains editable pre-populated content and has all options enabled:

- Sender’s e-mail address in the format donotreply@<OriaPublicFQDN>.com. The service provider can change the sender’s e-mail address if required.
- Greeting text.
- Footer text.
- Subject text: "Welcome to the User Portal", <lastname, firstname of the user as a suffix>

  > ⚠ **Note**
  > The Subject field supports plain text only.

- All the options are selected for the e-mail and portal.
- Branding in the e-mail is picked up from the service provider’s branding. The banner image is used in HTML e-mail messages.

Assign e-mail permissions

A service provider must assign customer administrators the e-mail capability in the Admin Bundle to allow them to resend the Welcome e-mail, reset passwords, and preview e-mail messages. The automatic sending of the Welcome e-mail on user creation is always set by the service provider.

The e-mail capability in Admin Bundle is required to let the Customer Admin send Welcome e-mails, reset passwords and preview e-mails. If a customer is not assigned with a bundle with the e-mail capability, only the service provider can "login as" a customer administrator to resend Welcome Emails or reset passwords. The customer administrator will not see those actions.

However, enabling or disabling the e-mail capability from the Admin bundle does not affect the automatic sending of Welcome Emails on user creation. The automatic sending of the Welcome e-mail is governed by a checkbox in the add/edit customer page.

Here is a summary of the permissions granted for e-mail templates and messages:

- E-mail template privileges are managed through Operations profiles.
- Only the service provider can create e-mail templates.
- A service provider should not include the e-mail capability in the Admin Bundle assign to a customer if the permission to send e-mail messages is not wanted.
- A service provider configures whether Welcome e-mail messages are automatically sent when a user is created. This will be done while creating the customer.
- A customer can send Welcome e-mail messages only when the Welcome e-mail template is assigned to them by a service provider.
- A customer can resend a Welcome e-mail or reset a password when assigned a bundle with those rights.
- With e-mail rights, a customer can upload instructions when configuring the e-mail template.

The instructions are sent with the e-mail and also appear on the **My Services** page.

Customize the Welcome e-mail content

You can customize the information in the welcome e-mail and have it automatically sent when a customer adds a new user to the portal. Service providers assign e-mail templates to Customers during Customer creation. Customers can then use the templates to send automatic e-mail messages with relevant information. For example, sending a reminder e-mail message when a password is reset.

Access to the Welcome e-mail feature is granted through:

- Any operations profile with the permission to create customers has access to the Welcome e-mail feature.
- All the Admin bundles that allow you the creation of users have access to the Welcome e-mail.

To customize the Welcome e-mail:

1. Configure the username in the subject of the e-mail and choose whether the name has a suffix or a prefix.
2. Add a custom header and footer. Headers and footers can contain HTML content.
3. Customize the e-mail message as required. You may want to include a note for the user who will install additional MiCollab Clients (for PC, Mac, or Mobile) that they will receive one or more additional e-mails with instructions for installing the MiCollab Clients on the various platforms.
4. Choose the options to include in the e-mail for the user, for example, the user name, password, links to application downloads and so on. Only the selected options appear in the e-mail message and the Services page.
5. (optional) Upload setup instructions that you want to send as an attachment.

To preview the Welcome e-mail:

1. Click Customer **> View Customers**.
2. Select the Customer and click the Log in as Customer icon.
3. From the Customer Administrator portal, click the Users and select the user.
4. Click **More > Preview Email**.

To resend the Welcome e-mail:

1. Click Customer **> View Customers**.
2. Select the Customer and click the Log in as Customer icon.
3. From the Customer Administrator portal, click the **Users** and select one or more users.

   > ⚠ An information pop-up is displayed if more than 25 users are selected. Click **OK** to continue or **Cancel** to cancel the action.

4. Click **More > Resend Welcome Email**.

To reset the password:

1. Click **Customer > View Customers**.
2. Select the Customer and click the **Log in as Customer** icon.
3. From the Customer Administrator portal, click the **Users** and select one or more users.

   > ⚠ An information pop-up is displayed if more than 25 users are selected. Click **OK** to continue or **Cancel** to cancel the action.

4. Click **More > Reset Passcode**.

Create e-mail templates

A service provider or anyone with e-mail template privileges can create and configure e-mail templates for customers. Customers then use the templates to send e-mail messages with specific information in them to one or more customers. For example, an e-mail message that reminds users to change their password.

To create an e-mail template:

1. From the **System** tab click **Email Template** and then click **Create Email Template**.
2. If creating a template for a customer, select **Customer Template** and click **Next**.
3. Enter the e-mail template details and select the content to include in the e-mail message.

Set up MiCollab Clients

Deploying MiCollab Client to users

There are many MiCollab Clients, including for PC, Mac, and the mobile operating systems. When creating the User bundles, assign the phone types as shown in the table.

WebRTC provides a web-based softphone that you access from a browser. The softphone supports audio calls using your PC microphone and speakers or USB headset.

For MiCollab Client	Include in User Bundle	Additional instructions
On Mac	PC SIP softphone	Enable MAC Client support. **
On PC	PC SIP softphone	Enable MAC Client support. **
On Web browser (WebRTC)	PC SIP softphone	Enable MAC Client support. ** **NOTE**: Chrome and Firefox are supported for WebRTC.
For Next Gen Mobile client	Next Gen Mobile softphone	
Basic Web Client	One of these: • Desk phone only or • ACD Agent only or • Hot desk only or • Generic SIP Device only	The MiCollab account has just the Default Feature Profile.

** Select the **Enable deployment of Next Gen Desktop Client (PC/MAC/Web). Minimum support for MAC/Web Client is MiCollab 7.1**. **The minimum support for PC Client is MiCollab 8.0** checkbox.

Each user who is assigned one or more phones will receive a Welcome e-mail and a Password e-mail from the Management Portal. Depending on the MiCollab Clients assigned to them (in their User Bundle), they will also receive zero (0) or more MiCollab Client Deployment e-mails.

The following table lists six scenarios and the e-mails each user will receive, based on the clients assigned to them. This table assumes:

- Minimum releases: MiCloud Business 4.0, MiCloud Management Portal 6.0, and MiCollab 8.0.
- **MAC Client support** is Enabled in each of these cases.

Scenario	Bundle with phones	Users will receive
1	One of the following: • Desk phone • PC MiNET* • PC SIP Softphone • Mobile SIP Softphone • Hot Desk phone • Generic SIP phone • MiVoice Conference Phone	Welcome e-mail Password e-mail 1 Deployment e-mail **NOTE**: PC MiNET softphone works only with the older PC clients.

Scenario	Bundle with phones	Users will receive
2	One of the following: • Desk phone • Mobile SIP Softphone • Hot Desk/Generic SIP • MiVoice Conference Phone PLUS • PC SIP Softphone	Welcome e-mail Password e-mail 1 Deployment e-mail
3	One of the following: • Desk phone • PC SIP Softphone • Hot Desk • Generic SIP • MiVoice Conference Phone PLUS • Next Gen Mobile	Welcome e-mail Password e-mail 1 Deployment e-mail
4	One of the following: • Desk phone • Hot Desk • Generic SIP • MiVoice Conference Phone PLUS • PC SIP Softphone PLUS • Next Gen Mobile	Welcome e-mail Password e-mail 2 Deployment e-mails
5	One of the following: • Desk phone • Mobile SIP Softphone • Hot Desk/Generic SIP • MiVoice Conference Phone PLUS • PC Minet Softphone*	Welcome e-mail Password e-mail 1 Deployment e-mail **NOTE**: PC MiNET softphone works only with the older PC clients.
6	ACD phone (MiCollab Client Service enabled)	Welcome e-mail Password e-mail
7	ACD with Softphone (MiCollab Client Service enabled)	Welcome e-mail Password e-mail

When you assign a Next Gen Mobile SIP Phone for MiCollab Client, consider adding text in the Welcome e-mail to notify users that they will receive an additional e-mail with instructions for deploying the Next Gen Mobile Phone. You can add more instructions, if required, to the Management Portal Welcome e-mail. See Create Welcome e-mail. For instructions on setting up MiCollab Client for Mobile users, see Optional: Prepare MiCollab Client for mobile users.

⚠ **Note**
If users are receiving the Welcome Email but not the Deployment email, make sure that the MiCollab server is able to contact the Redirect Server. Look in the MiCollab server logs for the error "Could not connect to Server... Network is unreachable".

Enable deployment of the Next Gen Desktop Client (PC/MAC/Web)

If you are deploying a PC/MAC/Web Client for the MiCollab Client service, you need to enable the service and assign the user a bundle that includes an PC SIP Softphone.

⚠ **Note**
If the MAC/Web/PC Client” checkbox is disabled after creating users, there is no impact on existing users who are already using the client application or logged in. The only way to remove the MAC/WEB/PC Client services is to perform change bundle to a non-PC SIP Softphone bundle.

To enable a PC/MAC/Web Client for the MiCollab Client Service:

1. On the **Customers** tab, click **View Customers**.

2. Click the customer name.

3. In the dialog box that appears, click the **Edit** icon in the top right-hand corner.

4. Click the **Service Bundles** tab.

5. In the **Next Gen Desktop Client** box, select **Enable deployment of Next Gen Desktop Client (PC/MAC/Web). Minimum support for MAC/Web Client is MiCollab 7.1**. **The minimum support for PC Client is MiCollab 8.0.**

6. Click **Save**.

Deployment e-mail template

Here is a recommended template to use for the MiCollab Client Deployment e-mail. MiCollab Client Server contains only one template for Deployment e-mails, so it's important to include details relevant to all users who will be deploying any of the MiCollab Client variations.

The variables are denoted with ####. The variables for Google Play Store, Apple Store, and so on, result in the appropriate clickable links being included in the email.

⚠ **Note**
For best results, copy this template into Microsoft NotePad, or similar, to remove all artifacts introduced by the PDF or HTML process. Then copy from NotePad to MiCollab Deployment.

Dear [####firstname####] [####lastname####],

You are receiving this e-mail because your Mitel MiCollab administrator has set up your Mitel MiCollab Client for your extension number ([####dn####]).

Note
If your extension number shows as (None), it means that you will have a deskphone, but no softphone on your PC or Mac.

As you start, open your Welcome E-mail.

If one of your phones shows as "Next Gen Mobile Client Softphone," this means that you are registered for a MiCollab Client for Mobile.
If you don't see "Next Gen Mobile Client Softphone,", you will install the Desktop Client (PC or Mac), which include the situation where the extension is shown as "None".

Step 1:

To install MiCollab Client on your mobile phone, click the App Store for your device.
(You have to be reading this e-mail on your mobile device for this to work.)

[####appstore####][####playstore####][####microsoftstore####][####bbworld####]

To install a MiCollab client on your Mac or Windows PC, click the appropriate button below.

[####appstore_mac####][####winpc####]

Step 2:

If you are reading this on your mobile phone, PC or MAC, and you have downloaded and installed the Next Gen Client application, use the following link to continue: [####link####]
This will launch your MiCollab Next Gen Client, and authenticate with the **key** shown below.

If you are reading this e-mail on your PC or MAC, or your administrator printed the e-mail, and you have downloaded and installed the MiCollab for Mobile application, use a QR-code reader application on your mobile phone to scan the QR-code below.
[####qrcode####]

You can also start the process by launching the MiCollab Client application on your phone, PC, or MAC. The client will request the authentication key.
Your key is: [####authtoken####]

Note:This is an automatic e-mail notification. Please do not reply to this email. Replies will not be read.

Bulk Import Users

Download the import spreadsheet for the customer, fill it in, and import the changes back into the portal. After filing in the information, import the spreadsheet back into the portal. It is best practice to import the spreadsheet back into the portal before making changes to customer MiVoice Business platforms, dialing privileges, bundles, or feature profiles. The maximum number of users you can delete at one time is 20.

If you have an Active Directory file, you can merge the .ldif file into the Management Portal Bulk Import workflow. See Map Active Directory Fields for Bulk Import.

To bulk import users:

1. From the **Customers** tab, click **Bulk Import**.
2. Click **Import Users** and do the following tasks:
    a. In **Step 1: Get Import File**, select the customer to which you want to add the users.
    b. Fill the required fields by following the instructions in the import spreadsheet.
        i. Password rules for **Admin Bundle** and **User Bundle** sheets:
            - On the spreadsheet, click the **Password*** column to view the password rule. If the password criteria is not met, warning message is indicated with different colors, as per the instructions provided in the instructions sheet.

        - Characters " is not allowed in password, due to Excel sheet limitations.
        - Characters [,], and [] are not allowed due to cracklib library limitation. These characters are valid only when combined with other characters. Example: Invalid: Andreasiskid123] valid: Andreasiskid@123]

    c. In **Step 2: Select Import File** Click Browse, select the updated spreadsheet.

        i. Following are the possible error messages that can appear after importing the file:

            - Password containing characters "," , "|" ,"'", username, webid, email will be invalid.
            - Password is too weak because of the dictionary pattern or word {word}.

3. Click **Submit**. To ensure the import runs smoothly, most of the portal locks during the import.

Configure Advanced Settings

Set key permissions

Set key permission to allow users to create and edit key templates and program phone keys.

To set key permissions:

1. From the **Systems** tab, click **Advanced**.
2. Click the **Key Permissions** tab.
3. Select the key permissions for these users; Service Provider (SP), Reseller (RS), Customer Administrator (CA) and End User (EU).
4. Click **Save**.

Program Auto Attendant

Auto Attendant settings display when the platform group type is MiVoice Business. For MiCollab and MiVoice Business Express, only the Voicemail Hunt Group Pilot Number field is displayed. You can program the following settings:

- **Voicemail Hunt Group Pilot Number**: Program the Voicemail Hunt Group Pilot Number. For example: 6000.
- **Bilingual Options for Auto Attendant**: Enable or disable the bilingual option for Auto Attendant and program the bilingual Key Number. For example: 8.
- **Default passcode for Auto Attendant Mailboxes**: Program the default passcode for Auto Attendant mailboxes. For example: 1111.
- **Supervised Transfer for Auto Attendant**: Enable or disable Supervised Transfer for the Auto Attendant and program the Ringback Timeout. For example: 17 seconds. For more information, see *System Applications* > *Messaging* > *Voice Mail (Embedded)* > *Programming* > *Setting the Auto Attendant Transfer Type* in the MiVoice Business System Administration Tool Help.

To program Auto Attendant settings:

1. From the **Systems** tab, click **Advanced**.
2. Click the **Auto Attendant** tab.
3. Enable, disable, and program the Auto Attendant settings.
4. Click **Save**.

Specify ranges

Lets you specify the lower and upper ranges for creating speed dials, generating auto attendant and general mailboxes, and generating directory numbers for call flows.

To program upper and lower ranges:

1. From the **Systems** tab, click **Advanced**.
2. Click the **Ranges** tab.

3. Program the ranges for Speed Dials, Auto Attendant and General mailboxes, and directory numbers for Call Flows.
4. Click **Save**.

Program call flows

Lets you specify default call flow settings:

Feature Access Codes: Program the Feature Access Codes the system will use for call flows:

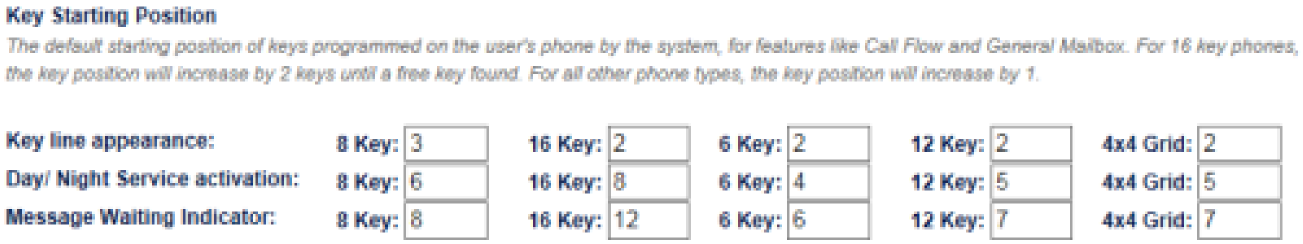
- Message Waiting - Activate
- Message Waiting - Deactivate
- Dialed Day/Night Service - Activate
- Call Forward - Follow Me - Third Party

Default Key Starting Position: Program the default phone key starting positions for users' phones.

- Key line appearance
- Message waiting indicator
- Day/Night service activation

To specify default call flow settings:

1. From the **Systems** tab, click **Advanced**.
2. Click the **Call Flow** tab.
3. Program the Feature Access codes and default key starting positions.
   Key starting positions apply when the user's prime phone is a Desktop phone. It does not apply to Hotdesk or ACD users. The Hotdesk/Hotdesk user's key starting position follows the 16 key phone.
4. Click **Save**.



Key Starting Position

The default starting position of keys programmed on the user's phone by the system, for features like Call Flow and General Mailbox. For 16 key phones, the key position will increase by 2 keys until a free key found. For all other phone types, the key position will increase by 1.

Key line appearance:	8 Key:	3	16 Key:	2	6 Key:	2	12 Key:	2	4x4 Grid:	2
Day/ Night Service activation:	8 Key:	6	16 Key:	8	6 Key:	4	12 Key:	5	4x4 Grid:	5
Message Waiting Indicator:	8 Key:	8	16 Key:	12	6 Key:	6	12 Key:	7	4x4 Grid:	7

Set billing change notifications

Click the **Billing Change Notification** tab to set the notification Customers see when they make changes that could affect their billing. You can set the text of the message, and the actions that will trigger display of the notification to Customers.

See Generate reports for detailed instructions for using these settings.

Set Platform Manager instance list caching

> **Note**
> The **Platform Manager** tab is shown only if Platform is registered with MiCloud Management Portal.

By default, Platform Manager refreshes the Platform instance list when configuring a platform. Select the **Cache Platform Instance List** option to schedule refresh of the list if there is a high number of Platform instances, and if there is a delay when when configuring the platforms.

To enable Platform Group Instance ID list caching:

1. From the **Systems** tab, click **Advanced**.
2. Click the **Platform Manager** tab.
3. Select **Cache Platform Instance List**.
4. In **Refresh Interval**, type a value between 1 and 1440 minutes. The default value is 60 minutes.

The Refresh interval indicates the interval after a current refresh option is completed. For example, if the refresh is scheduled every 1 minute, but the operation to fetch the platform IDs takes 5 minutes, then the next refresh will be started 1 minute after the completion of the earlier 5 minutes.

Getting started - Set up customers

Management Portal provides customers with access to the Customer Administrator self-service web portal. This section includes the following topics:

Make sure that you have registered a platform group for the customer and configured the bundles intended for sale. You will also need the customer's Calling Party Numbers (CPNs) and, if necessary, the customer's CESIDs.

⚠ You must create and provision users before connecting those users' phones. If not, you will receive an error indicating that the devices already exist on the MiVoice Border Gateway and cannot be assigned to those users.

Customers can perform the following specific site administration operations:

- Add and delete users
- Create customized device key templates for users
- Configure call groups (hunt, ring, and pickup)
- Setup group voicemail box
- Add and delete groups
- Create company-wide system speedcall numbers

Additionally, users have access to a variety of phone features defined by their assigned bundle. Management Portal enables the service provider to offer a self-service web portal where end users can perform the following tasks:

- Check missed calls even when away from their desk (applies to desktop phones only)
- Customize their phone and setup multiple speed dial keys
- Quickly search the company directory for contact details
- Change their voicemail passcode
- Configure their twinning settings, for example a phone and cell phone

Ensure that all collected customer and business requirements have been implemented in the portal. To provide a customer access to Management Portal, you must provide the unique URL of the customer portal. If the customer is given full site administration privileges, send the customer the administrator the primary account username and password.

Set up platform groups

Use Management Portal to assign one or more platform groups to a customer. To make a platform group available to a customer, register it and set it up as a site in a resilient or non-resilient environment. After setting up a site, you can set up MiCollab Client Multi-Tenant servers.

❗ It is not recommended to register MXe server via MiCloud Management Portal.

Enter a public facing domain name for each platform group you register so that users can access Mitel platforms and the Management Portal. Public facing fully qualified domain names (FQDN) are used to construct URLs. An FQDN is required for the following products:

- MiVoice Business
- MiVoice Business Express
- MiCollab
- Mitel Border Gateway

> Although the MiCollab Platform based solution includes MiVoice Business nodes there is no NAT support for the MiVoice Business only Platform solution.

Register a platform group

Registering a platform group with Management Portal allows you to assign it to a customer. Register a platform group with one MiVoice Business or with multiple resilient pairs. For each MyVoice Business pair, you must configure cluster elements in the System Administration Tool.

Important: When registering a platform group in Management Portal, the IP or FQDN entered for the hostname appears as the public facing domain name. You can choose to leave the default name or change it. The setting is available in the Advanced Settings page. Only a service provider can change the settings.

To register a platform group:

1. From **Platforms > Platform Groups**, click **Register Platform**. **Note**: Click **Save** to save the changes in the current tab before moving on to the next tab.
2. Select the platform type from the **Type** list.

   > **Notes**
   > It is important to enter the MSL Username and Password in the appropriated fields when registering a MiCollab or MiCollab with Voice platform group. Otherwise, the registration will fail.
   > When migrating from MiCollab 5.0 SP2 to MiCollab 6.0 SP1, you need to re-enter the MSL Username and Password credentials when performing edit operations (such as when editing a platform group).

3. Click **Submit** to register the platform group.
4. Add the MiVoice Business instance(s).
5. Add Sites as necessary to associate with the platform group. To add a site:
   a. Click the **Sites** tab.

      > When creating (or subsequently modifying) Sites and configuring the associated MBG(s), the User Phone Details will show up to four user phones that can be programmed on the MBG. Both the MiCloud Business Multi Instance and MiCloud Business Virtual Entry UCC Bundle has four phones associated with it. See Planning Bundles for the phone types supported for each license type. To ensure that the user's SIP phone number is programmed on the MBG, verify that the Third Phone check box is selected. To ensure that the user's SIP phone number is programmed on the MBG, verify that the Third Phone check box is selected.

   b. Click ➕ and follow the instructions.
6. Add MiCollab Client Tenants as necessary. To enable MiCollab MiTeam, click **MiTeam Service**.

To edit a platform group:

1. From **Platforms > Platform Groups**, click on the name of the platform group.
2. Click **Edit** icon (✎) on the right corner of the window.
3. Do the required changes in the following tabs:
   a. **Platform**
   b. **MiVoice Business**
      To Configure Voice Admin Password
      The **Voice Admin Password** field is displayed only for MiVoice Business version 9.0 and up. There are two conditions to display the **Voice Admin Password**:
      i. Enable SSH in MiVoice Business MSL. See ACD Greetings and Music on Hold to enable SSH.
      ii. If the Voice Admin Password is not displaying, check if MiVoice Business is up. Click **Save** once the MiVoice Business is up.

Enter **Voice Admin Password** (Optional). Voice Admin Password is required to communicate with the voice admin account present in MSL.

> ⚠ It is important to configure the Voice Admin Password in MiVoice Business MSL, else Management Portal throws an error that it is unable to upload the audio files as the Voice Admin Password does not exist.

To update Voice Admin Password for MiVoice Business using maintenance command

- Login to the Management Portal service provider portal (http://xx.xx.xx.xx/konos/sp/spLogin.do). Replace xx.xx.xx.xx with the Management
  Portal server IP address or FQDN.
- Enter this URL in the same active service provider browser session (https://xx.xx.xx.xx/konos/commands.jsp) Replace xx.xx.xx.xx with the
  Management Portal server IP address or FQDN. This will open up Management Portal Service Provider maintenance command window.
- Enter the following command to update a single MiVoice Business and click **Submit**.

  ```
  updateVoiceAdminPasswordForMcds IPADDRESS:PASSWORD
  ```

- Split the command using pipe character as below to update multiple MiVoice Business and click **Submit.**

  ```
  updateVoiceAdminPasswordForMcds IPADDRESS_1:PASSWORD_1|
  IPADDRESS_2:PASSWORD_2….. |IPADDRESS_5:PASSWORD_5
  ```

4. **MiCollab Client Tenant**
5. **SIP Billing Number**
6. **Sites**
7. **DIDs:**

> ⚠ When Management Portal is upgraded to Release **6.1** from any previous release, a **E.164** support checkbox for Upgrade is added in the **DID** tab. The **E.164** feature helps plus dialling support for creating, editing, and deleting the **DID** range.
> If MiVoice Border Gateway (embedded and external) is not registered in Management Portal, then the **E.164** support checkbox for Upgrade is hidden.

8. **To create DID range**
   a. Enter the values for **Range Start** and **Range End**.
   b. Select the **MBG Cluster**.
   c. Select the **SIP trunk**.
   d. Select the **Site**.
   e. Select the checkbox **E.164** for plus dialling support in creating a **DID** range. If the checkbox is selected, then **+DID** is generated in the MiVoice Border Gateway.

   > ⚠ If the checkbox is not selected, then only **DID** (without +) is generated in the MiVoice Border Gateway.

   f. Click **Save**.

To edit DID range

a. Click the ✎ . Edit the required fields.

> ⚠
> i. If the **E.164** checkbox is checked, then the plus sign is added before the selected **DID** range in the MiVoice Border Gateway for the existing DID range.
> ii. If the **E.164** checkbox is unchecked, then the plus sign is removed from the selected **DID** range in the MiVoice Border Gateway for the existing DID range.

b. Click ✓ . The changes are saved.

To delete DID range

   a. Click ✕ . The **DID** range is successfully deleted from MiVoice Border Gateway and Service Provider portal.

9. **Ranges**
10. **ACD Embedded RADs**
11. Click **Save**, once the required fields are updated.

To delete a platform group:

1. From **Platforms > Platform Groups, c**lick on the name of the platform group.
2. Click Delete icon on the right corner of the window.

   > If you are trying to delete MiVoice Business from MiCollab platform group, make sure that any user created directly on MiCollab do not reference the MiVoice Business in anyway.

Create a platform group using a Platform Manager blueprint

Platform Manager provides a way for Service Providers to create MiVoice Business and MiVoice Business Express platform groups based on blueprints created with Platform Manager.

> **Note**
> If you make a change to the Platform Manager server, for example change the credentials, make sure that you also change them in Management Portal.

To use Platform Manager blueprints in Management Portal, follow these steps:

1. Enable the Platform Manager feature.
2. Register Platform Manager.
3. Register a Platform Manager blueprint.
4. Create a platform group using a Platform Manager blueprint.

Step 1 Enable the Platform Manager feature:

1. From the **System** tab, click **Operations Profile**.
2. Do one of the following:
   a. To create a new profile and enable Platform Manager, click **Create Operations Profile**, select **Platform Managed** and other features and responsibilities to include in the profile.
   b. Select the profile, click the **Edit** icon, and select **Platform Managed**.
3. Click **Submit**.

Step 2 Register Platform Manager:

1. From the **System** tab, click **Platform Manager Registration**.
2. Do all for the following:
   a. In the **Host Name** field, enter the Platform Manager IP address or FQDN.
   b. In the **Username** and **Password** fields, enter the MSL Admin username and password.
   c. In the **Password Token** field, enter the token for establishing a trusted relationship between Management Portal and Platform Manager.
3. Click **Submit**.

Step 3 Register a Platform Manager blueprint:

Register a Platform Manager blueprint configured in Platform Manager so that you can automatically generate base platform instances during Customer provisioning.

To register a Platform Manager blueprint:

1. From the **Platforms** tab, click **Platform Manager Blueprints Assignment**.
2. Click **Register Platform Manager Blueprint**.
3. Enter a unique and meaningful name for the blueprint.
4. Select the Platform Manager blueprint to register.
5. Enter a description for the blueprint, including the specific platform features that are included. Some special characters [/, <, >, :, etc] are not supported.
6. Click **Submit.**

Step 4 Create a platform group using a blueprint or custom instance:

Create as many platform groups as you need using a blueprint or custom instance.

> ⚠ **Notes**
> After you create a platform group using a blueprint, you cannot add any more instances to that group.
> If you select **Configure Management Host Names for the Platform,** you need to configure the host names for each MiVoice Business instance in the MiVoice Business tab.

To create a MiVoice Business platform group:

1. From **Platforms > Platform Groups**, click **Register Platform**.
   Note: When registering a platform, click **Save** when working in each of the tabs associated with the task at hand, before moving on to the next tab.
2. From the **Type** drop-down list, select **MiVoice Business.**
3. From the **Blueprints** drop-down list, select the blueprint to use to create the platform group.
4. If you select **Managed Platform**, do the following steps:

   > ⚠ **Note**
   > If the platform comes from Platform Manager, you can deselect the Managed Platform option. After you disable the Managed Platform option and submit the change, it cannot be undone.

   From **Select instance by**, click **Blueprint**.
   a. From the **Blueprints** list, select the blueprint to use to create the platform group. OR
   b. From **Select instance by**, click **Custom** to select a custom instance.
   c. From the **Custom Instances** list, select the instance to use to create the platform group.
5. In **Public Facing FQDN/IP Address**, enter the FQDN.
6. Enter a description for the platform group.
7. Click **Submit**.

To create a MiVoice Business Express platform group using a blueprint or custom instance:

> ⚠ **Notes**
> When registering a platform, click **Save** when working in each of the tabs associated with the task at hand, before moving on to the next tab.
> When registering a platform in Management Portal, the IP or FQDN entered for the hostname appears as the public facing domain name. You can choose to leave the default name or change it. The setting is available in the Advanced Settings page. Only a service provider can change Advanced settings

1. From **Platforms > Platform Groups**, click **Register Platform**.
2. From the **Type** drop-down list, select **MiVoice Business Express.**
3. If you select **Managed Platform**, do the following steps:

> ⚠ **Note**
> If the platform comes from Platform Manager, you can deselect the Managed Platform option. After you disable the Managed Platform option and submit the change, it cannot be undone.

4. From **Select instance by**, click **Blueprint**.
    a. From the **Blueprints** list, select the blueprint to use to create the platform group. OR
    b. From **Select instance by**, click **Custom** to select a custom instance.
    c. From the **Custom Instances** list, select the instance to use to create the platform group.
5. In **Public Facing FQDN/IP Address**, enter the FQDN.
6. Select any additional platform options required for MBG, Mitel Management Gateway, third party NAT or VCNS.
7. Enter a description for the platform group.
8. Click **Submit**.

Update a registered Platform Manager server

You can modify all the settings after you register a Platform Manager server. If the IP address now points to a different Platform Manager server, make sure that you restore a backup from the original Platform Manager server.

> ⚠ **Caution**
> Pointing to a completely different Platform Manager server can result in unpredictable results.

Delete a registered Platform Manager server

You can delete a registered Platform Manager server if no platform groups are configured on it. Deleting the Platform Manager server also deletes all the configured Platform Manager blueprints.

Manage Platform Manager blueprints

Edit Platform Manager blueprints

You can change the Name, Description and Deprecated fields anytime after creating a blueprint. However, after you use a Platform Manager blueprint to create a platform group, you cannot change it. If you delete the platform(s) that use the blueprint, you can edit the blueprint again.

Delete Platform Manager blueprints

Similar to the Edit operation, you cannot delete a blueprint that was used to create a platform group. If you delete the platform(s) that use the blueprint, you can delete the blueprint.

Deprecate a Platform Manager blueprint

You can deprecate a Platform Manager blueprint so that it can no longer be used to create platform groups. A blueprint that is marked as "Deprecated", does not affect any existing platform groups created with the blueprint.

Set up MiCollab in a NAT network

NAT-based networks are required for MiCollab Platform-based solutions in MLB and SB deployments.

For Management Portal to access nodes (for example, MiVoice Business) from the SP Network, two IP addresses are required:

- Customer Host Name - the IP address configured on the node itself (for example MiVoice Business).
- Management Host Name - the IP address needed to access nodes (for example MiVoice Business) from the Service Provider network.

Step 1 Register the MiCollab platform with NAT support:

1. Click the **Platforms** tab, select **Platform Groups**, then click **Register Platform**.
2. Select **Configure Management Host Names For This Platform**. This information tells Management Portal that the MiCollab is deployed in a NAT network.

   > ⚠ **Note**
   > You cannot disable the **Requires Management Host Name Configuration** after you register the MiCollab platform.

3. Enter the required information.

   > ⚠ **Note**
   > Make sure you enter the Management Host Name IP address in the Host Name field. The Management Host Name IP address is used to access MiCollab from the Service Provide network and is not the actual IP Address (or FQDN) of the MiCollab on the Customer Network. The Public Facing FQDN/IP Address field is independent and has no effect on this configuration.

4. Click **Submit**.

Step 2 Configure the MiVoice Business node with the Management Host Name:

After MiCollab is registered, the MiVoice Business tab lists any MiVoice Business nodes that you add to MiCollab. By default MiVoice Business displays its own IP Address as configured in the Customer Network (the Customer Host Name field). Use the following procedure to configure the Management Host Name so that Management Portal can access the MiVoice Business from the Service Provider network.

1. Click the **MiVoice Business** tab.
2. Click the **Edit** button for the first MiVoice Business listed.
3. In the **Management Host Name** field, enter the IP Address that is used to access MiVoice Business from the Service Provide network.
4. Click **Save**.
5. If required, configure other MiVoice Business instances.

Step 3 Complete the MiCollab registration:

All tabs except for Platform Details and MiVoice Business are disabled until you enter the Management Host Name in Step 2.

1. Use the tabs to configure Sites, SIP Billing Number, and other platform group settings.
2. Click **Save**.

Reconfigure MiCollab to enable NAT support

If you previously registered MiCollab without NAT support, you can enable it using the following steps.

To reconfigure MiCollab to enable NAT support:

1. Click **Platforms** and then click the **Edit** icon for the MiCollab platform.
2. From the **Platform Details** tab, enable the **Requires Management Host Name Configuration**.

To configure MiVoice Business node with management host name:

1. Select the **MiVoice Business** tab. The MiVoice Business nodes are listed with defaulted “Management Host Name” values. The “Management Host Name” is defaulted to the “Local Host Name” (which is the IP Address/FQDN of the MiVoice Business in the Customer network).
2. Click the **Edit** button on the first MiVoice Business instance. This will bring up a dialog to enter the “Management Host Name”. Remove the defaulted “Management Host Name” IP Address, and enter the IP Address that is used to access the MiVoice Business from the Service Provide network and click Save.
3. Repeat this process as needed for all the listed MiVoice Business instances.

⚠ **Note**
A MiCollab registered with “Requires Management Host Name Configuration” cannot be reconfigured to disable NAT support. This MiCollab needs to be deleted and re-added.

Create Customers

Before you can create a customer, you must have register a platform group for the customer and configure the bundles intended for sale. Once those are in place, you can create the customer from the Customers tab. When creating a customer, make sure you have the first customer user's information, the customer's Calling Party Numbers (CPNs) and, if necessary, the customer's CESIDs.

Ensure that all collected customer and business requirements have been implemented in the portal. Management Portal provides a way for service providers to create MiVoice Business platform groups based on blueprints created with Platform Manager.

⚠ **Note**
If you make a change to the Platform Manager server, for example change the credentials, make sure that you also change them in Management Portal.

To use Platform Manager blueprints in Management Portal, follow these steps:

1. Enable the Platform Manager feature.
2. Register Platform Manager.
3. Register a Platform Manager blueprint.
4. Create platform groups using a Platform Manager blueprint.

⚠ **Note**
Blueprints apply to MiVoice Business type platform groups only.

You must provide the unique URL of the customer portal. If the customer is given full site administration privileges, send the customer the administrator the primary account username and password.

Customer administrator tasks and performance

A customer administrator can carry out simple tasks that do not rely on referenced records while new background tasks are pending (asynchronous). More complex tasks that rely on referenced records (for example general mailboxes) may need to complete before starting new tasks that reference the current background task.

⚠ **Note**
If you choose an extension length of 7 for a customer and then create a bundle with two or more phones, the customer will not be able to create a user with that bundle.

> ⚠ **Note**
> Make sure that you configure the voicemail Hunt Group correctly on the MiVoice Business platform before you create a customer.

To create a customer:

1. From the **Customers** tab, click **View Customers**.
2. Click **Create Customer**.

   > ⚠ If you delete a customer and then recreate it with the same information, you will get an error message when you try to log into the Customer Administrator portal using either the Web ID or through the Service Provider portal. To fix this issue, reboot Management Portal and try to log in again.

3. Enter the following information:

1. **Customer Details**:
   a. Enter customer details.
   b. Select portal branding.
   c. Enter the WebID.
2. **Platform Assignment**:
   a. Select **Platform**.
   b. Select **Extension Length**.
   c. Select dialing privileges.
   d. (optional)Select **Key template**.
   e. (optional)Select **Welcome mail**.
   f. (optional) Select **Customer must confirm any changes that will affect their billing**.
3. **Time Zone**:
   The following fields are applicable for the customers where the version is lesser than MiVoice Business 9.0. If the version is MiVoice Business 9.0 or greater, the SP Admin will set the Time Zone manually in MiVoice Business MSL.
   a. Select **Time Zone**.
   b. Select either **MBG Managed** or **MiVoice Business Managed**.
   c. CPN Substitution:
      Click **Add** and enter the caller ID information that will appear on the called party's phone.
   d. Click **Save**.
4. **Service Bundles**:
   - Enter the quantity of each type of bundle to assign to the customer.
   - Select dialing privileges.
   - (optional): Click the check box to enable Billing Change Notification.
   - **Next Gen Desktop Client** - To enable deployment of the Next Gen Desktop Client. This is enabled by default.
5. **Hotdesk Devices**:
   a. Select one or more hotdesk devices to add as options for this customer.
6. **CPN Substitution**:
   a. Click **Add** and enter the caller ID information that will appear on the called party's phone.
   b. Click **Save**.
7. **Emergency Response Locations**:
   a. Click **Add**.
   b. Enter the emergency site name, number, location, and zone emergency information.
8. **Key Templates**:
   a. Add or remove phone key templates.
9. **DID Ranges**:
   a. Click **+** to add DID ranges or click **–** next to the DID range to delete it.
10. **User Settings**:
    a. Select the Welcome e-mail.
    b. Specify passwords.
    c. Assign a platform to the customer.
    d. Select the extension length for phones.

- Click **Submit**.

To edit a customer:

1. From the **Customers** tab, click **View Customers**.
2. Click a customer that you want to edit.
3. Click the **Edit** icon and select the **User Settings** tab.
4. Make the required changes.

   ⚠ If the portal password is already defined and minimum password length is modified using sysprop command, the portal password has to be adjusted manually, according to the new length. If not, the existing portal password will be used.

5. Click **Save**.

To assign a platform group to a customer:

1. Create a new customer and assign a Platform Group using the Create Customer wizard.
2. Create a new user for the customer and assign a Site using the Create User wizard.

⚠ **Notes**
Management Portal prohibits the creation of duplicate SIP usernames. Do not create users with duplicate SIP user names for multiple customers that share the same MiVoice Border Gateway. You will get an error when you try to create the second one with the same SIP.
When modifying a Customer that requires a connection to the MiCollab Server, and if the connection to the Platform Group fails for any reason and an error message displays or if the rollback fails, carry out the following and re-try the edit operation again:

- Check the network connection.
- Ping the Platform to ensure it is reachable.
- Try editing another Customer (if applicable) to see if the same error occurs. A live network connection is to MiCollab and MiVoice Business is required to create a platform.

Add or remove DID ranges

A Direct Inward Dialing (DID) number is the number dialed from a public network through a trunk line to a site's PBX and then to a user's phone. It provides an individual phone number per person in a company by allowing multiple lines to be connected to the PBX all at once without requiring each to have a physical line connecting to the PBX.

To add DID ranges:

1. From the **Customers** tab, click **View Customers**.
2. Select the customer and click the **Edit** icon.
3. Click the **DID Ranges** tab.
4. Do any of the following:
   a. To add a DID or DID range, enter the Range Start and Range End value and click the **+** sign.
   b. To remove a DID or DID range, enter the Range Start and Range End value and click the **-** sign or click the **X** next to the range you want to remove.
5. Click **Save**.

Map Active Directory Fields for Bulk Import

A Service Provider can now merge an LDIF file into the Management Portal Bulk Import workflow. Active Directory Association uses existing fields in Active Directory (AD) and allows you to re-use them to map to specific fields in the Management Portal Bulk Import or add custom fields into an AD schema.

See also Active Directory Mapping Examples.

Considerations

Keep these points in mind:

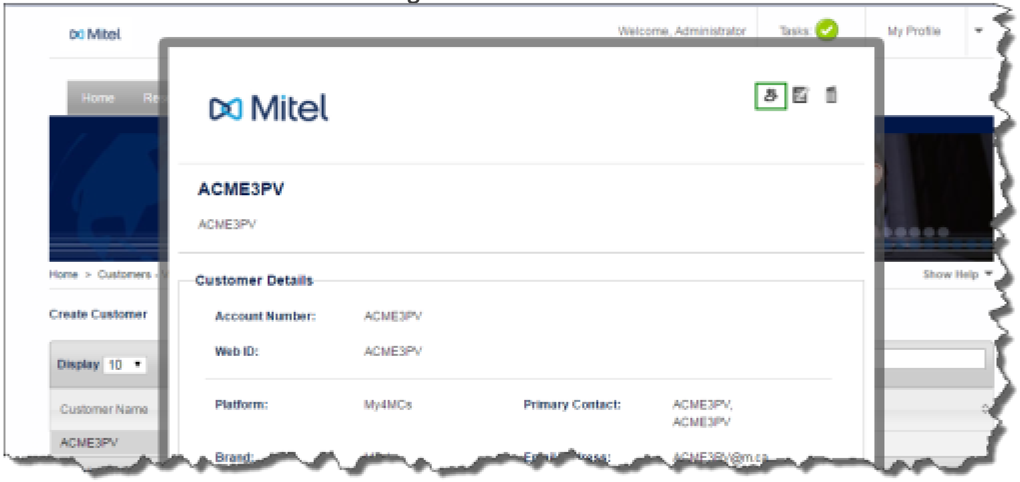
- Active Directory (AD) is accessible only when a Service Provider performs **Log in as Customer**.
- AD imports only LDIF files created from AD.
- Administrators can upload and work with only one LDIF file at a time.
- Administrators must know and understand the attributes in an LDIF file in order to perform the mappings.

Associate AD with the Management Portal Bulk Import

- Step 1: Log in to access Active Directory Association.
- Step 2: Upload the LDIF files (.ldif extension).
- Step 3: Map the fields.
- Step 4: Assign bundles to users.
- Step 5: Download the Bulk Import Spreadsheet.
- Step 6: Import the changes back into the portal.

Step 1 Log in to access Active Directory Association:

1. From the Service Provider Portal, select **Customers > View Customers**.
2. Select the customer and then click the **Login as customer administrator** icon.



ACME3PV

ACME3PV

Customer Details

Account Number: ACME3PV

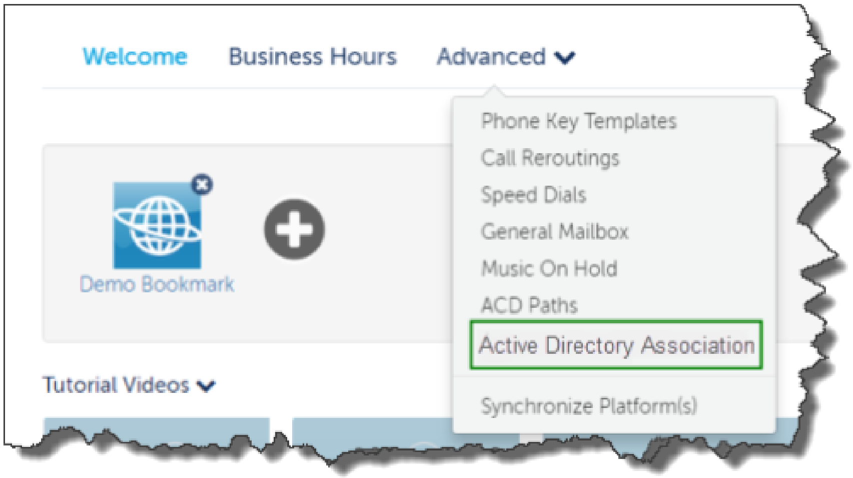
Web ID: ACME3PV

Platform: My4MCs

Primary Contact: ACME3PV, ACME3PV

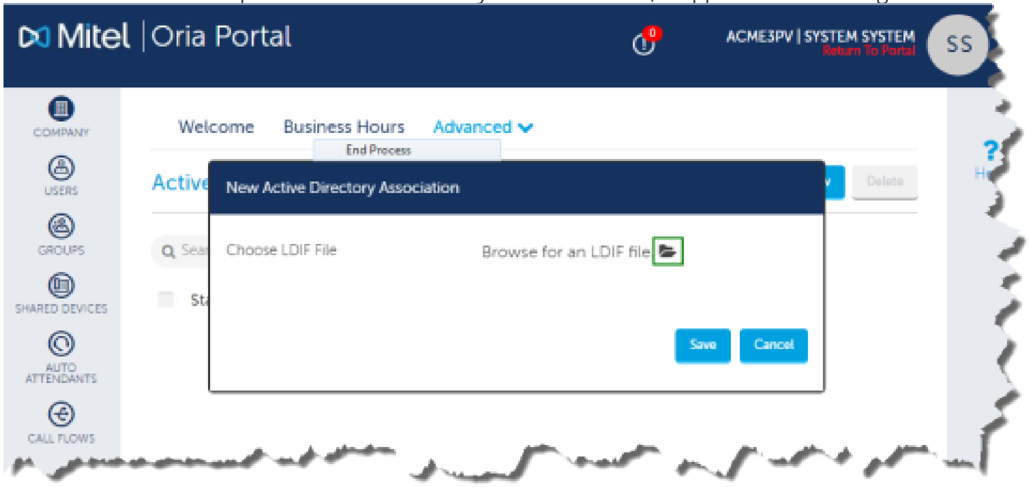
Brand:

3. From the Customer Administrator Portal, select **Advanced > Active Directory Association**.

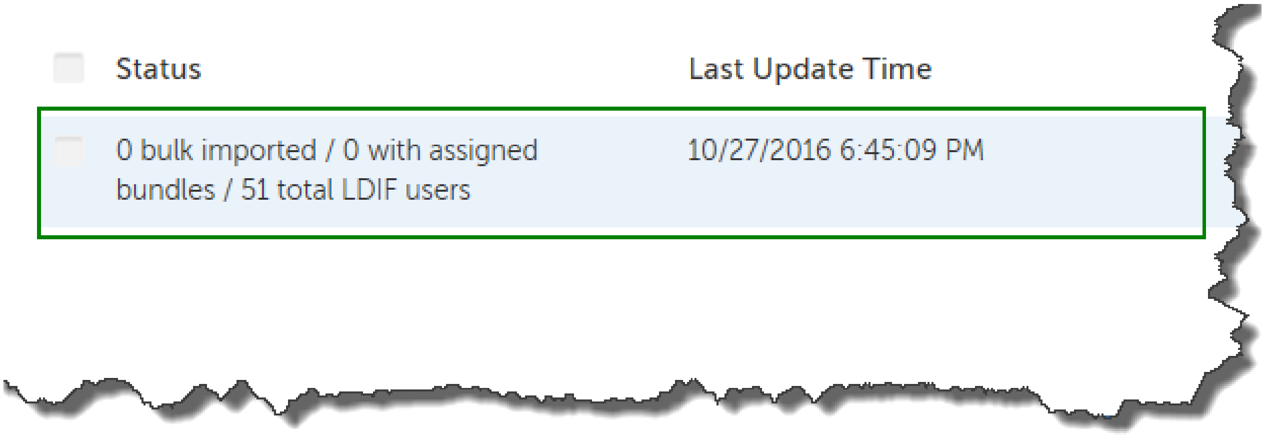


Step 2 Upload the LDIF files:

1. After you select **Active Directory Association**, you are taken to the **Active Directory Association** page.
2. Click **Add New**. The New Active Directory Association upload dialog box appears.
3. Click the folder icon to upload the .ldif file. After you select the file, it appears in the dialog box.



4. Click **Save**.
5. The uploaded file displays the following information:
   a. The number of users that have been bulk imported into Management Portal.
   b. The number of users that have bundles assigned to them.
   c. The total number of users in the .ldif file.



Status	Last Update Time
0 bulk imported / 0 with assigned bundles / 51 total LDIF users	10/27/2016 6:45:09 PM

6. Select and click the file to open it. If you want to delete the uploaded file, select the file and click **Delete**.

Step 3 Map the fields:

Take the following information into consideration before performing the field mappings between Management Portal and AD. To map the Management Portal field names (see below) between AD to Management Portal, the same value must reside on Management Portal. The more fields you can map the less work is needed in the Bulk Import Spreadsheet.

Management Portal Field Names

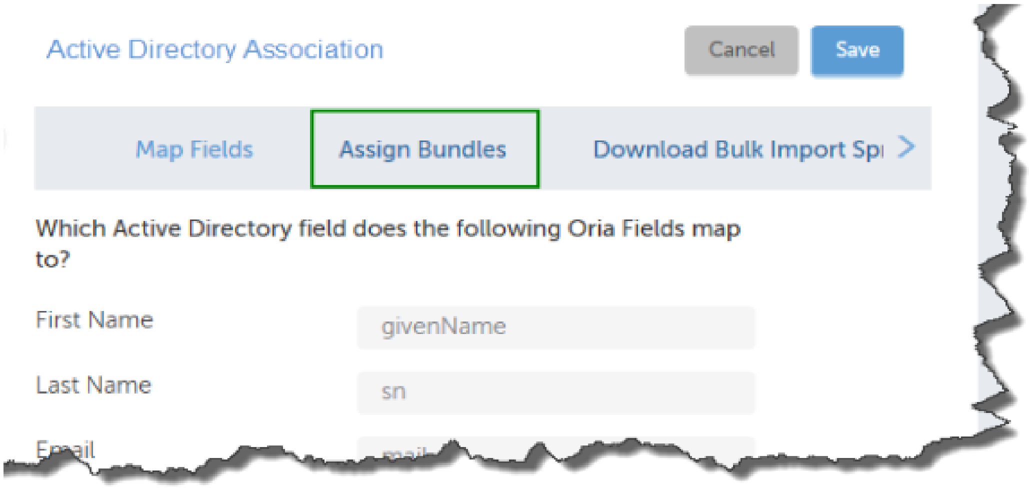
Site	**Dialing Privileges**	**DID**	**Prime Phone CPN**
Prime Phone Key Template	Prime Phone Device Type	Prime Phone Emergency Location	Second Phone Emergency Location
Third Phone Emergency Location	Fourth Phone Emergency Location		

1. After you open the LDIF file, you can perform the mappings.
2. Some default mappings are filled in for you. You can edit these mappings.
3. Enter the **Active Directory** attributes into the empty fields on the right. The attributes you enter in the fields map to the corresponding Management Portal attribute on the left.
4. After all the fields are mapped, click **Save**. All mappings are saved so that you can return to the .ldif file later if needed. Management Portal will take you to the main page in AD. To continue working on the mapping, click the imported LDIF file again.

Step 4 Assign bundles to users:

After you've completed mapping the fields, assign bundles to users.

1. In the **Map Field** form, click the **Assign Bundles** tab. The **Assign Bundles** form displays a **Search** feature and lists all the users in the LDIF file.



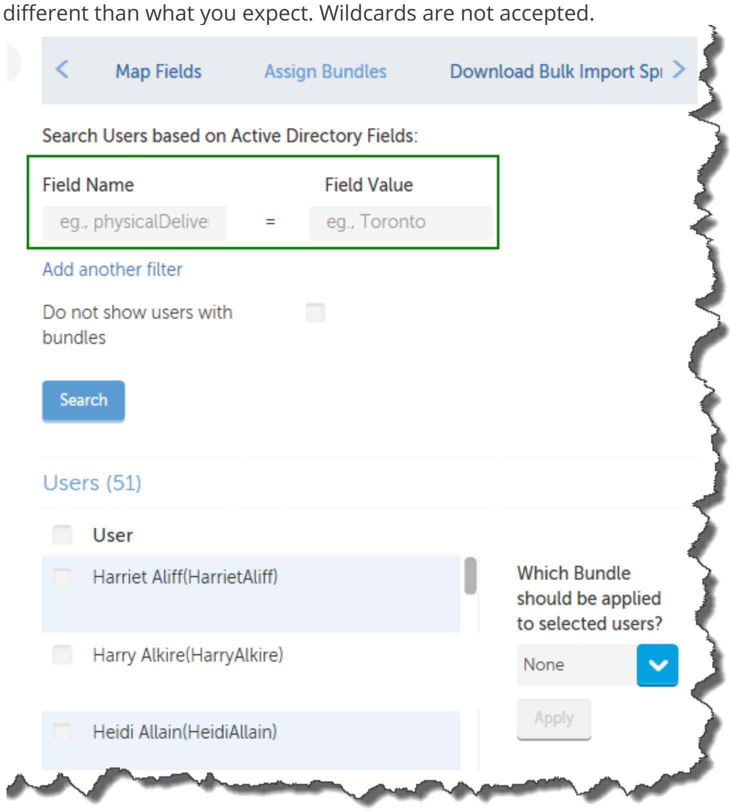
Which Active Directory field does the following Oria Fields map to?

First Name: givenName

Last Name: sn

Email

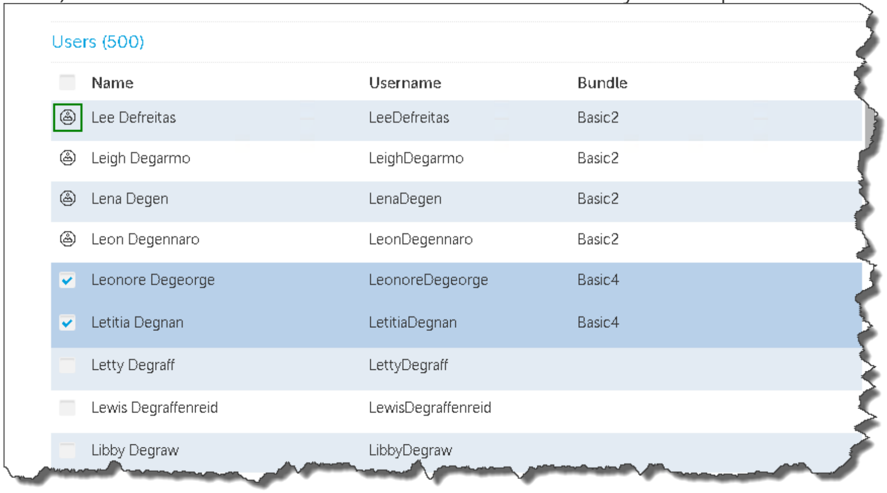
2. To perform a search do the following:
   a. Enter the **Active Directory** attribute in the **Field Name** box. Wild cards are not accepted.
   b. In **Field Value**, enter the criterion to search on. You must enter the values correctly or your search results could be different than what you expect. Wildcards are not accepted.


Map Fields
Assign Bundles
Download Bulk Import Spı
Search Users based on Active Directory Fields:
Field Name
eg., physicalDelive
=
Field Value
eg., Toronto
Add another filter
Do not show users with bundles
Search
Users (51)
User
Harriet Aliff(HarrietAliff)
Harry Alkire(HarryAlkire)
Heidi Allain(HeidiAllain)
Which Bundle should be applied to selected users?
None
Apply

   c. Click **Search**. The user list is updated to matching the search criterion.
   d. To add several search criteria, click **Add another filter**.

e. To remove values to search on, click the **Garbage Can** icon next to Field Value and then click **Search** again. This will update your user list.

3. After you have the list of users, assign a bundle as follows:
   a. Select the users on the list to assign a bundle to. From the drop-down list of bundles, select a bundle. The icon (shown below) beside the user name indicates that the user has already been imported into Management Portal.



Users (500)

☐	Name	Username	Bundle
👤	Lee Defreitas	LeeDefreitas	Basic2
👤	Leigh Degarmo	LeighDegarmo	Basic2
👤	Lena Degen	LenaDegen	Basic2
👤	Leon Degennaro	LeonDegennaro	Basic2
☑	Leonore Degeorge	LeonoreDegeorge	Basic4
☑	Letitia Degnan	LetitiaDegnan	Basic4
☐	Letty Degraff	LettyDegraff	
☐	Lewis Degraffenreid	LewisDegraffenreid	
☐	Libby Degraw	LibbyDegraw	

   b. Click **Apply**. The bundle name appears in the bundle column.
   c. If you want to search for more users to apply a bundle to, but you don't want already assigned users to appear in the list, select **Do not show users with bundles** and click **Search**. This step removes all users from the list that both meet your search criteria and have a bundle already assigned to them.
   d. To remove a bundle from a user, select the user and from the bundle drop-down list, select **None**. This will remove the bundle from the user.
4. After you have assigned bundles to the list of users, click **Save** to save your work and return to the **Active Directory** page, or continue to work on bundle assignment.

Step 5 Download the Bulk Import Spreadsheet:

1. Click **Download Bulk Import Spreadsheet** to download a bulk import Excel spreadsheet.
2. To change any of the bundle assignments, click **Map Fields** or **Assign Bundles** and make the changes.

Step 6 Import the Spreadsheet back into the portal:

After you complete the Bulk Import spreadsheet, return to Service Provider Portal and perform a Bulk Import. See Bulk Import Users for details.

Active Directory Mapping Examples

Here are two examples of AD mapping; Site and Prime Phone Device Type.

Example 1: Mapping a Site

A Service Provider created two sites for a Customer in Management Portal: Ottawa and Nepean.

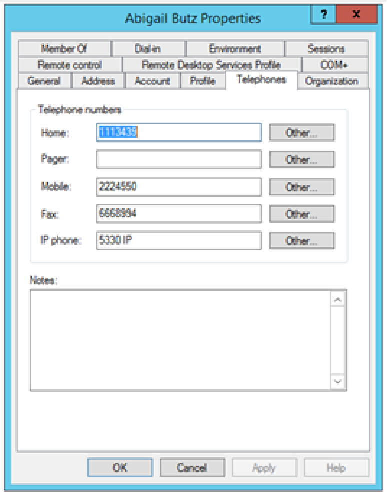
In Active Directory the City location attribute for a user has the same name as the Site name in Management Portal, they are both called Ottawa.

- On the "Map Fields" form the default mapping for "Site" is ''physicalDeliveryOfficeName" attribute in Active Directory.
- If we look at the user's information in Active Directory, the attribute ''physicalDeliveryOfficeName" or Office, is called "Kanata Mitel".

- If you were to keep the current mappings, when you open the “Bulk Import Spread Sheet” the Site location would be empty. This is because Management Portal does not have a Site called “Kanata Mitel”.
- If the current mappings for a filed do not produce the correct output, the field will remain empty in the “Bulk Import Spread Sheet”.
- We need to change the mappings in the Active Directory Association “Map Fields” form.
- Change the “Site” attribute from ‘‘physicalDeliveryOfficeName” to ‘l’ which is the “Active Directory” attribute for “City”.
- This will ensure that all users in “Active Directory” that are in the City of Ottawa or Nepean will be Mapped to the Sites of Ottawa or Nepean in Management Portal.

Example 2: Prime Phone Device Type

- To map a Prime Phone Device Type, the device type in Active Directory must be a Mitel supported device. See Supported Phone Sets for details.
- Active Directory has an attribute called **ipPhone**. The user information below shows that they have an IP phone with a value of 5330 IP. This is a supported Mitel device.



Telephone numbers

Home: 1113439

Pager:

Mobile: 2224550

Fax: 6668994

IP phone: 5330 IP

Notes:

- On the **Map Fields** page, enter the **Active Directory** attribute **ipPhone**.
- When you open the Bulk Import Spreadsheet it will show all of the users that have a supported Mitel device.
- If the device is not a supported device, the field will be empty and you will be required to select one.

Set up MiCollab Clients for multiple tenants

Management Portal allows a Service Provider to set up MiCollab Clients for multiple Customers on the same MiCollab Client server. The Tenants configured in Management Portal on the same MiCollab Client server appear as a unique Enterprises per Tenant.

Terminology: Note that on the MiCollab Client Server, we use the term Enterprises. On Management Portal, we use the term Tenants. When you create users, they are grouped into their corresponding Tenant/Enterprise.

When the platform group is registered with a MiCollab Client Tenant, Management Portal creates an appropriate Enterprise on the MiCollab Client server.

⚠ **Note**
After you configure MiCollab through Management Portal, changes should not be made on the MiCollab Client server; this will cause configuration issues and possible loss of MiCollab Client services.

There are some limitations and restrictions for MiCollab Clients (e.g. Calendar integrations). Refer to the MiCollab Client Administrator Guide and the MiCollab Client Administrator Web Help for more information (go to Document Center).

Synchronize platforms when using MiCollab Multi-Tenant

A new user created in MiVoice Business does not appear in MiCollab until a synchronization between MiCollab Multi-Tenant and MiVB takes place, which by default is every 24 hours. To synchronize platforms at anytime, use the **Synchronize Platforms** button in the Customer Administrator portal:

- Click **Company** and then select **Advanced > Synchronize Platforms**.

Enable MiCollab MiTeam

MiCollab MiTeam is a mobile-first on-demand collaboration tool. It provides a persistent workspace for team collaboration with messaging, content sharing, white boarding, and real-time voice and video meetings, allowing teams to communicate in real time no matter where they are.

MiCollab MiTeam is available with Entry UCC based Service Bundles in the SMB architecture and is available with Premium UCC Service Bundles in the MLB architecture. See Planning Bundles for Customers.

To enable MiCollab MiTeam:

1. Register the platform group.
2. Click the **MiCollab Client Tenant** tab.
3. Select **MiTeam Services**.
4. Click **Save**.

Set the MiCollab MiTeam data center location

You can set the location of the MiCollab MiTeam data center in the Service Provider Portal to support Data Sovereignty requirements. Management Portal with MiCloud Business supports three locations for hosting MiTeam user data; US (default), Europe, and China.

If you have users that reside in both Europe and the US, set the data center location to EU. The laws in the US allow data storage in Europe.

> ⚠ **Note**
> If you upgraded to Management Portal but are using MiCloud Business 3.2 or earlier, the MiTeam data center location is set to US by default and is read-only (grayed out). The data location setting was not available in MiCloud Business 3.2 and earlier or MiCollab versions earlier than 7.3.

To set the MiTeam data center location:

1. Go to **Platforms > Platform Groups**, select the platform group, and then click the **Edit** icon.
2. Click the **MiCollab Client Tenant** tab.
3. From the **MiTeam Data Center Location** list, select the new location.
4. Click **Save**.

Getting started - Set up ACD

Set up Automatic Call Distribution (ACD) to disperse incoming calls to contact center agents or employees who have specific skill sets.

The recommended process for Management Portal Release 6.1 and up is to configure and program ACD paths, RAD greetings, and MOH on Management Portal rather than on the MiVoice Business. You can configure automatic call distribution (ACD) through Management Portal, so it is no longer necessary to program ACD fields directly on the MiVoice Business.

Management Portal reads the ACD Paths and Groups in MiVoice Business platforms created by Management Portal and presents the data in the portal where an administrator can edit it.

> ⚠ It is prudent to assume that Management Portal is the "master," and that the MiVoice Business settings will be overwritten only for RADs and ACD Music On Hold settings you update in Management Portal.

How ACD works with Management Portal

Here is an overview of the ACD items that you should manage from Management Portal and the communications workflow between Management Portal and other systems.

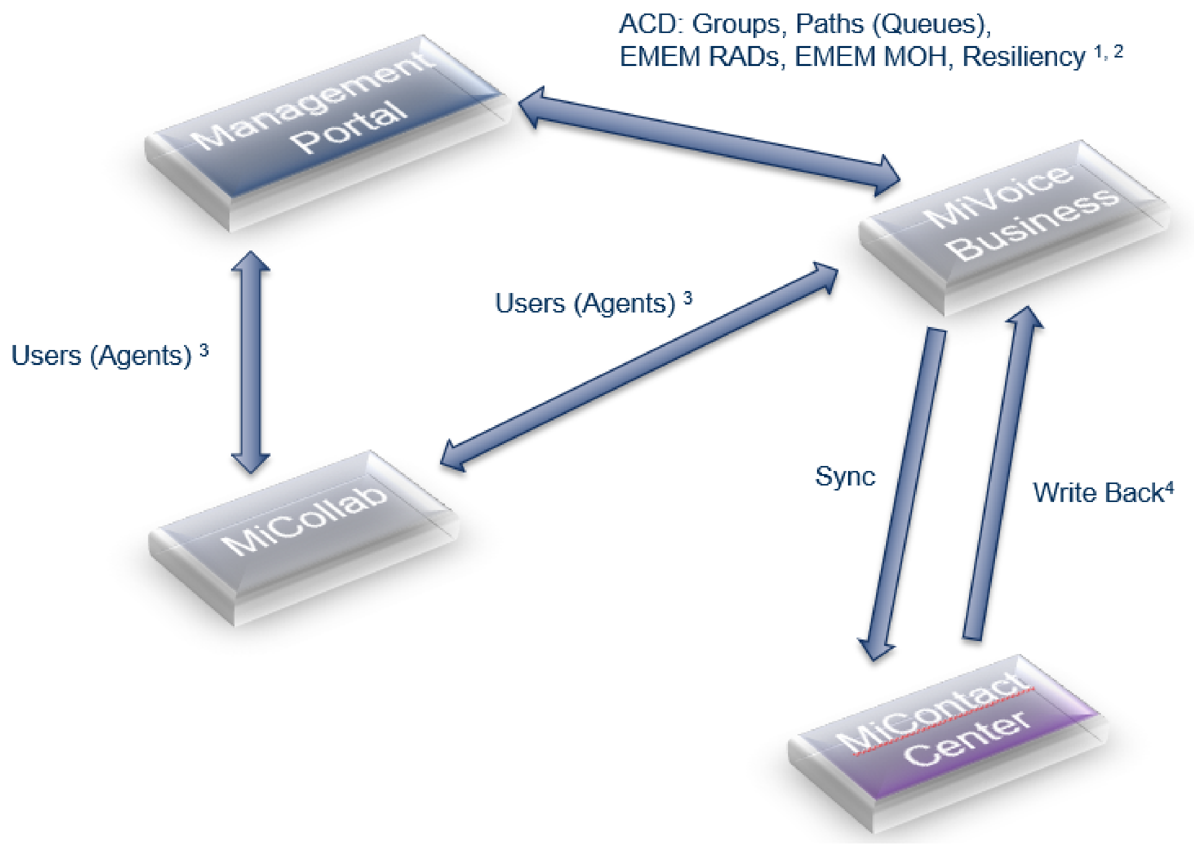
What items should you manage in Management Portal?

- Agents / Users
- ACD Groups
- ACD Paths (Queue)
- ACD Greetings
- ACD Music on Hold
- ACD Resiliency
- Greenfield only (migration of an existing setup is a delete and add of ACD)

Communications flow between Management Portal and other systems

Here are the best practices for communications between Management Portal, MiCollab, MiVoice Business, and MiContact Center.

1. Create groups and paths (queue) from Management Portal. Otherwise, the group or path is not visible in Management Portal.
2. Perform all management activities for EMEM RAD/MOH and ACD resiliency from Management Portal. Otherwise, errors may occur in the automation which Management Portal provides around these features.
3. Create users/agents from Management Portal. Otherwise, the User/Agent becomes an unmanaged user in Management Portal.
4. Management Portal does not support editing the extension number of the User/Agent in a resilient ACD Path.



Considerations

Consider the following notes and recommendations when programming ACD:

- Do not program the resilient MiVoice Business as a primary platform in a second site. Attempting to configure RAD's will cause configuration issues.
- RAD Uploads are only supported with MiVoice Business 8.0 SP3 and up.
- The record a RAD feature does not appear when you have a resilient site.
- Program resilient ACD Greetings and ACD MOH on the same site as the resilient ACD Path that will use them. This will prevent errors later if you decide to change the resilient controller for that site.
- Editing the secondary controller (change or remove) on a site may cause errors related to the ACD path and ACD Greetings on that site. If an error occurs, see the server logs for more information on how to fix the issue.
- Editing ACD Greetings on a site may affect resilient ACD Paths on a different site if they are referencing the ACD Greetings.
- Record a RAD does not appear if you have a resilient site.

Pre-provision resources for ACD and MOH

You must have manually pre-provisioned resources for ACD and MOH in MiVoice Business before you can configure and program ACD and MOH in Management Portal. Here are the pre-provisioning steps required depending on your setup:

ACD greetings and MOH

Go to	Do this
MiVoice Business	1. Program a voicemail hunt group and add appropriate members if you want to use embedded voicemail system (EMEM). Ensure there are enough voicemail ports allocated in the range of voicemail ports for Management Portal to convert to Recorded Announcement Device (RAD) ports. See the *MiVoice Business System Administration Tool Help* for details. 2. Program a COS for a RAD hunt group and a COS for the RAD port. See the *MiVoice Business System Administration Tool Help* for details. 3. Ensure that you remove all existing RAD programming. We recommend that you delete any existing programming and re-program from Management Portal. 4. Ensure there are enough free MOH indices available for Management Portal to use. 5. Enable **SSH** to upload audio files for MiVoice Business 9.0 version and up using SFTP, perform the following steps in MSL: a. Select **Security** > **Remote access**. b. Under **Secure Shell Settings** section, select **Allow access only from trusted and remote management networks** from the **Secure shell access** drop-down list. c. Select **Yes** from **Allow administrative command line access over secure shell** drop-down list. d. Select **Yes** from **Allow secure shell access using standard passwords** drop-down list.
Management Portal	For each MiVoice Business platform, update the ACD Embedded RAD settings in the Management Portal platform group. See Configure RAD source and greetings. • Voicemail hunt group (if applicable) • RAD hunt group number for Management Portal to create and manage • RAD COS • RAD port numbers for Management Portal to manage • RAD port COS • RAD indices available for Management Portal, and the MOH indices for Management Portal to use • Customer Administrator Portal uses SFTP to upload audio files for MiVoice Business 9.0 version and up. To use SFTP, configure the Voice Admin Password in Edit a platform group.

Class of Service

For RAD ports and RAD hunt group COS options below must be set. Same COS can be used for both RAD hunt group and RAD ports.

Example programming:

Recorded Announcement Device - Advanced = Yes

Recorded Announcement Device = Yes

Non-Resilient ACD

Go to	Do this
MiVoice Business	1. Program the necessary trunk controller to route directly to the ACD path. 2. Program the following on the path controller manually: The necessary Zones for the needed time zones for the customer.
Management Portal	In the ACD path page, set the Zone ID for the time zone needed for the path. See Create ACD paths.

Resilient ACD

Go to	Do this
MiVoice Business	1. (optional) Program a secondary trunk controller. 2. Route the trunk to the Trunk Route Directory Number on the path controllers. **Note**: You must first determine this number from the customer. 3. Program the following on the primary path controller manually: • Set the general mailbox if voicemail is used in the path. See more information and an example here: General mailbox • Configure the necessary zones for the needed time zones for the customer.

Go to	Do this
Management Portal	In the ACD Path page, program the following settings: • Directory number of the ACD queue. • Zone ID for the time zone needed for the path. • Voicemail mailbox number that represents the general mailbox if voicemail is used in the path. **Note**: The voicemail mailbox is automatically managed by Management Portal in the non-resilient case.

General mailbox

- The MiVoice Business platform does not natively support resilient ACD paths. The calling number which lands on a path is not consistent when the call lands on the Secondary compared with the Primary Path Controller.
- To work around the issue, a named tag hunt group is used to provide a consistent calling number to land on a single mailbox independent if the call came through the Primary or Secondary Path Controller.

Example programming:

- Create a mailbox in EMEM with mailbox number 4000 on both the Primary and Secondary Path Controller
- Create a resilient Name Tag Hunt Group = 3000
- Set the Name Tag= 4000
- Create a member 3001 (MWI for the mailbox will be assigned to the first member of the group)
- Use hunt group 3000 as the answer point in the ACD path for mailbox 4000.
- Set MWI keys to monitor extension 3001 for the MWI for mailbox 4000.

Provision ACD

Here are the provisioning steps required for ACD and MOH:

Initial provisioning workflow for ACD programming without resiliency

Go to	Do this
MiVoice Business	Ensure that you have completed the manual steps in the platform setup section for a non-resilient ACD system. See Non-resilent ACD.

Go to	Do this
Management Portal	1. Ensure that the platform group is up-to-date. 2. Program the EMEM RAD (if required). See Program ACD greetings. 3. Program MOH (if required). See Program ACD Music on Hold. 4. Create agents (users). Skip this step if you are importing users with the bulk import feature in Management Portal. See Add, edit, and remove agents. 5. Create an ACD group. See Add, edit, and remove groups. 6. Program the ACD path (Queue). See Add, edit, and remove paths.
MiContact Center	1. Configure YourSite Explorer (YSE) to sync with the MiVoice Business platform. See MiContact Center Business - MiVoice Business Installation and Administrator Guide. 2. Complete initial provisioning of YSE according to best practices. **Note:** Enable read/write in YSE.

Initial provisioning workflow for ACD programming with resiliency

Go to	Do this
MiVoice Business	Ensure that you have completed the manual steps in the platform setup section for a resilient ACD system. See Resilient ACD.

Go to	Do this
Management Portal	1. Ensure that the platform group is up-to-date. 2. Ensure you are following the ACD resiliency instructions. 3. Program EMEM RAD (if required). See Configure ACD RAD and Music on Hold resiliency. 4. Program MOH (if required). See Configure ACD RAD and Music on Hold resiliency. 5. Create agents or users (skip if this is done via bulk import). See Add, modify, and delete users. 6. Create the ACD group. See Add, edit, and remove groups. 7. Program the ACD path (Queue). See Add, edit, and remove paths.
MiContact Center	1. Configure YSE to sync with MiVoice Business. See MiContact Center Business - MiVoice Business Installation and Administrator Guide. 2. Complete initial provisioning of YSE as per best practices. **Note**: Enable read/write in YSE. Write back is not supported on the resilient ACD path programming

Add, edit, and remove agents

Add an agent from Management Portal

Go to	Do this
Management Portal	1. Ensure the preconditions on Management Portal have been met for ACD agent. 2. In the Customer Administrator portal, create an Agent/User with ACD bundle. See Add, modify, and delete users.

Go to	Do this
MiContact Center	Open YourSiteExplorer (YSE) and perform a Synchronization. See MiContact Center Business - MiVoice Business Installation and Administrator Guide.

Edit an agent from YSE

Go to	Do this
MiContact Center	In YSE, edit the ACD agent in the **Agent** tab. **Caveat**: The YSE application does not support write back of DN changes.
Management Portal	Verify that the changes are automatically synchronized back to Management Portal.

Remove an agent from Management Portal

Go to	Do this
Management Portal	In the Customer Administrator portal, remove the ACD agent from the group. See Add, modify, and delete users.
MiContact Center	Open YSE and perform a Synchronization or wait for the sync to execute during the nightly maintenance. See MiContact Center Business - MiVoice Business Installation and Administrator Guide.

Edit an agent from Management Portal

Go to	Do this
Management Portal	Edit the properties of the agent or user from the Customer Administrator portal. See Add, modify, and delete users.

Go to	Do this
MiContact Center	Open YSE and perform a Synchronization. See MiContact Center Business - MiVoice Business Installation and Administrator Guide.

Add, edit, and remove groups

Add an agent group from Management Portal

Go to	Do this
Management Portal	Create an ACD agent group from the Customer Administrator portal. See Create ACD groups.
MiContact Center	Open YSE and perform a Synchronization.

Edit a group from Management Portal

Go to	Do this
Management Portal	Edit the properties of the ACD group from the Customer Administrator portal. ⚠ When the Administrator adds one or more ACD Agent in the ACD Group from MiVoice Business, it is mandatory to perform To edit an ACD group procedure in the Customer Administrator Portal.
MiContact Center	Open YourSiteExplorer application and perform a Synchronization.

Edit a group from YSE (writeback)

Go to	Do this
MiContact Center	Open YSE and edit an Agent group. See MiContact Center Business - MiVoice Business Installation and Administrator Guide.

Go to	Do this
Management Portal	Verify that changes are automatically synchronized back to Management Portal.

Remove a group from Management Portal

Go to	Do this
Management Portal	1. Remove the group from ACD Path (if programmed). 2. Delete the agent group from the Customer Administrator portal. See Create ACD groups.
MiContact Center	Open YSE and perform a Synchronization. See MiContact Center Business - MiVoice Business Installation and Administrator Guide.

Add, edit, and remove paths

Add a path from Management Portal

Go to	Do this
Management Portal	Create an path in the Customer Administrator portal. See Create ACD paths.
MiContact Center	Open YourSiteExplorer application and perform a Synchronization. See MiContact Center Business - MiVoice Business Installation and Administrator Guide.

Edit a path from Management Portal

Go to	Do this
Management Portal	In the Customer Administrator portal, modify your ACD Paths with or without resiliency.

Go to	Do this
MiContact Center	Open YSE and perform a Synchronization. See MiContact Center Business - MiVoice Business Installation and Administrator Guide. **Caveat**: Because ACD Path resiliency is managed by Management Portal, we do not recommend the use of YSE writeback to the ACD Paths.

Remove a path from Management Portal

Go to	Do this
Management Portal	Remove the path from the Management Portal Customer Administrator portal. See Create ACD paths.
MiContact Center	Open YSE application and perform a Synchronization. See MiContact Center Business - MiVoice Business Installation and Administrator Guide.

Assign Customer Admin Features for ACD

When creating Customer administrators, you can decide what privileges they will have. You do this on the **Select Features** page.

⚠ Service Provider Portal Admins automatically have access to the **Advanced ACD Groups**, **Advanced ACD Paths**, **RAD Programming**, and **ACD Music On Hold** features; that is, they have all of the privileges associated with these features.

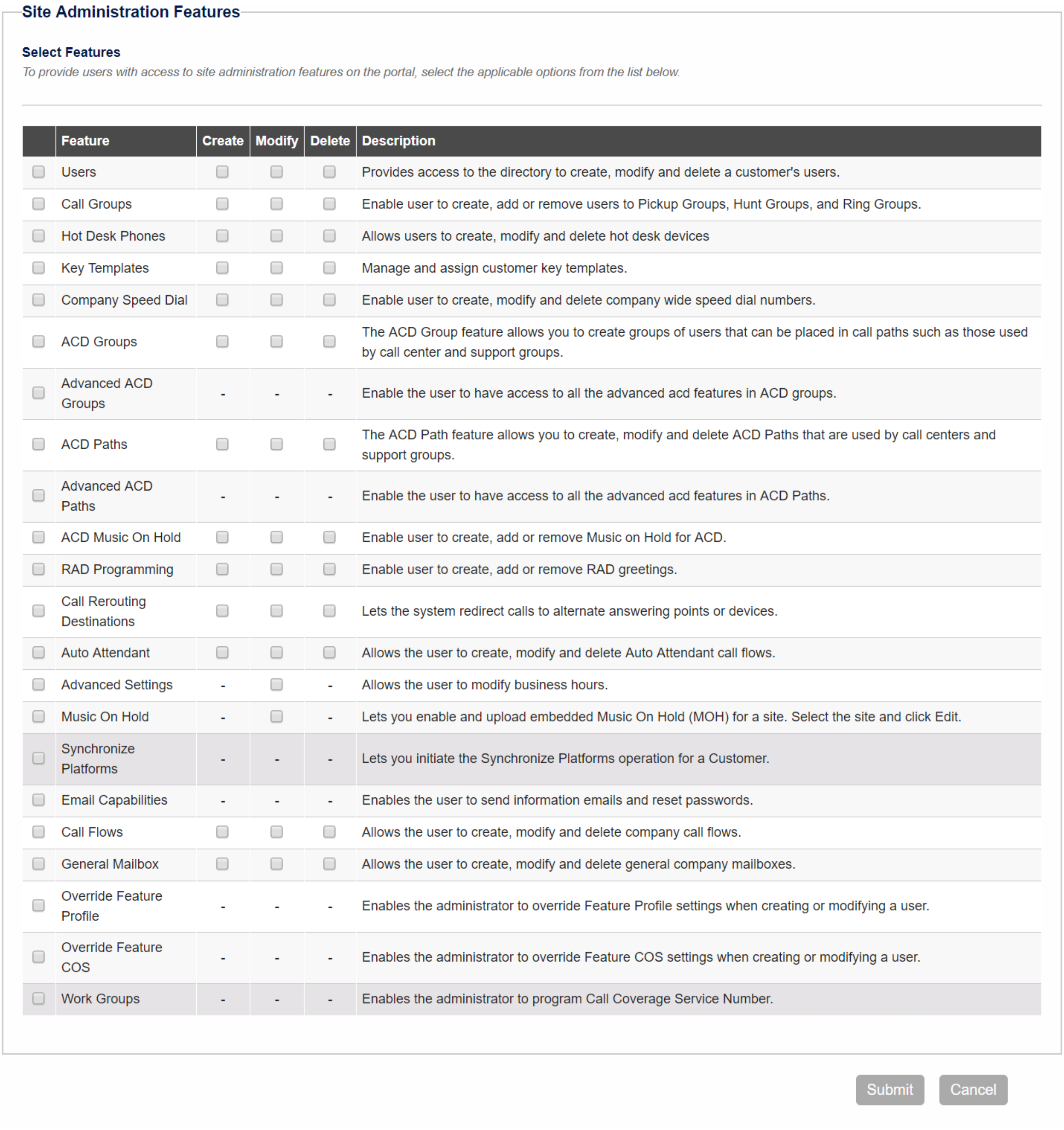
The ACD features have changed for Management Portal 6.1. The Management Portal 6.0 ACD feature is now broken down as follows:

- **ACD Groups**: A part of the old ACD feature.
- **Advanced ACD Groups**: Gives access to the new advanced ACD Groups features. If this feature is selected, the Admin also has the **ACD Groups** feature, by default.
- **ACD Paths**: A part of the old ACD feature.
- **Advanced ACD Paths**: Gives access to the new advanced ACD Paths features. If this feature is selected, the Admin also has the **ACD Paths** feature, by default.
- **ACD Music On Hold:** Gives access to the new ACD Music On Hold features.
- **RAD Programming**: Allows the Admin to create, modify, and delete RAD messages.

⚠ RAD programming and ACD Music On Hold is supported on SB and MLB customer platforms.
RAD Programming and ACD Music On Hold is not supported on SMB customer platforms.

For a list of the Basic and Advanced fields and their naming in Management Portal, see Basic and Advanced Admin Features for ACD.

⚠ The Management Portal 6.0 MOH feature is used for System Music on Hold only. Management Portal 6.1 now also supports ACD Music on Hold.



Site Administration 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
□	Users	□	□	□	Provides access to the directory to create, modify and delete a customer's users.
□	Call Groups	□	□	□	Enable user to create, add or remove users to Pickup Groups, Hunt Groups, and Ring Groups.
□	Hot Desk Phones	□	□	□	Allows users to create, modify and delete hot desk devices
□	Key Templates	□	□	□	Manage and assign customer key templates.
□	Company Speed Dial	□	□	□	Enable user to create, modify and delete company wide speed dial numbers.
□	ACD Groups	□	□	□	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.
□	Advanced ACD Groups	-	-	-	Enable the user to have access to all the advanced acd features in ACD groups.
□	ACD Paths	□	□	□	The ACD Path feature allows you to create, modify and delete ACD Paths that are used by call centers and support groups.
□	Advanced ACD Paths	-	-	-	Enable the user to have access to all the advanced acd features in ACD Paths.
□	ACD Music On Hold	□	□	□	Enable user to create, add or remove Music on Hold for ACD.
□	RAD Programming	□	□	□	Enable user to create, add or remove RAD greetings.
□	Call Rerouting Destinations	□	□	□	Lets the system redirect calls to alternate answering points or devices.
□	Auto Attendant	□	□	□	Allows the user to create, modify and delete Auto Attendant call flows.
□	Advanced Settings	-	□	-	Allows the user to modify business hours.
□	Music On Hold	-	□	-	Lets you enable and upload embedded Music On Hold (MOH) for a site. Select the site and click Edit.
□	Synchronize Platforms	-	-	-	Lets you initiate the Synchronize Platforms operation for a Customer.
□	Email Capabilities	-	-	-	Enables the user to send information emails and reset passwords.
□	Call Flows	□	□	□	Allows the user to create, modify and delete company call flows.
□	General Mailbox	□	□	□	Allows the user to create, modify and delete general company mailboxes.
□	Override Feature Profile	-	-	-	Enables the administrator to override Feature Profile settings when creating or modifying a user.
□	Override Feature COS	-	-	-	Enables the administrator to override Feature COS settings when creating or modifying a user.
□	Work Groups	-	-	-	Enables the administrator to program Call Coverage Service Number.

Bundle changes after upgrading

Admin Bundles with ACD automatically get basic ACD Groups and basic ACD Paths when upgrading to Management Portal 6.1.

Upon upgrade, the ACD features assigned to Customer Admin Bundles change as follows:

- **ACD Groups:** If the bundle already had **ACD**, then it will automatically have **ACD Groups** after upgrade.
- **Advanced ACD Groups:** For existing Customer Admin bundles, this feature is not turned on by default.
- **ACD Paths:** If the bundle already had **ACD**, then it will automatically have **ACD Paths** after upgrade.
- **Advanced ACD Paths:** For existing Customer Admin bundles, this feature is not turned on by default.
- **ACD Music On Hold:** For existing Customer Admin bundles, this feature is not turned on by default.
- **RAD Programming:** For existing Customer Admin bundles, this feature is not turned on by default.

For the upgrade from pre-6.1 to Management Portal 6.1, the new features remains un-selected for existing Customer Admin Bundles. To give these advanced permissions to Customer Admins, change the Bundle to grant all admins with that bundle Advanced ACD, RAD programming and/or ACD Music On Hold privileges.

Basic and Advanced Admin Features for ACD

You can specify which fields should be available to the untrained Customer Admin (meaning the admin that has the **ACD Groups** and/or the **ACD Paths** privileges in their Admin Bundle). The intent of this field is to add a few fields (like some of the timer fields) to the list of fields the untrained admin can access. For Customer Admins who are trained and capable of programming their own ACD functionality, you can give them **Advanced ACD Groups** and **Advanced ACD Paths** privileges so they can have access to all of the ACD Groups and ACD Paths fields.

The following tables show the ACD Group and Path fields, and whether they are in the Basic or Advanced feature set.

Some of the field names have been simplified, compared to the MiVoice Business System Administration Tool names. The Management Portal names are also shown, if they are different.

Field	Can configure?	Advanced/ Basic	Simplified Field Name
Name	No	Basic	Same as in MiVoice Business UI
DN	No	Basic	Same as in MiVoice Business UI
Prime/ Secondary MCD (Site)	No	Basic	Same as in MiVoice Business UI
Reporting Number	No	Basic	Same as in MiVoice Business UI
Local Only DN	Yes	Advanced	Local-only
Group Members	No	Basic	Same as in MiVoice Business UI
Group Member skill level	Yes	Basic	Skill Level
First Status Threshold time (mm:ss)	Yes	Advanced	Same as in MiVoice Business UI
Second Status Threshold time (mm:ss)	Yes	Advanced	Same as in MiVoice Business UI
Alert Device	Yes	Advanced	Same as in MiVoice Business UI
Group Real Time Events Enabled	Yes	Advanced	Group Real Time Events Enabled
Queue Callers To Group When No Local Agents are logged in and present	Yes	Advanced	Same as in MiVoice Business UI
Group uses skill level	Yes	Advanced	Same as in MiVoice Business UI

Field	Can configure?	Advanced/Basic	Simplified Field Name
Name	No	Basic	Same as in MiVoice Business UI
Prime MiVB (Site)	No	Basic	Same as in MiVoice Business UI
DID(s)	No	Basic	Same as in MiVoice Business UI
DN	No	Basic	Same as in MiVoice Business UI
Reporting Number	No	Basic	Same as in MiVoice Business UI
VM mailbox passcode	No	Basic	Same as in MiVoice Business UI

Field	Can configure?	Advanced/Basic	Simplified Field Name
VM send to email	No	Basic	Same as in MiVoice Business UI
VM to email address	No	Basic	Same as in MiVoice Business UI
Prime skill group	No	Basic	Same as in MiVoice Business UI
Overflow 1 group	No	Basic	Same as in MiVoice Business UI
Overflow 2 group	No	Basic	Same as in MiVoice Business UI
Overflow 3 group	No	Basic	Same as in MiVoice Business UI
Local-only DN	Yes	Advanced	Local-only
Class of Service Day	Yes	Advanced	Class of Service - Day
Class of Service Night 1	Yes	Advanced	Class of Service - Night1
Class of Service Night 2	Yes	Advanced	Class of Service - Night2
Recording 1: Delay to Start Time Minutes/Seconds	Yes	Advanced	Greeting 1 Answer Time
Recording 1: Directory Number	Yes	Advanced	Greeting 1
Recording 1: Embedded Music Source	Yes	Advanced	Music On Hold 1
Recording 1: Alternative Recording Device	Yes	Advanced	Alt Recording Device 1
Recording 1: Path Interflow Dialing List	Yes	Advanced	Greeting 1 Option List
Recording 1: Release Digit Receiver After Recording	Yes	Advanced	Option choice during greeting only
Recording 2: Delay to Start Time Minutes/Seconds	Yes	Advanced	Greeting 2 Answer Time
Recording 2: Directory Number	Yes	Advanced	Greeting 2
Recording 2: Embedded Music Source	Yes	Advanced	Music On Hold 2
Recording 2: Alternative Recording Device	Yes	Advanced	Alt Recording Device 2
Recording 2: Path Interflow Dialing List	Yes	Advanced	Greeting 2 Option List
Recording 2: Release Digit Receiver After Recording	Yes	Advanced	Option choice during greeting only
Recording 3: Delay to Start Time Minutes/Seconds	Yes	Advanced	Greeting 3 Answer Time
Recording 3: Directory Number	Yes	Advanced	Greeting 3
Recording 3: Embedded Music SourceYes	Yes	Advanced	Music On Hold 3
Recording 3: Alternative Recording Device	Yes	Advanced	Alt Recording Device 3

Field	Can configure?	Advanced/Basic	Simplified Field Name
Recording 3: Path Interflow Dialing List	Yes	Advanced	Greeting 3 Option List
Recording 3: Release Digit Receiver After Recording	Yes	Advanced	Option choice during greeting only
Recording 4: Delay to Start Time Minutes/Seconds	Yes	Advanced	Greeting 4 Answer Time
Recording 4: Directory Number	Yes	Advanced	Greeting 4
Recording 4: Embedded Music Source	Yes	Advanced	Music On Hold 4
Recording 4: Alternative Recording Device	Yes	Advanced	Alt Recording Device 4
Recording 4: Path Interflow Dialing List	Yes	Advanced	Greeting 4 Option List
Recording 4: Release Digit Receiver After Recording	Yes	Advanced	Option choice during greeting only
Repeat Last Recording Enabled	Yes	Advanced	Repeat last greeting
Last Recording Repeat Interval Minutes/Seconds	Yes	Advanced	Repeat last greeting time
Interflow Enabled	Yes	Advanced	Interflow Enabled
Interflow Time Out Minutes/Seconds	Yes	Advanced	No Answer Timer
Interflow Point Directory	Yes	Advanced	No Answer Destination
Allow Overflow to Interflow Before Time Out	Yes	Advanced	Allow Overflow to Interflow Before Time Out
Path Real Time Events Enabled	Yes	Advanced	Path Real Time Events Enabled
Path Unavailable Answer Point Directory Number	Yes	Advanced	Queue Unavaliable Destination
Interflow To This Path Uses This Path Priority	Yes	Advanced	Interflow To This Path Uses This Path Priority
DTMF Receiver Unavailable Action Play RAD Skip Divert	Yes	Advanced	DTMF Receiver Unavailable Action Play RAD
DTMF Receiver Unavailable Answer Point Directory Number	Yes	Advanced	DTMF Receiver Unavailable Answer Point Directory Number
Primary Agent Skill Group Overflow Timer Minutes/ Seconds	Yes	Advanced	Primary Agent Skill Group Overflow Timer
Primary Agent Skill Group Predictive Overflow Average Call Duration Minutes/Seconds	Yes	Advanced	Primary Agent Skill Group Predictive Overflow Average Call Duration
Primary Agent Skill Group Remote Agent Skill Group Priority	Yes	Advanced	Primary Agent Skill Group Remote Agent Skill Group Priority

Field	Can configure?	Advanced/Basic	Simplified Field Name
Primary Agent Skill Group Remote Agent Blocking Timer	Yes	Advanced	Primary Agent Skill Group Remote Agent Blocking Timer
Overflow 1 Agent Skill Group Overflow Timer Minutes/ Seconds	Yes	Advanced	Overflow 1 Agent Skill Group Overflow Timer
Overflow 1 Agent Skill Group Predictive Overflow Average Call Duration Minutes/Seconds	Yes	Advanced	Overflow 1 Agent Skill Group Predictive Overflow Average Call Duration
Overflow 1 Agent Skill Group Remote Agent Skill Group Priority	Yes	Advanced	Overflow 1 Agent Skill Group Remote Agent Skill Group Priority
Overflow 1 Agent Skill Group Remote Agent Blocking Timer	Yes	Advanced	Overflow 1 Agent Skill Group Remote Agent Blocking Timer
Overflow 2 Agent Skill Group Overflow Timer Minutes/ Seconds	Yes	Advanced	Overflow 2 Agent Skill Group Overflow Timer
Overflow 2 Agent Skill Group Predictive Overflow Average Call Duration Minutes/Seconds	Yes	Advanced	Overflow 2 Agent Skill Group Predictive Overflow Average Call Duration
Overflow 2 Agent Skill Group Remote Agent Skill Group Priority	Yes	Advanced	Overflow 2 Agent Skill Group Remote Agent Skill Group Priority
Overflow 2 Agent Skill Group Remote Agent Blocking Timer	Yes	Advanced	Overflow 2 Agent Skill Group Remote Agent Blocking Timer
Overflow 3 Agent Skill Group Overflow Timer Minutes/ Seconds	Yes	Advanced	Overflow 3 Agent Skill Group Overflow Timer
Overflow 3 Agent Skill Group Predictive Overflow Average Call Duration Minutes/Seconds	Yes	Advanced	Overflow 3 Agent Skill Group Predictive Overflow Average Call Duration
Overflow 3 Agent Skill Group Remote Agent Skill Group Priority	Yes	Advanced	Overflow 3 Agent Skill Group Remote Agent Skill Group Priority
Overflow 3 Agent Skill Group Remote Agent Blocking Timer	Yes	Advanced	Overflow 3 Agent Skill Group Remote Agent Blocking Timer

Configure ACD

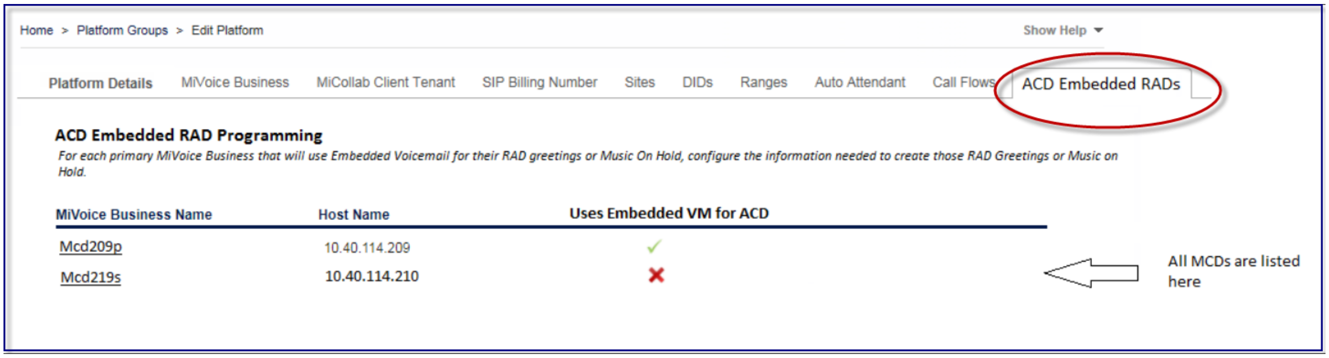
Here are the steps to configure ACD in Management Portal:

Configure RAD source and greetings

There are many possible RAD sources, including MiContact Center and NuPoint Messenger. Management Portal supports EMEM RAD programming as long as EMEM is installed on the MiVoice Business platform.

The **ACD Embedded RADs** tab in **Edit Platform** allows Service Provider to setup the resources to be used when programming RADs from the CA Portal.

ACD Embedded RADs tab is not displayed if the platform type is MiVoice Business Express.

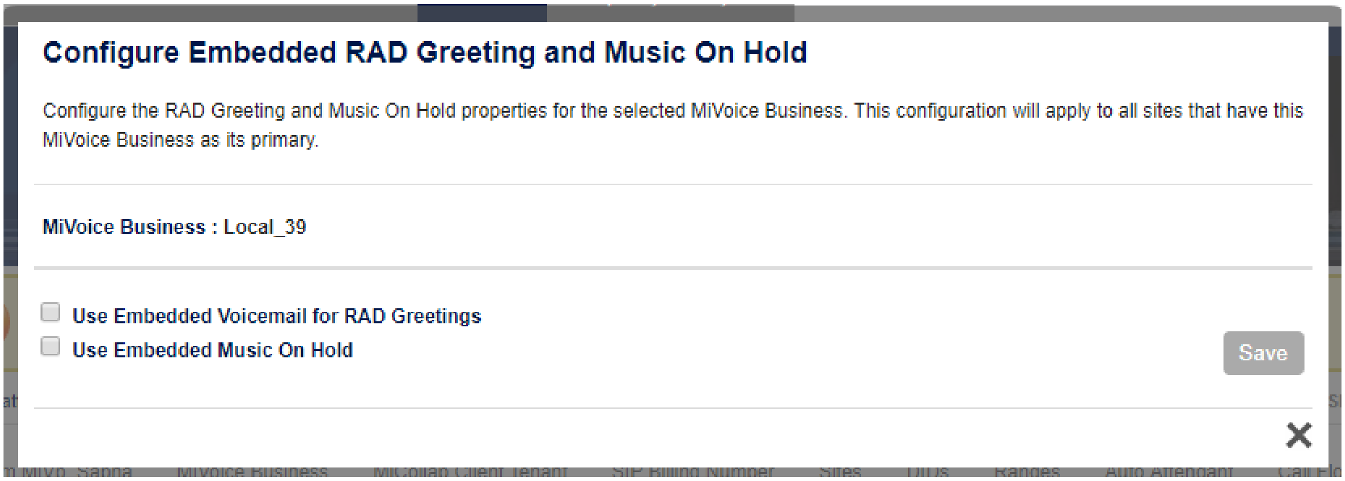


ACD Embedded RAD Programming

For each primary MiVoice Business that will use Embedded Voicemail for their RAD greetings or Music On Hold, configure the information needed to create those RAD Greetings or Music on Hold.

MiVoice Business Name	Host Name	Uses Embedded VM for ACD
Mcd209p	10.40.114.209	✓
Mcd219s	10.40.114.210	✗

Click the MiVoice Business instance to program the **Embedded RAD** and **Music on Hold**. The following dialog box appears for configuration of the Embedded Voicemail. By default, no check-boxes are selected, and all fields are hidden.



Configure Embedded RAD Greeting and Music On Hold

Configure the RAD Greeting and Music On Hold properties for the selected MiVoice Business. This configuration will apply to all sites that have this MiVoice Business as its primary.

MiVoice Business : Local_39

□ Use Embedded Voicemail for RAD Greetings

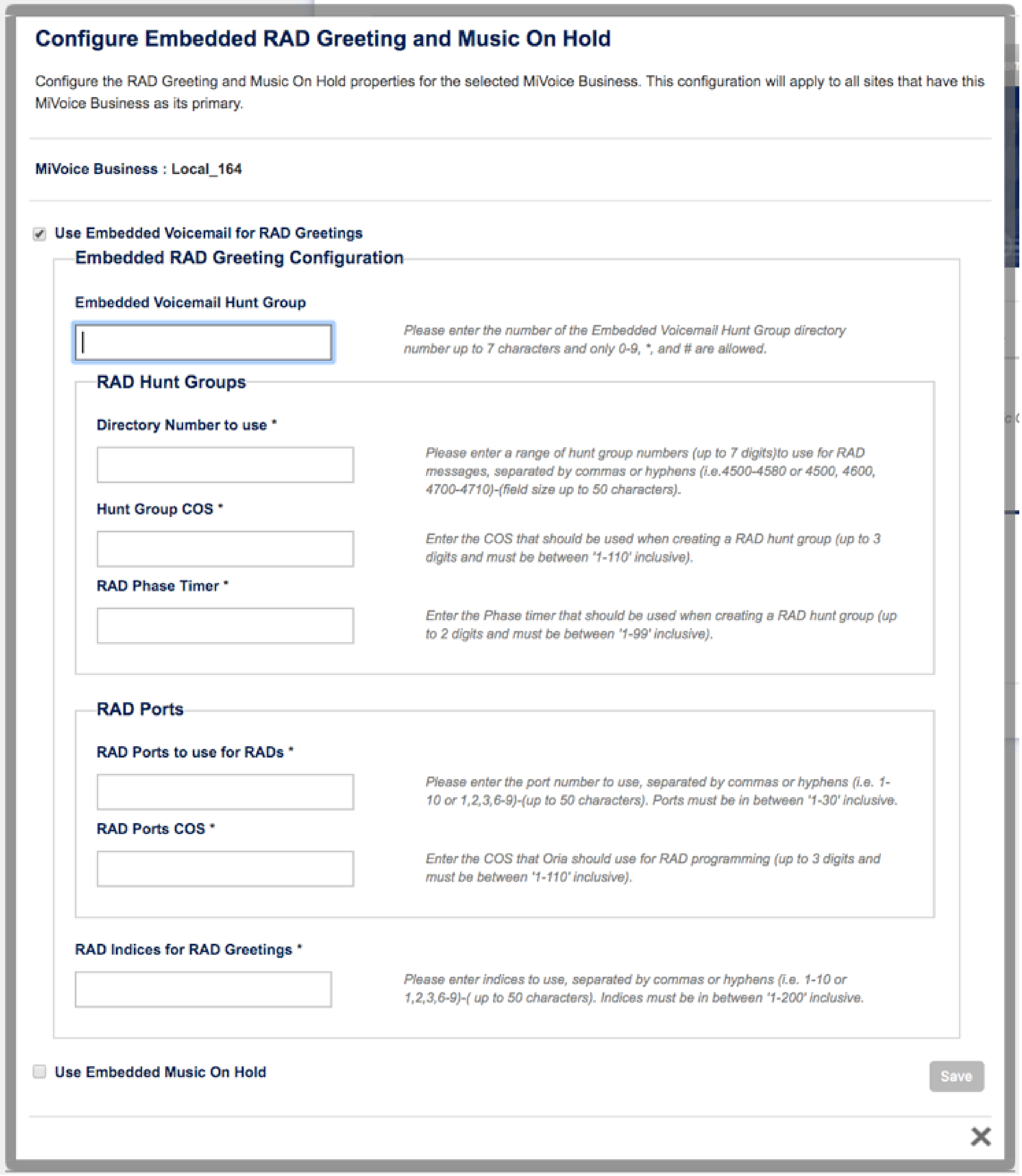
□ Use Embedded Music On Hold

The Customer Admin Portal does not use the term "RAD". Instead, Customer Admins see "Greetings".

After you select a checkbox, the fields are displayed for that item. Note that the fields marked with * are mandatory.

Caution
When you configure sites that share MiVoice Business platforms, be careful that MOH settings do not overlap. For example, if some of the MOH settings are used for both the primary and secondary MiVoice Business platforms, there is a chance that they will both use the same settings causing one to override the other.

Customer Administrator Portal uses SFTP to upload audio files for MiVoice Business 9.0 version and up. To use SFTP, configure the Voice Admin Password in Edit a Platform Group.



Configure Embedded RAD Greeting and Music On Hold

Configure the RAD Greeting and Music On Hold properties for the selected MiVoice Business. This configuration will apply to all sites that have this MiVoice Business as its primary.

MiVoice Business : Local_164

☑ **Use Embedded Voicemail for RAD Greetings**

Embedded RAD Greeting Configuration

Embedded Voicemail Hunt Group

*Please enter the number of the Embedded Voicemail Hunt Group directory number up to 7 characters and only 0-9, *, and # are allowed.*

RAD Hunt Groups

Directory Number to use *

Please enter a range of hunt group numbers (up to 7 digits)to use for RAD messages, separated by commas or hyphens (i.e.4500-4580 or 4500, 4600, 4700-4710)-(field size up to 50 characters).

Hunt Group COS *

Enter the COS that should be used when creating a RAD hunt group (up to 3 digits and must be between '1-110' inclusive).

RAD Phase Timer *

Enter the Phase timer that should be used when creating a RAD hunt group (up to 2 digits and must be between '1-99' inclusive).

RAD Ports

RAD Ports to use for RADs *

Please enter the port number to use, separated by commas or hyphens (i.e. 1-10 or 1,2,3,6-9)-(up to 50 characters). Ports must be in between '1-30' inclusive.

RAD Ports COS *

Enter the COS that Oria should use for RAD programming (up to 3 digits and must be between '1-110' inclusive).

RAD Indices for RAD Greetings *

Please enter indices to use, separated by commas or hyphens (i.e. 1-10 or 1,2,3,6-9)-(up to 50 characters). Indices must be in between '1-200' inclusive.

□ **Use Embedded Music On Hold**

- **Embedded Voicemail Hunt Group**: (optional) If it is left blank, the RAD port DN used for a RAD greeting will not be removed from any voice mail hunt group; it will be used directly.
- **RAD Hunt Groups Directory Number to use:** This is a free form text field, and is mandatory. Specify the hunt group numbers to use when creating a RAD hunt group. The values can be entered as a range (4000-5000), or as individual comma-separated numbers (4000,4001), or a combination of the two. When Management Portal creates a RAD hunt group, the next free number will be taken from this list. Management Portal assumes that these hunt groups do not already exist. Valid characters include digits, hyphens, commas, and spaces. The maximum number of characters accepted is 50.
- **RAD Hunt Group COS:** This is the Class of Service (COS) that Management Portal will use when creating the RAD Hunt Group, and the COS will be assigned to the hunt group. Only one COS is supported, and it must already be programmed. This field is mandatory. Valid characters include digits only. The maximum number of characters accepted is three.
- **RAD Phase Timer:** This value is used when creating RAD hunt group. It is up to 2 digits with the range value 1 to 99.
- **RAD Ports:** These are the ports that Management Portal can use for RADs when creating a RAD hunt group. This is a free form text field. The range/values can be entered as a range (1-10), or individual comma-separated numbers (1,2) or a combination of the two. When Management Portal creates a RAD hunt group, the next free port will be taken from this list. This field is mandatory. Valid characters include digits, hyphens, commas, and spaces. The maximum number of characters accepted is 50.
- **RAD Port COS:** This is the Class of Service (COS) for Management Portal to use when creating a RAD Hunt Group. This COS will be assigned to each port in the RAD hunt group. Only one COS is supported, and it must already be programmed. This field is mandatory. Valid characters include digits only. The maximum number of characters accepted is three.
- **RAD indices used for RAD Greetings:** This is a free form text field for specifying the index numbers to used when uploading RAD indices. The range/values can be entered as a range (1-10), or individual comma separated numbers (1,2) or a combination of the two. When the Customer admin creates a new RAD greeting, the next free index will be taken from this list. This field is mandatory. Valid characters include digits, hyphens, commas, and spaces. The maximum number of characters accepted is 50.
- **Use Embedded Music On Hold** checkbox: Select the checkbox to display the following:
    - **Music On Hold Indices used for ACD:** This is used for ACD Music On Hold feature only. This is a free form text field where the SP must specify index numbers to be used when uploading Music On Hold. The range/values can be entered as a range (1-10), or individual comma separated numbers (1,2) or a combination of the two. When the admin creates a new MOH, the next free index is taken from this list. This field is mandatory. Maximum characters accepted is 50.

Existing Bundles

After upgrading Management Portal, existing bundles do not have RAD programming enabled.

Configure ACD RAD and Music on Hold resiliency

ACD Greetings (RAD) resiliency

An ACD Greeting is programmed as resilient when there is a secondary (resilient) controller on its Site.

Create the RAD Greetings

Follow the instructions in Program ACD greetings to program ACD Greetings for a Customer. As long as there is a resilient controller in the site selected for the ACD Greeting, the greeting will be programmed on both the primary and secondary controller.

> ⚠ Customer Administrator Portal uses SFTP to upload audio files for MiVoice Business 9.0 version and up. To use SFTP, configure the Voice Admin Password in Edit a Platform Group.

⚠ If you need to use a secondary system of a resilient pair as a primary system for a site, different RAD port range should be programmed on Management Portal for Primary and Secondary MiVoice Business. Failure to do so results in greetings getting overwritten.
In MiVoice Business, on secondary MiVoice Business, same ports should be programmed as Primary MiVoice Business and its ports need to be programmed as per its own range.
When Management Portal configures a resilient greeting, it uses the same ports on both primary and secondary. These ports are taken from the primary port list regardless of secondary ports configured.

⚠ When creating an ACD Greeting, if you select a site with a resilient controller, you will not be able to record a greeting using the keys on your telephone.

Changing the secondary controller

A Site can be edited and the secondary controller can be changed while editing the Platform Group:

1. If the Site did not have a secondary controller and you edit the site and add a secondary controller, all ACD Greetings created through the MiCloud Management Portal will be programmed on the secondary.

⚠ Once the Site is created, it cannot be edited.

ACD Music on Hold resiliency

ACD Music on Hold is programmed as resilient when there is a secondary (resilient) controller on its Site.

Create the ACD Music On Hold

Follow the instructions in Program ACD Music on Hold to program ACD Music On Hold for a Customer. As long as there is a resilient controller in the site selected for the ACD Music On Hold, it will be programmed on both the primary and secondary controller.

Changing the secondary controller

A Site can be edited and the secondary controller can be changed while editing the Platform Group:

1. If the Site did not have a secondary controller and you edit the site and add a secondary controller, all ACD Music On Hold created through the MiCloud Management Portal will be programmed on the secondary.

⚠ Once the Site is created, it cannot be edited.

Configure ACD Path resiliency

⚠ The configuration tasks discussed in this topic are performed in the Customer Administrator Portal. To configure resilient ACD paths or RADs for a customer, log in to the Customer Administrator Portal using the Customer Admin account for that customer.

ACD Path resiliency

The fields specific to making an ACD Path resilient are available to you if you are either:

- Logged in to the Service Provider Portal and you have performed a "login as" the Customer Admin.
- A Customer Admin who has the **Advanced ACD Paths** feature in their Admin Bundle.

Create Trunks

You can program the SIP trunks on the Trunk controller using the normal procedure in the MiVoice Business System Administration Tool.

When that is complete:

1. Create a Trunk Route Directory Number (also sometimes called a Phantom DN) that will be the Route point for a particular ACD Path. The Direct Inward Dial Service form is programmed, routing the the DID to this number.
2. Use this Route Point DN when creating the resilient Paths.

Create ACD Paths

Follow the instructions (in the Customer Administrator Portal help) to program ACD Paths for a Customer using the Trunk Route Directory number generated when creating the ACD Path.

Specify either two different ACD Path DNs for the primary and secondary controllers (must not be local-only), or the same DN for both ACD Paths. They are then created as local only.

Management Portal creates the resilient path and sets up the programming to route the calls from the Trunk Route Point to the ACD Paths.

❗ You can change the ACD Path, however, you cannot change the local-only field.

Changing the secondary controller

⚠ The Hunt Group Number should be set as 6000 in the secondary MiVoice Business to handle the change of non-resilient ACD path with VM to resilient ACD path.

1. Complete the configuration of the Customer with only primary MiVoice Business controllers for the site. Before creating resilient ACD Paths, you first specify a resilient MiVoice Business.
2. When the Path programming is complete:
   a. Edit the Site in the **Edit Platform Group** (in the Service Provider Portal) to add the resilient MiVoice Business.
   b. Edit the ACD Path and select **Enable ACD Path Resiliency**.
   c. Add the DN for the resilient Path and the optional Trunk Route Directory Number.
3. Change the secondary controller for the site.

Management Portal removes all of the resilient ACD Paths from the old controller and programs all resilient ACD Paths for that site on the new secondary controller.

Program ACD and MOH

MiCloud Management Portal supports programming ACD paths and groups, ACD Greetings, and Music on Hold.

- Create ACD Groups
- Program ACD Greetings
- Program ACD Music on Hold
- Create ACD Paths

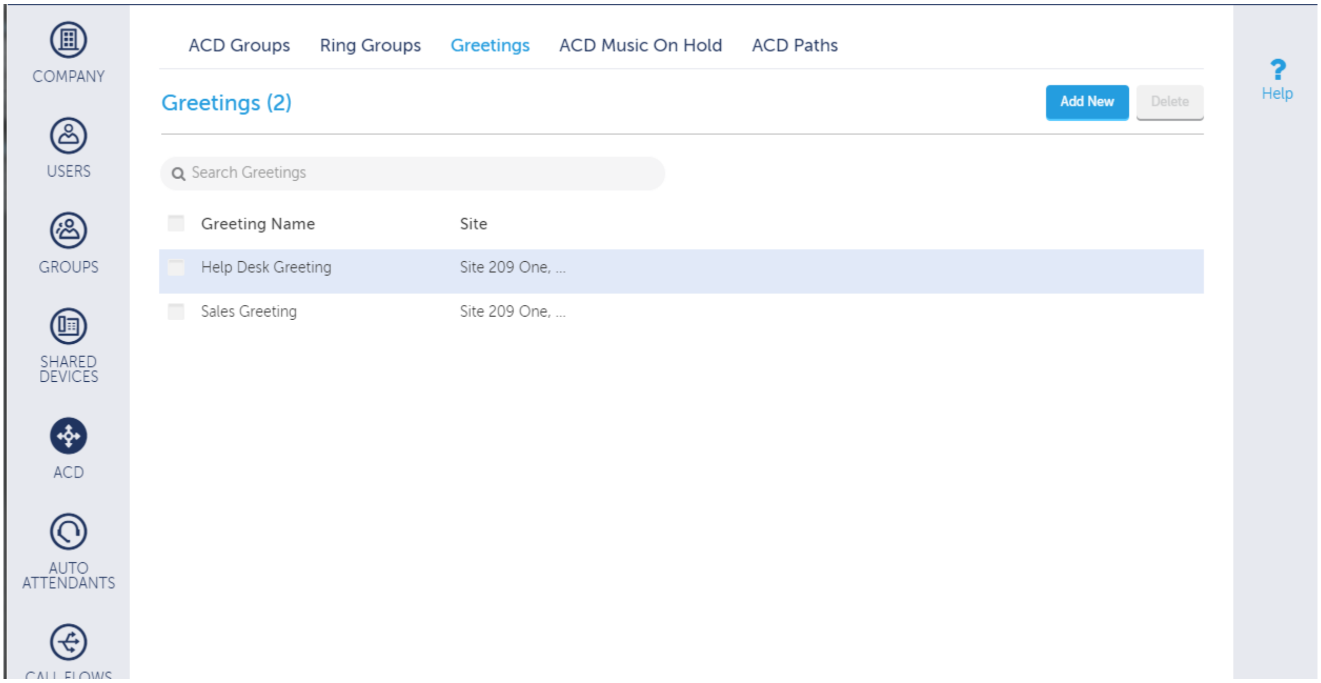
For notes and recommendations when programming ACD, see Considerations.

Program ACD greetings

The Greetings tab appears on the ACD page in the Customer Administrator portal when the user is the SP/VAR/VSP or a customer administrator who has the RAD Programming privilege.

Customer administrator view

A customer administrator, with the proper privilege, can search for (by name), create, edit, or delete ACD greetings. Here is the view of the landing list for the customer administrator:

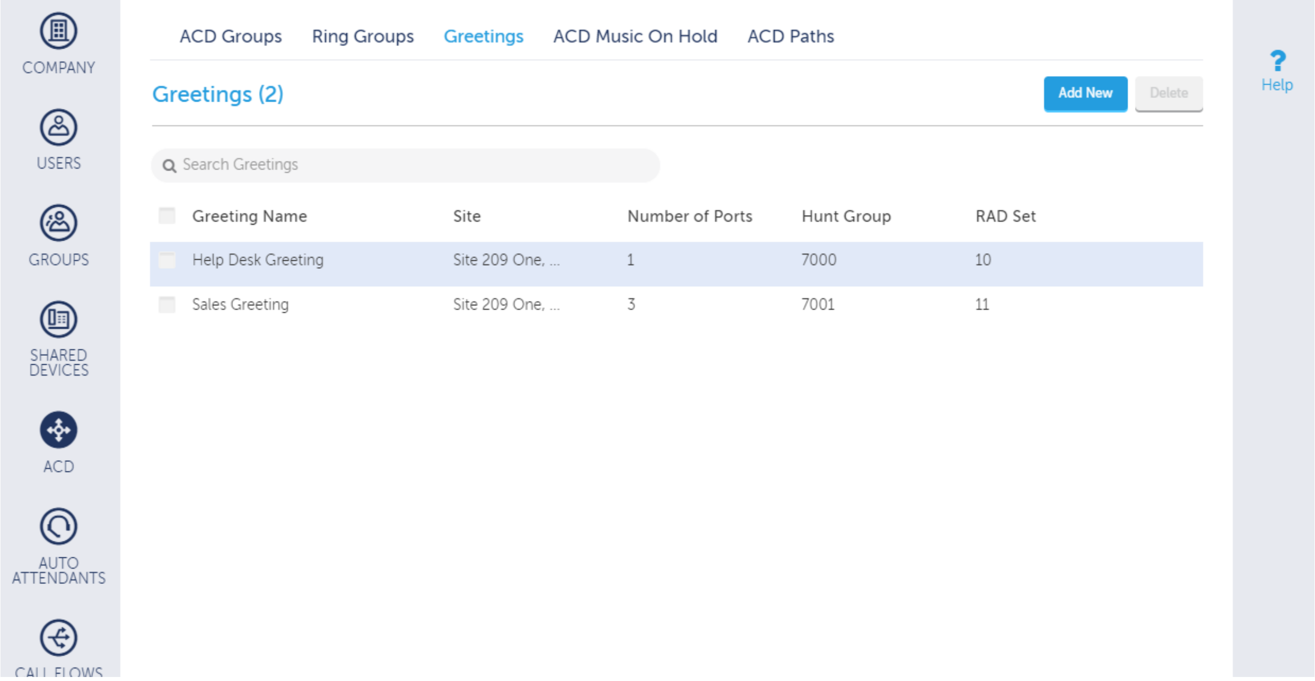


Greetings (2)

	Greeting Name	Site
□	Help Desk Greeting	Site 209 One, ...
□	Sales Greeting	Site 209 One, ...

SP, VAR, and VSP administrator view

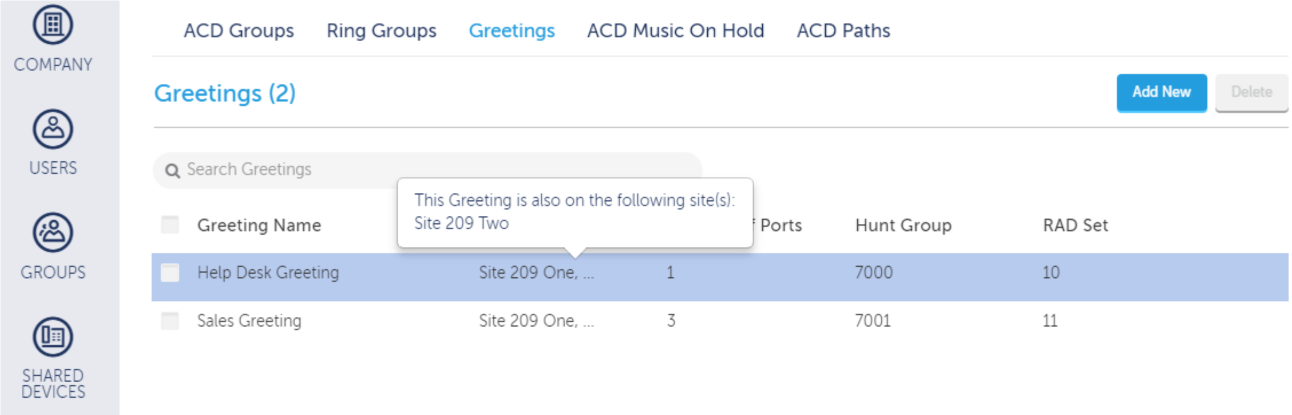
In the screen image below, the Number of Ports, Hunt Group, and RAD Set columns appear for a SP, VAR, and VSP users:



Greetings (2)

	Greeting Name	Site	Number of Ports	Hunt Group	RAD Set
□	Help Desk Greeting	Site 209 One, ...	1	7000	10
□	Sales Greeting	Site 209 One, ...	3	7001	11

Because sites can have duplicate MiVoice Business pairs, any greeting created on one site will be available to another site that has the same prime MiVoice Business. When the greeting is available on more that one site, the administrator can hover over the site name to see the sites the greeting is available on:

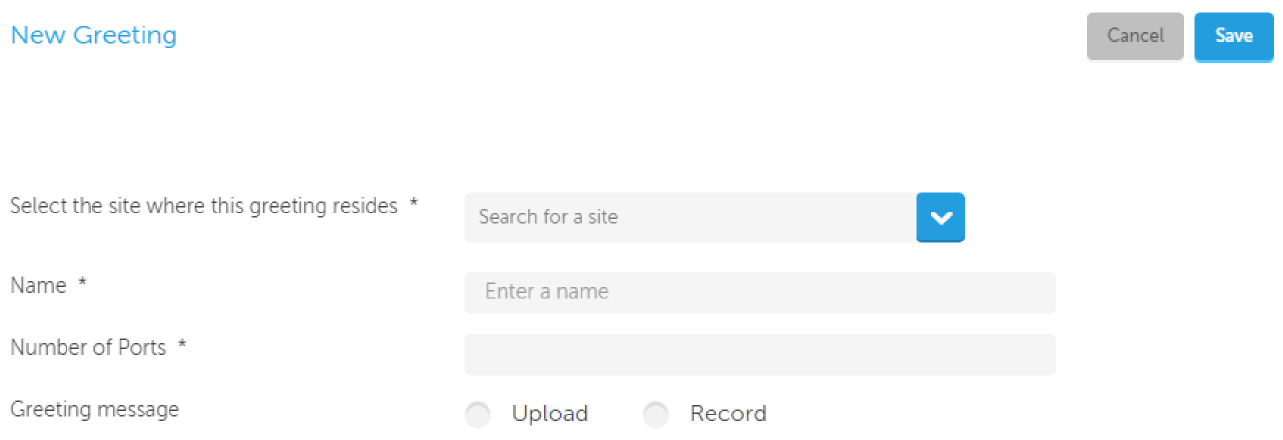


Greetings (2)

This Greeting is also on the following site(s):
Site 209 Two

	Greeting Name		Ports	Hunt Group	RAD Set
□	Help Desk Greeting	Site 209 One, ...	1	7000	10
□	Sales Greeting	Site 209 One, ...	3	7001	11

To create a new greeting (Add New), you must specify a site, name for the greeting, and the number of ports to use for the greeting and then record the greeting. After the greeting is created, you can select it when creating ACD paths (Audio settings tab in ACD Paths).



New Greeting

Cancel Save

Select the site where this greeting resides *	Search for a site
Name *	Enter a name
Number of Ports *	
Greeting message	○ Upload ○ Record

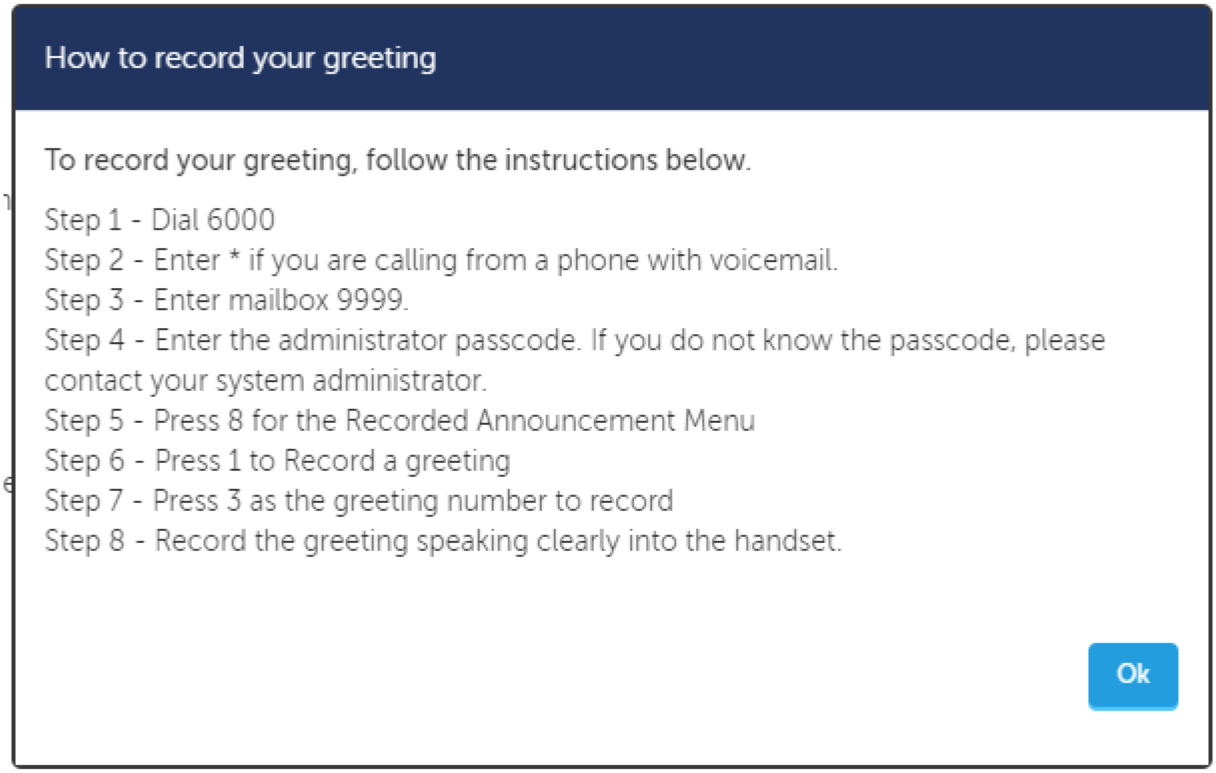
Site The destination where the greeting message is uploaded. The audio file is uploaded to both MiVoice Business platforms in the site.

Name The administrator can change the name to a meaningful label. The portal will display this label in the dropdown for the RAD greeting in the audio settings tab in the ACD Path editing pages. The name is mandatory. The maximum characters allowed for the name is 20 (because this name will be used for the hunt group name and the MiVoice Business can only have 20 chars for the hunt group name).

Number of Ports The number of ports you want to assign to the RAD hunt group. This number is based on the expected number of callers and greeting length, and how long callers can be expected to wait to hear the greeting. The maximum characters allowed for the field is 2. Digits only allowed. This field is mandatory. It is not displayed to the customer admin when creating an ACD Greeting, and in their case, the Number of Ports used is 1. See the MiVoice Business documentation for more details.

Greeting Message You can either upload or record the message. When you select Record, instructions on how to record a greeting display. The Upload option is available with MiVoice Business version 8.0 SP3 or later.

Here are the instructions that display for recording a greeting:



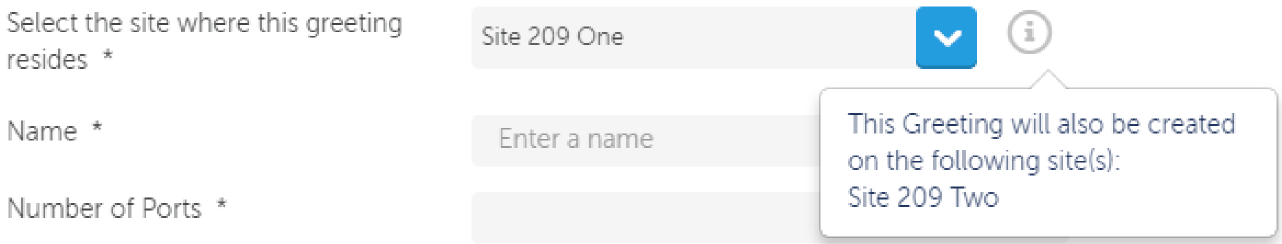
How to record your greeting

To record your greeting, follow the instructions below.

Step 1 - Dial 6000
Step 2 - Enter * if you are calling from a phone with voicemail.
Step 3 - Enter mailbox 9999.
Step 4 - Enter the administrator passcode. If you do not know the passcode, please contact your system administrator.
Step 5 - Press 8 for the Recorded Announcement Menu
Step 6 - Press 1 to Record a greeting
Step 7 - Press 3 as the greeting number to record
Step 8 - Record the greeting speaking clearly into the handset.

Note
You cannot create new greetings when there are no free hunt group numbers, port indices, or greeting indices. You will get an error message that there are not enough resources to create a greeting.

You must specify a site when creating a Greeting (RAD). If that customer has more than 1 site where the prime MiVoice Business platform is the same, an information icon will be displayed. When the admin hovers over it, it will explain that the greeting will be available to multiple sites.

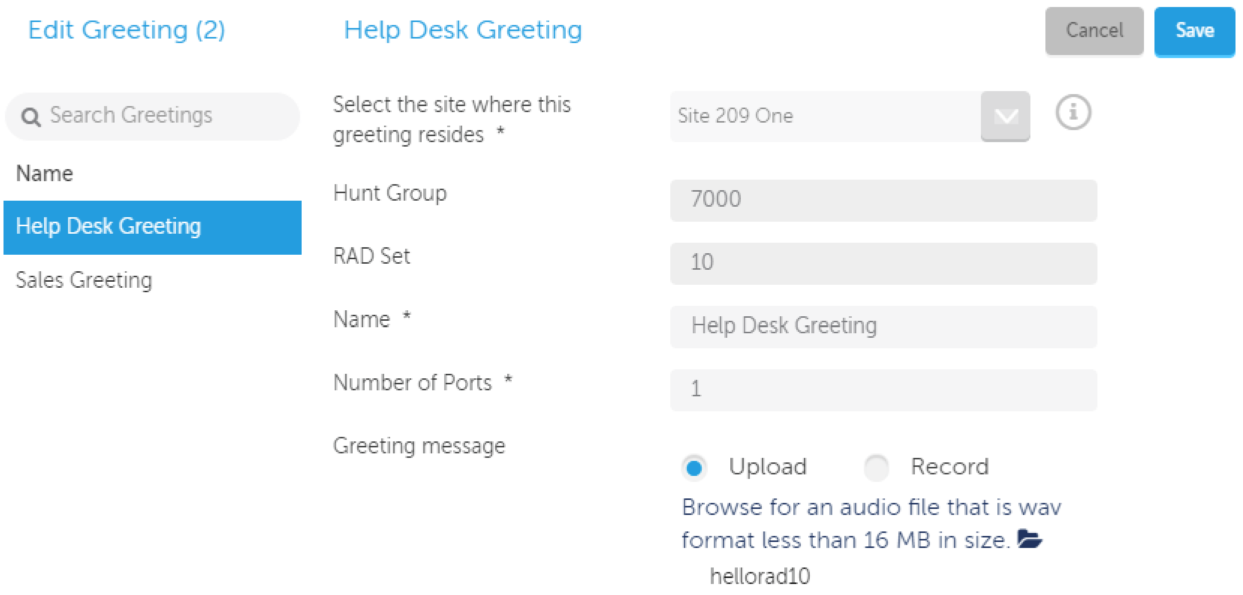


Select the site where this greeting resides *	Site 209 One
Name *	Enter a name
Number of Ports *	

This Greeting will also be created on the following site(s):
Site 209 Two

The user can also edit a RAD message. The Site is not changeable. The customer admin will not see the number of ports field, RAD Set or Hunt Group fields.

The user can change the name of the greeting, adjust the number of simultaneous greetings ports (SP/VSP/VSR Admins only), or upload or record a new message.



Edit Greeting (2)

Help Desk Greeting

Name
Help Desk Greeting
Sales Greeting

Select the site where this greeting resides *: Site 209 One

Hunt Group: 7000

RAD Set: 10

Name *: Help Desk Greeting

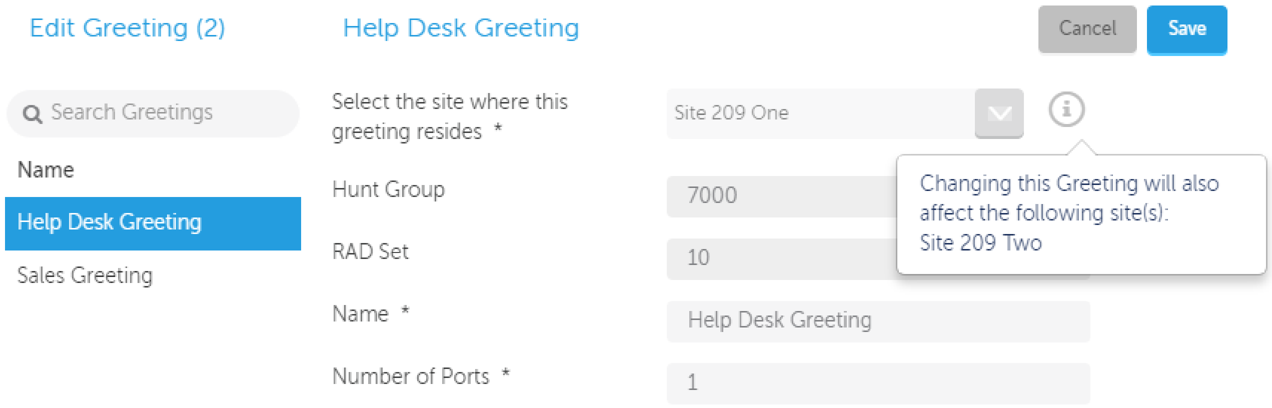
Number of Ports *: 1

Greeting message: ● Upload ○ Record

Browse for an audio file that is wav format less than 16 MB in size.

hellorad10

If the rad greeting is assigned a site that has a MiVoice Business platform is a prime of multiple sites, then that rad greeting will be available to other sites. If this is the case, the info icon, will be displayed and if the admin hovers over icon, a popup will be displayed listing the other sites as shown below.



Edit Greeting (2)

Help Desk Greeting

Name
Help Desk Greeting
Sales Greeting

Select the site where this greeting resides *: Site 209 One

Changing this Greeting will also affect the following site(s):
Site 209 Two

Hunt Group: 7000

RAD Set: 10

Name *: Help Desk Greeting

Number of Ports *: 1

If you delete a RAD greeting, the ports are returned to VM ports and the hunt group is deleted and all RAD greeting forms will be cleaned up. The message associated with the RAD greeting can not be deleted though, but the index can certainly be re-used for another RAD greeting.

Note

Management Portal is the assumed master view for the RAD Programming because it automates RAD management as much as possible. Assume that when there is data contention between Management Portal programmed RAD data versus the data that is overwritten using ESM, Management Portal wins and overwrites the data in the MiVoice Business platform.

Program ACD Music on Hold

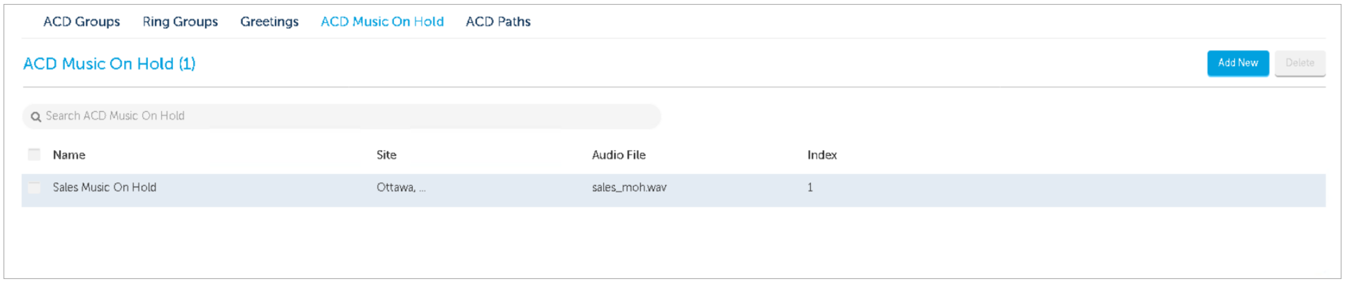
Music on Hold is the music heard between recorded greetings and messages (RAD). This page describes the ACD MOH (Music On Hold), which is new for Management Portal 6.1. Management Portal has supported System MOH for the last few releases.

ACD Music On Hold is available in the UI only if:

- The RAD source is Embedded Voicemail, and
- There are MOH indices programmed in the **ACD Embedded RADs** tab of the the Platform Group.

Note
Only Customer Admins with the **ACD Music On Hold** permission will see the Music On Hold feature.

- Customer Admins do not see the Index field in the MOH entries.



ACD Music On Hold (1)

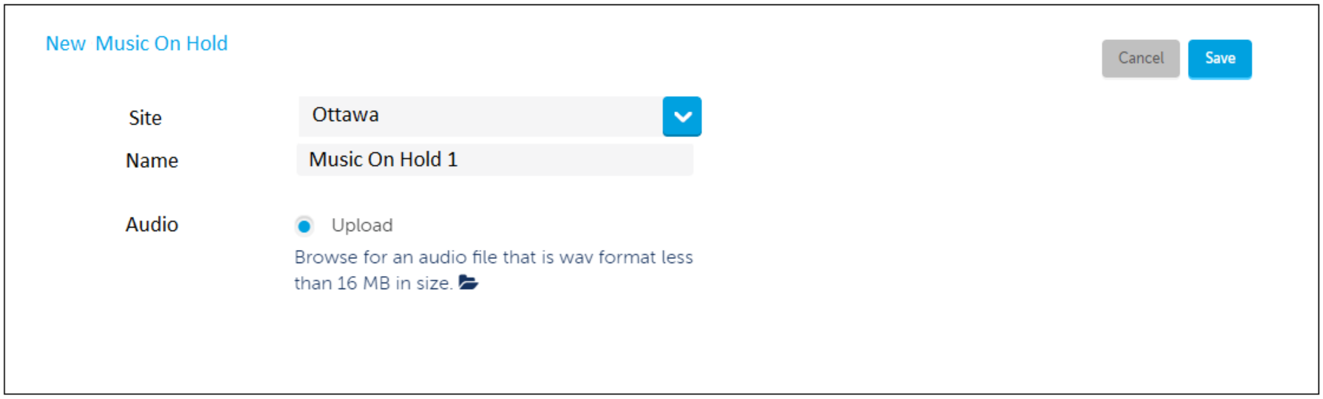
Name	Site	Audio File	Index
Sales Music On Hold	Ottawa, ...	sales_moh.wav	1

Creating a new Music on Hold entry

To create a new MOH entry:

1. Select the **Site** to upload the MOH to. The audio file will be uploaded to both primary and secondary MiVoice Business on the site.
2. Enter a **Name** for the new MOH entry. This label is displayed on the ACD Path editing pages.

Upload an audio file to use for Music on Hold. You can re-use audio files used elsewhere in Management Portal.



New Music On Hold

Site: Ottawa

Name: Music On Hold 1

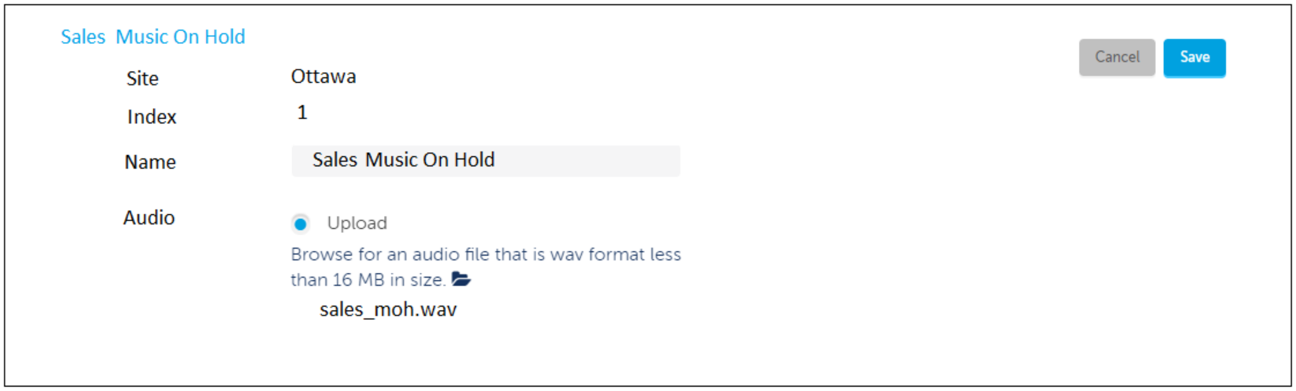
Audio: ● Upload

Browse for an audio file that is wav format less than 16 MB in size.

Customer Admin MOH

The Customer Admin can edit Music on Hold entries, if they have the Music On Hold feature enabled.

- **Site** cannot be edited.
- **Name** can be changed.
- The **Audio** file can be changed. In edit mode, the name of the current MOH file is displayed.



Sales Music On Hold

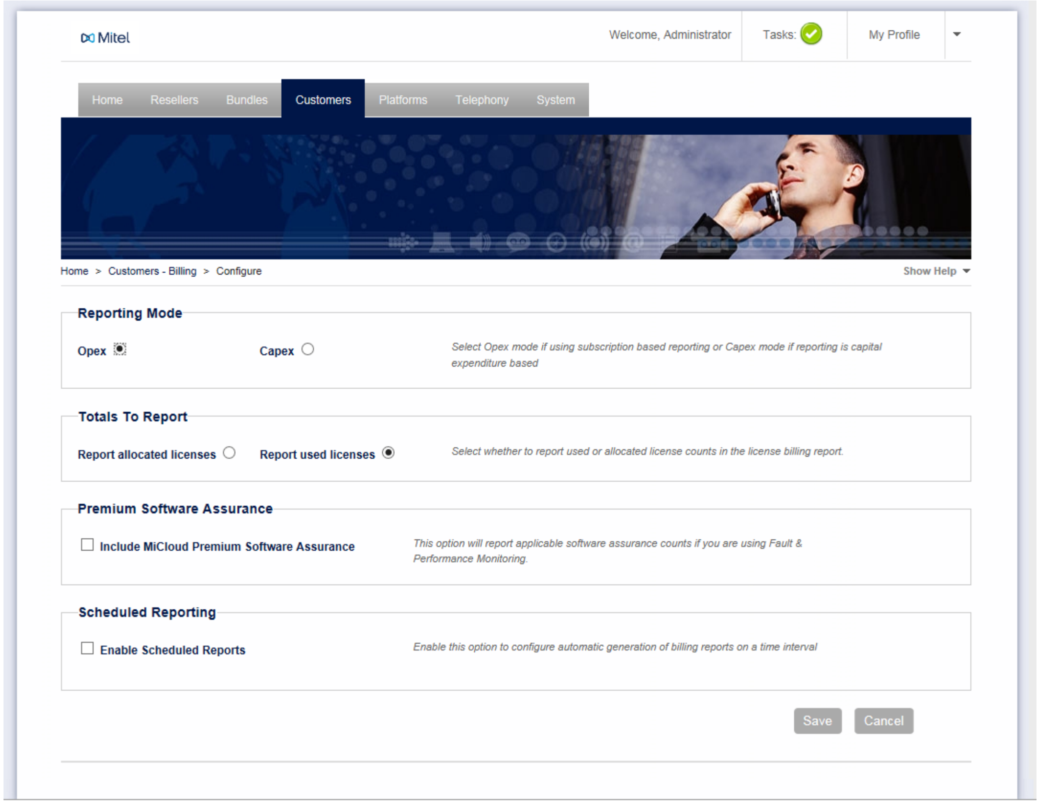
Site	Ottawa
Index	1
Name	Sales Music On Hold
Audio	● Upload Browse for an audio file that is wav format less than 16 MB in size. sales_moh.wav

Administer

Management Portal allows you to configure and generate reports and manage users through the Customer Administrator portal in these topics:

- Manage users
- Add a resilient MiVoice Business instance
- Manage billing reports

Report management in the Service Provider portal



Reporting Mode

Opex ● Capex ○

Select Opex mode if using subscription based reporting or Capex mode if reporting is capital expenditure based

Totals To Report

Report allocated licenses ○ Report used licenses ●

Select whether to report used or allocated license counts in the license billing report.

Premium Software Assurance

□ Include MiCloud Premium Software Assurance

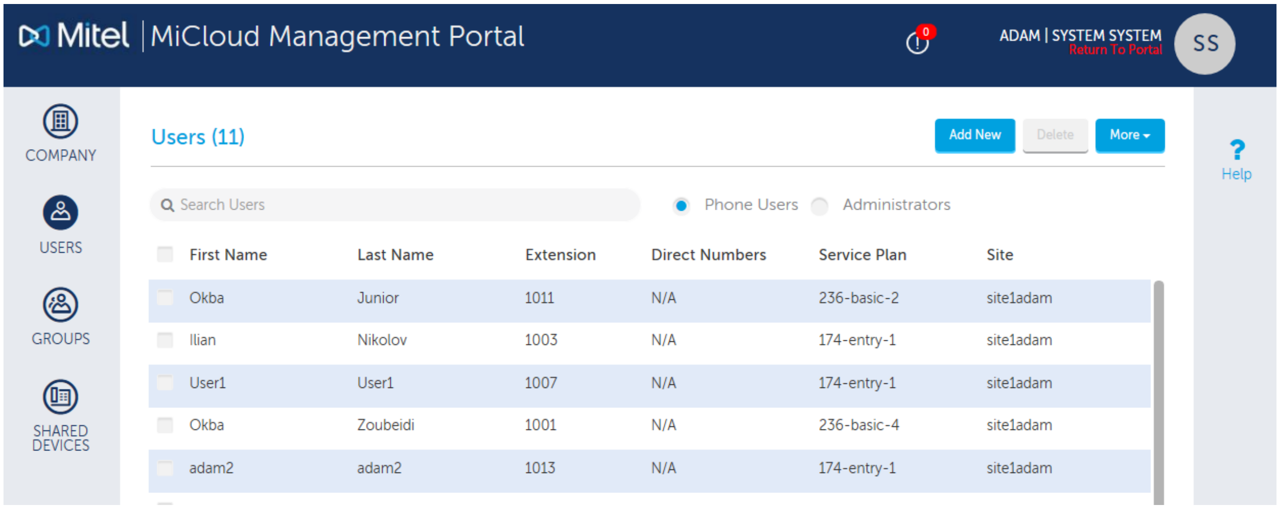
This option will report applicable software assurance counts if you are using Fault & Performance Monitoring.

Scheduled Reporting

□ Enable Scheduled Reports

Enable this option to configure automatic generation of billing reports on a time interval

User management in the Customer Administrator portal



First Name	Last Name	Extension	Direct Numbers	Service Plan	Site
Okba	Junior	1011	N/A	236-basic-2	site1adam
Ilian	Nikolov	1003	N/A	174-entry-1	site1adam
User1	User1	1007	N/A	174-entry-1	site1adam
Okba	Zoubeidi	1001	N/A	236-basic-4	site1adam
adam2	adam2	1013	N/A	174-entry-1	site1adam

Manage users

By default, MiCloud Management Portal manages users and allows service providers to edit and delete users, change user bundles, and perform other administration tasks.

How Management Portal manages users

Actions that make users become unmanaged

A user can become unmanaged when you make changes outside of MiCloud Management Portal, for example, you create a user in MiCollab Client Service or edit fields externally. This means that the fields in MiCloud Management Portal are no longer synchronized with the fields changed externally and they become read-only fields in MiCloud Management Portal. You must return to MiCollab Client Service to edit the fields. See MiCollab Client Service and MiCloud Management Portal field overrides for details.

A user becomes unmanaged when you:

- Change the number and types of services so much that they no longer match the MiCloud Management Portal bundle and site definition. For example, adding a device that is not supported in MiCloud Management Portal, or adding 5 phones in MiCollab Client Service when a maximum of four phones is supported in MiCloud Management Portal.
- Change the user e-mail address from MiCollab Client Service.
- Change the user Login ID from MiCollab Client Service.
- Change the Location field from MiCollab Client Service.
- Change the Speech Auto Attendant Associated Phone field in MiCollab Client Service to a non-prime number, for example, 54*70.
- Set Auto Attendant Privacy in MiCollab Client Service.
- Change MAC Addresses that are not related to Set Replacement or Installer PIN operations.

To make the user manageable

When the user is modified outside MiCloud Management Portal, for example, MiCollab/MiVoice Business, the user becomes unmanageable. To make the user manageable, run the following maintenance command:

```
reconcile_extension webId extension
```

Considerations regarding unmanaged users

- The End User Portal is not available for unmanaged users.
- The "Create new user from existing user" feature is not available in the Customer Administrator Portal.
- The first available extension is picked when a user created in MiCollab Client Serves does not have an extension that is digit only. For example, it would select "54*57" if the extensions available were 54*57, 54*68, and 54*70.

Operations that you cannot manage concurrently

Other operations that you cannot manage from MiCollab Client Service when they are managed from MiCloud Management Portal:

- Teleworker
- E-mail deployment

Usage and billing information for unmanaged users

When MiCloud Management Portal cannot synchronize a user and associated services, the user is highlighted as unmanaged. However, MiCloud Management Portal still provides usage and billing information around for that user. When a user is no longer managed, MiCloud Management Portal:

- Collects license information.
- Displays user fields as “Read Only”.
- Indicates "unmanaged" in the Bundle column.

MiCollab Client Service and MiCloud Management Portal field overrides

The following tables list the fields that you can override using MiCollab Client Service. They also indicate whether those fields stay managed in MiCloud Management Portal.

User tab

MiCollab Client Service field	MiCloud Management Portal field	Can configure in MiCollab Client Service?	User stays managed in MiCloud Management Portal field?
First Name	First Name	yes	yes
Last Name	Last Name	yes	yes
E-mail	E-mail	yes	no
Login	User Name	yes	no
Location	CESID Name	yes	no
Department	n/a	yes	yes
Prompt Language	Language Preference	yes	partial - Chooses the closest language, for example French Canadian if localized. If language not found, defaults to English.

MiCollab Client Service field	MiCloud Management Portal field	Can configure in MiCollab Client Service?	User stays managed in MiCloud Management Portal field?
UCC Bundle	Bundle License Type	yes	no
IDS Manageable	n/a	yes	yes
Password *	Auto-generated	yes	yes
TUI Passcode *	Auto-generated	yes	yes

Phone tab

MiCollab Client Service field	MiCloud Management Portal field	Can configure in MiCollab Client Service?	Stays managed in MiCloud Management Portal field?
Number	Extension Number	yes	no
Service Label	n/a	yes	yes
DID Service Number	DID	yes	no
CESID	Emergency Response Location	yes	yes
Hot Desk User	Phone Type	yes	no
ACD Agent	Phone Type	yes	no
External Hot Desk License	Phone Type	yes	no
Hot Desk User External Dailing Prefix	Prefix	yes	yes
Hot Desk User External Number	Simultaneous Ringing Number	yes	yes Note: This field is not updated in the Management Portal end user portal.
Deployment Profile	Auto managed	Do not edit this field.	no
Preferred Set	Hard coded	yes	yes
Service Level	Hard coded	yes	yes
Zone ID	Part of Sites	yes	yes
Call Coverage Service Number	n/a	yes	yes

MiCollab Client Service field	MiCloud Management Portal field	Can configure in MiCollab Client Service?	Stays managed in MiCloud Management Portal field?
COS	Feature Profile	yes	yes
COR	Dialing Plan	yes	yes
Send Deployment E-mail	Welcome E-mail code	n/a	n/a
SIP Device Capabilities	Hardcoded	yes	yes
SIP Password *	Auto-generated		
SAA associated phone	Auto managed	yes	no
SAA Privacy	Private	yes	no
Device Type	Device Type	yes	no
MAC Address	MBG device	no	only for installer PIN case

MiCollab Unified Messaging

MiCollab Client Service field	MiCloud Management Portal field	Can configure in MiCollab Client Service?	Stays managed in MiCloud Management Portal field?
Extension	Hardcoded to prime phone in MiCollab	yes	yes
Attendant Extension	In MiCloud Management Portal field bundle	yes	yes
FCOS	In MiCloud Management Portal field bundle	yes	yes
LCSOS	In MiCloud Management Portal field bundle	yes	yes
MWI #1	In MiCloud Management Portal field bundle	yes	yes
MWI #2	In MiCloud Management Portal field bundle	yes	yes
Standard UM	In MiCloud Management Portal field bundle	yes	yes
Advanced UM	In MiCloud Management Portal field bundle	yes	yes
Record-a-Call	n/a	yes	yes

MiCollab Client

MiCollab Client Service field	MiCloud Management Portal field	Can configure in MiCollab Client Service?	Stays managed in MiCloud Management Portal field?
Feature Profile	In MiCloud Management Portal field bundle	yes	no
Deskphone Extension	In MiCloud Management Portal field bundle	yes	no
Softphone Extension	In MiCloud Management Portal field bundle	yes	no
Mailbox Number	Hardcoded	yes	no
MiTeam	In MiCloud Management Portal field bundle	no	n/a
E-mail List	User Profile	yes	yes

When a group member becomes unmanaged

When a group member becomes unmanaged, Management Portal detects the unmanaged user (during save) and you receive an error message. However, you can have an unmanaged user as an overflow point or voicemail operator.

Changing DID numbers outside of Management Portal

You can use periodic syncs in the billing scheduler to sync and update user data between Management Portal and MiCollab. When set up, the sync updates and saves the first name, last name, extension information, and DID data in the Management Portal database.

> ❗ * Auto-generated passwords are not HIPAA compliant.

Add, edit, and delete users

Log in as a Customer Administrator from Management Portal and create, modify, and delete users.

Note: After you create a user or update a user's Direct Number, the change may not appear in the Direct Number list right away. The Direct Number list will update after the data from MiVoice Business is synchronized with MiCollab.

To add a user:

1. From the Customer Administrator portal, click the **Users** tab.
2. Click **Add New**.
3. **User Profile**
    a. Enter the User details. Fields marked with an asterisk (*) are required. Enter a minimum of 4 characters for the username.
    b. Click **Next**.
4. **Service Plan**

   a. Click **Select** to choose a phone plan for the User. The chosen plan is highlighted and **Selected** will display.
   b. Click **Next**.
5. **Service Programming**
   a. Select the service details for the User. Fields marked with an asterisk (*) are required.

      > ⚠ When you create an ACD Hotdesk user with a softphone, a shared device is automatically created for the user.
      > If you select a basic plan that does not include voicemail, you can still forward calls to voicemail (Call Handling Rules) however the calls will go to your corporate voicemail.

   b. Click **Next**.
6. **Phones**
   a. From the **Phone Type** list, select the type of phone for this user.
   b. From the **Emergency Response Location** list, select the location to which emergency call will be sent.
   c. (Optional): From the **Select a predefined key template to be applied to this phone** drop-down list, choose a key template for the primary phone. Phone key templates apply to the primary phone only.
   d. (Optional): Enter the MAC Address of the phone.

      > ⚠ When a user is created without MAC address, in case of registration from the device using **##, admin need has to run the billing sync to add the device on MBG.

   e. Click **Next**.
7. **Phone Keys**(optional)
   When you choose a MiNet phone type, a step is added to allow you to program the phone keys. You can also edit the prime phone key and specify the Ring type on all phones that allow key programming.
   When you select a MiNet Phone type for example the 5330e IP, you can program the phone keys as follows:
   a. Click a key on the phone diagram.
   b. Select what should happen when a phone user presses the key.
   c. Click **OK**.
   d. Repeat steps a to c to program other keys and click **Save**.
8. **Advanced**
   a. Select the call handling rules.
9. Click **Save**.

To edit a user:

Important: If you change the e-mail address from MiCollab Client Service, it will not update in Management Portal. See How Management Portal manages users.

1. From the Customer Administrator portal, click the **Users** tab and select one or more users.
2. Make the required changes to the user's profile.

   > ⚠ Only similar types of bundles are listed in the **Service Plan** tab.

3. Click **Save**.

To delete a user:

Deleting a user is quick when you use the action list. The Delete User action permanently removes the user’s profile and access to the Management Portal. You can delete one user at a time only.

1. From the Customer Administrator portal, click the **Users** tab and select one or more users.
2. Click **Delete**.
   If you are trying to delete more than one user, a message is displayed that deleting the users belonging to n group(s) takes n mins.

Delete and modify users externally

When a user is added on Management Portal and then deleted externally, for example from MiCollab the user is deleted when a sync is performed in Management Portal.

Reset passwords

The Management Portal server generates a new password and sends an e-mail to the user with the new password. The Customer Admin can reset the passwords from the Customer Admin portal under Users.

Management Portal can reset following types user passwords:

- MiCollab password
- Portal password
- Phone PIN
- SIP password
- Voicemail password

If you select SIP Password and you have more than one SIP capability (for example MBG SIP and SIP softphone) Management Portal will reset and send both passwords.

Single user selection

Selecting a single user generates a new user password for the portal. Other passwords are also generated and sent depending one the bundle assigned to the user.

Multiple user selection

Selecting multiple users generates a new password for the portal only. Because the other passwords depend on bundles assigned to users, you must select one user at a time to reset other passwords. You can select a maximum of 25 users at a time.

To reset passwords:

1. From the Customer Administrator portal, click the **Users** tab and select one or more users.
2. In the **Select an Action** list, click **Reset Password**.
3. Select the type of password(s) to reset.
4. Click **Reset Password & Send Email**.

Resend the welcome e-mail

The Resend Welcome E-mail option is available in the Customer Administrator Portal for single and multi-user selection. Portal and MiCollab passwords are reset to system generated passwords when you resend the Welcome e-mail.

If you need to resend the Welcome e-mail to more than 25 uses, resend it from the Service Provider Portal using maintenance commands. See "Bulk resend the Welcome e-mail" for details.

To resend the Welcome e-mail:

1. From the **Customer Administrator** portal, click the **Users** tab and select the recipient for the e-mail message.
2. In the **Select an Action** drop-down list, click **Resend Welcome Mail**.

You can also create and assign other e-mail templates, for example, important notifications such as password updates, voicemail updates and so on. Any e-mail template created and assigned to a Customer is accessible from the Users tab.

Bulk resend the Welcome e-mail

To resend a Welcome e-mail to more than 25 users, use the maintenance commands.

Step 1 Launch the command page:

- Login to the Management Portal service provider portal (http://xx.xx.xx.xx/konos/sp/spLogin.do). Replace xx.xx.xx.xx with the Management Portal server IP address or FQDN.
- Enter this URL in the same active service provider browser session (https://xx.xx.xx.xx/konos/commands.jsp) Replace xx.xx.xx.xx with the Management Portal server IP address or FQDN. This will open up Management Portal Service Provider maintenance command window.

Step 2 Run one of the following RESEND WELCOME EMAIL commands:

To resend the Welcome mail for <u>one bundle and one customer</u>:

1. Make sure that bundle is assigned to the customer.
2. Run the following command and click on Submit.
   `$$RESEND WELCOME EMAIL$$ <BN1>|<CUSTWEBID1>`
3. Replace following variables...

    - BN1 with Bundle Name
    - CUSTWEBID1with Customer Web-ID.
    - Semi Colon (;) should be used as delimiter/separator between bundle name and same should be used in case of Customer Web-Ids.
    - Set of Bundle names and set Customer Web-Ids should be separator by Pipe (|).

Example:

```
$$RESEND WELCOME EMAIL$$ Entry3PhoneNextGenBundle|CQ001
```

To resend the Welcome for <u>one bundle and multiple customers</u>:

1. Make sure that all the bundles are assigned to all the customers.
2. Run the following command and click on Submit.
   `$$RESEND WELCOME EMAIL$$ <BN1>|<CUSTWEBID1>;<CUSTWEBID2>;<CUSTWEBID3>`
3. Replace following variables...

    - BN1 with Bundle Name
    - CUSTWEBID1, CUSTWEBID2, CUSTWEBID3 with Customer Web-ID. Semi Colon (;) should be used as delimiter/separator between bundle name and same should be used in case of Customer Web-Ids.
    - Set of Bundle names and set Customer Web-Ids should be separator by Pipe (|).

Example:

```
$$RESEND WELCOME EMAIL$$ Entry3PhoneNextGenBundle|CQ001;CQ002;CQ003
```

To resend the welcome mail for <u>multiple bundles and multiple customers</u>:

1. Make sure that all the bundles are assigned to one of the provided customer.
2. Run the following command and click on Submit.
   `$$RESEND WELCOME EMAIL$$ <BN1>;<BN2>;<BN3>|<CUSTWEBID1>;<CUSTWEBID2>;< CUSTWEBID3>`
3. Replace following variables...

    - BN1, BN2, BN3 with Bundle Name
    - CUSTWEBID1, CUSTWEBID2, CUSTWEBID3 with Customer Web-ID.
    - Semi Colon (;) should be used as delimiter/separator between bundle name and same should be used in case of Customer Web-Ids.
    - Set of Bundle names and set Customer Web-Ids should be separator by Pipe (|).

Example:

```
$$RESEND WELCOME EMAIL$$ Entry3PhoneNextGenBundle;Stand4PhoneNextGenBundle |CQ001;CQ002;CQ003
```

Update bundles

To update a bundle:

1. From the Management Portal service provider portal, click the **Bundles** tab.
2. Select the bundle you want to modify.
3. Click the **Edit** icon and make the required changes.
4. Upload any updated setup instructions that you want to include as an attachment in the welcome email.
5. Click **Save**.

Add a resilient MiVoice Business instance

If you set up a customer on a single MiVoice Business instance, you can add another MiVoice Business instance to the platform group later to make it resilient. To add a MiVoice Business instance to an existing platform group, add the new MiVoice Business to the Site as a secondary controller. All user devices on the primary MiVoice Business instance are updated with the new secondary MiVoice Business instance.

> ⚠ **Note**
> Changing a resilient MiVoice Business platform to another MiVoice Business platform is not supported for users or shared devices.

Considerations

When a user	Management Portal does this
Adds a resilient MiVoice Business platform	• Adds the secondary element to ACD Groups created on that site. • Adds ACD Greetings created on that site to the resilient MiVoice Business platform. • Adds ACD MOH created on that site to the resilient MiVoice Business platform. • Adds the secondary element to users and shared devices created on that site.
Changes a resilient MiVoice Business platform to another MiVoice Business platform	• Changes the secondary element of ACD Groups created on that site to the new controller. • Removes ACD Greetings created on that site from the old controller and adds them to the new controller. • Removes ACD MOH created on that site from the old controller and adds them to the new controller. • For ACD Paths that are resilient, removes ACD Paths created on that site from the old controller and adds them to the new controller.
Removes a resilient MiVoice Business platform	• Removes the secondary element from ACD Groups created on that site. • Removes ACD Greetings created on that site from the resilient MiVoice Business platform. • Removes ACD MOH created on that site from the resilient MiVoice Business platform. • Removes the secondary element for users and shared devices created on that site. • For ACD Paths that are resilient, removes ACD Paths created on that site from the resilient MiVoice Business platform.

To add a resilient MiVoice Business instance:

1. Log out any Hotdesk users before adding a resilient MiVoice Business.

2. From the **Platforms** tab, click **Platform Groups**.
3. Select the customer and then click the **Edit** icon.
4. Click the **Sites** tab.
5. Do the following:
    a. Click the **Edit** icon for the site that you want to apply resiliency.
    b. Click the **MiVoice Business** tab.
    c. Select the resilient MiVoice Business.
6. Click **Save**.

All user devices on the primary MiVoice Business instance are updated with the new resilient MiVoice Business instance. The customer is locked from making changes during this time.

To remove a resilient MiVoice Business:

1. From the **Platforms** tab, click **Platform Groups**.
2. Select the platform group and then click the **Edit** icon.
3. Click the **Sites** tab.
4. Click the **Edit** icon next to the customer site that contains the resilient MiVoice Business instance.
5. Click the **Mivoice Business** tab.
6. In the **Resilient MiVoice Business** drop-down list, select **No Resilient MiVoice Business**.

    > ⚠ **Note**
    > All user devices on the primary MiVoice Business instance are updated when MiVoice Business resiliency is removed. The customer is locked from making changes during this time.

7. Click **Save**.

Avoid scheduled maintenance during setup

Do not execute and disable any scheduled maintenance on the MiVoice Business when you run the MiVoice Business Resiliency option in Management Portal. For example, if the DBMS CHECK command starts to execute during that time, it will lock the MiVoice Business instance and cause errors in updating users.   If you encounter errors, you may try the operation again. This second try only updates those users that failed the first time. If you would like to set all users' resiliency values again, instead of only those that failed, then delete the task from the background task results list and run the Resiliency option again.

Manage billing reports

Reports simplify the workflow for service providers when they need to provide billing summaries to Mitel.

How Reporting Works

XML Report

The xml report, is of course an .xml file. This is a basic summary of the format.

There are five main sections to the report:

- General Report information

    Indicates the date and time the report was generated, the last sync time and the billing reporting mode.

- Bundles

    Includes details the features all the bundles the Service Provider has, plus the allocated and used count.

- Customers

  A list of all customers, their allocated bundles, devices, sites, users and voice mailbox details.
- Resellers

  A list of all Value-Added Resellers and Virtual Service Providers, including their customer's data.
- Service Provider License Details

  A list of all manually entered license counts specified in the Edit Licensing page.

The basic structure of the xml will be formatted as shown below.

```
<Billing>
    <ServiceProviderSnapshot>
        General information ...
        <BundleDetailsList>
            Bundle details ...
        </BundleDetailsList>
        <CustomerSnapshotList>
            Customer details ...
        </CustomerSnapshotList>
        <ResellerSnapshot>
            Reseller details ...
        </ResellerSnapshot>
        <ServiceProviderLicenseDetails>
            Manual License details ...
        </ServiceProviderLicenseDetails>
    </ServiceProviderSnapshot>
</Billing>
```

The following sections will describe each bolded section above in more detail.

General Information

The bolded sections below show where the general information is in the report.

```
<Billing>

    <ServiceProviderSnapshot>

        <billingMode></billingMode>

        <BundleDetailsList>

            Bundle details ...

        </BundleDetailsList>

        <CustomerSnapshotList>

            Customer details ...

        </CustomerSnapshotList>

        <ResellerSnapshot>

            Reseller details ...

        </ResellerSnapshot>

        <ServiceProviderLicenseDetails>

            Manual License details ...

        </ServiceProviderLicenseDetails>

        <time></time>

        <synctime></synctime>

    </ServiceProviderSnapshot>

</Billing>
```

Details about each highlighted field:

Field name	Format	Description	Possible values
Billing Mode	<billingMode></billingMode>	The mode the Service Provider is reporting in, which is either OPEX or CAPEX.	• OPEX • CAPEX
Report Generation Time	<time></time>	The time the report was generated.	Time format is YYY/MM/DD - HH:MM:SS and is in 24 hour clock format
Last Platform Sync time	<synctime></synctime>	The last time a platform synchronization was done before this report was generated.	Time format is YYY/MM/DD - HH:MM:SS and is in 24 hour clock format

Bundle Details

The bolded values below show where the Bundle details are found in the report.

Within the **<BundleDetailsList>,** each Service Provider bundle will be listed with its details which is contained in the **<BundleDetails>** tag.

```
<Billing>
    <ServiceProviderSnapshot>
        <BundleDetailsList>
            <BundleDetails>
                <allocated></allocated>
                <ALaCarteFeatures>
                    <phoneButtonManagement></phoneButtonManagement>
                    <chat></chat>
                    <knowledgeManagement></knowledgeManagement>
                    <launchpad></launchpad>
                    <miCollabClientForSmartPhones></miCollabClientForSmartPhones>
                    <presence></presence>
                    <presenceOnMitelSets></presenceOnMitelSets>
                    <compactMode></compactMode>
                    <softphone></softphone>
                    <sipmobile></sipmobile>
                    <rssWindow></rssWindow>
                </ALaCarteFeatures>
                <id></id>
                <licenseType></licenseType>
                <miteamEnabled></miteamEnabled>
                <name></name>
                <productCode></productCode>
                <serviceType></serviceType>
                <used></used>
            </BundleDetails>
        </BundleDetailsList>
        <CustomerSnapshotList>
            Customer details ...
        </CustomerSnapshotList>
        <ResellerSnapshot>
            Reseller details ...
        </ResellerSnapshot>
        <ServiceProviderLicenseDetails>
            Manual License details ...
        </ServiceProviderLicenseDetails>
    </ServiceProviderSnapshot>
</Billing>
```

General Bundle Details

The general bundle details are bracketed by the **<BundleDetails>** tag. Here are the details about each highlighted field:

Field name	Format	Description	Possible values
Allocated count	<allocated></allocated>	The total number of this bundle allocated across all customers.	integer
A la Carte Features	<ALaCarteFeatures> </ALaCarteFeatures>	The optional features allocated to a bundle.	See the table below for the list of all optional features.
Bundle Identifier	<id></id>	Unique Management Portal internal identifier	string
License Type	<licenseType></licenseType>	The UCC License Type this bundle is based on.	• Basic IPT • Standard IPT • Entry UCC • Standard UCC • Premium UCC
MiTeam Feature	<miteamEnabled></ miteamEnabled>	Indicates whether MiTeam is enabled for this bundle	• true • false
Bundle Name	<name></name>	The name assigned to the bundle by the Service Provider when the bundle was created	string
Product Code	<productCode></productCode>	The produce code assigned to the bundle by the Service Provider when the bundle was created. For bundles discovered during platform sychronization, this field will be empty.	string
Platform Service Type	<serviceType></serviceType>	What type of platform is this bundle targeted to. This is assigned when the bundle is created by the Service Provider.	• MiCloud Business Multi-tenant • MiCloud Business Virtual
Bundle Used Count	<used></used>	The total number of this bundle used across all customers	integer
Managed State	<managed></managed>	Indicates whether this bundle was created in Management Portal or discovered during platform synchronization.	• true • false

A la Carte Features

The A la Carte Features for each bundle are bracketed by the **<ALaCarteFeatures>** tag. Here are the details about each highlighted field within that tag:

Field name	Format	Description	Possible values
Phone Button Programming	<phoneButtonManagement></phoneButtonManagement>	Users can configure the buttons on their 6905, 6910, 6920, 6930, 6940, 5312, 5320, 5324, 5330, 5340, or 5360 IP phone from the Desktop Client. This feature is limited to users on MiVoice Business communication platforms only.	• 0 if this feature is not enabled • 1 if the feature is enabled
Chat	<chat></chat>	Users can participate in online chat sessions with other MiCollab Client users also licensed for chat. Users access the Chat submenu from the Corporate Contacts context menu.	• 0 if this feature is not enabled • 1 if the feature is enabled

Field name	Format	Description	Possible values
Knowledge Management	<knowledgeManagement></knowledgeManagement>	Users can index computer files and documents associated with a contact. When the user receives an incoming call, the Knowledge Management popup window appears presenting the user with a list of files associated with the caller including e-mail messages, contact entries, and documents (Microsoft Word, Excel® PowerPoint ®, Outlook and Adobe® Portable Document Format).	• 0 if this feature is not enabled • 1 if the feature is enabled
Launchpad	<launchpad></launchpad>	Users can access the Launchpad view, which provides quick access to frequently completed actions, from their Desktop Client. Actions include dialing a number, browsing to a URL, running a program, and exploring a folder.	• 0 if this feature is not enabled • 1 if the feature is enabled
MiCollab Mobile Client for Smart Devices	<miCollabClientForSmartPhones></miCollabClientForSmartPhones>	Users can install and use the MiCollab Mobile Client client application on their Android, BlackBerry, iPad, or iPhone mobile device. The MiCollab Mobile Client application provides Dynamic status updates based on location, time, WiFi, GPS and/or Bluetooth (depending on the device). The application also provides an integrated environment in which users can manage Dynamic Status, communicate with corporate contacts, and access visual voice mail and call history. The MiCollab Mobile Client for Smart Devices was formally known as the Locator.	• 0 if this feature is not enabled • 1 if the feature is enabled
Presence	<presence></presence>	MiCollab Client Service uses Dynamic Presence (which is a replacement for Universal and On-Demand Presence) for telephony presence. The Desktop client will display presence for the contacts in the current view.	• 0 if this feature is not enabled • 1 if the feature is enabled
Presence on Mitel Sets	<presenceOnMitelSets></presenceOnMitelSets>	Users can configure presence information for multiple contacts on their 5320, 5330, 5340, or 5360 IP phone from the Desktop Client. This feature is limited to users on MiVoice Business communication platforms only.	• 0 if this feature is not enabled • 1 if the feature is enabled
Compact Mode	<compactMode></compactMode>	Users can switch between the full mode and compact mode Desktop Client interfaces.	• 0 if this feature is not enabled • 1 if the feature is enabled
Softphone	<softphone></softphone>	Users' softphone extensions, as programmed on the PBX, are integrated with MiCollab Client.	• 0 if this feature is not enabled • 1 if the feature is enabled
Mobile SIP Softphone	<sipmobile></sipmobile>	Allows user to have SIP-Based Softphone on Android and iOS clients. This feature is supported on MiVoice Office 250 and MiVoice Business systems only	• 0 if this feature is not enabled • 1 if the feature is enabled

Field name	Format	Description	Possible values
RSS Window	<rssWindow></rssWindow>	Users have access to the RSS window, located at the bottom of the desktop client UI. Typically, RSS feeds provide syndicated content such as events listings, news stories, headlines, excerpts from discussion forums, or corporate information to the user. Depending on how you configure the RSS Window options for the user's account, users may be able to hide or display the RSS window and change the RSS URL.	• 0 if this feature is not enabled • 1 if the feature is enabled

Customer Details

The bolded values below show where the Customer details are found in the report.

Within the **<CustomerSnapshotList>,** each Service Provider customer will be listed with its details which is contained in the **<CustomerSnapshot>** tag.

```
<Billing>

    <ServiceProviderSnapshot>

        General information ...

        <BundleDetailsList>

            Bundle details ...

        </BundleDetailsList>

        <CustomerSnapshotList>

            <CustomerSnapshot>

                <accountNumber></accountNumber>

                <CustomerBundleDetails>

                    <BundleList>

                        <Bundle>

                            Same as the information shown for a Bundle in the Service Provider bundle list

                        </Bundle>

                    </BundleList>

                </CustomerBundleDetails>

                <CustomerDeviceDetails>

                    <DeviceList>

                        <Device>

                            <id>9</id>
                            <name></name>
                            <numberUsed></numberUsed>
                        </Device>
                    </DeviceList>
                </CustomerDeviceDetails>
                <CustomerDidDetails>
                    <numberAssigned></numberAssigned>
                    <numberUsed></numberUsed>
                </CustomerDidDetails>
                <CustomerHotDeskPhoneDetails>
                    <HotDeskPhoneList>
                        <HotDeskPhone>
                            <deviceName></deviceName>
                            <extension></extension>
                            <name></name>
                        </HotDeskPhone>
                    </HotDeskPhoneList>
                </CustomerHotDeskPhoneDetails>
                <CustomerSiteList>
                    <CustomerSite>
                        <primaryMcdName></primaryMcdName>
                        <secondaryMcdName></secondaryMcdName>
                        <siteId></siteId>
                        <siteInUse></siteInUse>
                        <siteName></siteName>
                    </CustomerSite>
                </CustomerSiteList>
                <CustomerUserDetails>
                    <UserList>
                        <User>
```

```
                    <bundleName></bundleName>
                    <deviceName></deviceName>
                    <extension></extension>
                    <firstName></firstName>
                    <lastName></lastName>
                    <licenseType></licenseType>
                    <productCode></productCode>
                    <siteId></siteId>
                    <siteName></siteName>
                    <username></username>
                </User>
            </UserList>
        </CustomerUserDetails>
        <customerVoiceMailDetails>
            <numberVoicemailboxesByAA></numberVoicemailboxesByAA>
            <numberVoicemailboxesByGroup></numberVoicemailboxesByGroup>
            <numberVoicemailboxesByUser></numberVoicemailboxesByUser>
            <totalnumberVoicemailboxes></totalnumberVoicemailboxes>
        </customerVoiceMailDetails>
        <name></name>
        <reportingStatus></reportingStatus>
        <time></time>
        <synctime></synctime>
    </CustomerSnapshot>
</CustomerSnapshotList>
<ResellerSnapshot>
    Reseller details ...
</ResellerSnapshot>
<ServiceProviderLicenseDetails>
    Manual License details ...
```

```
        </ServiceProviderLicenseDetails>

    </ServiceProviderSnapshot>

</Billing>
```

Customer General Information

The general information for each Customer are bracketed by the **<CustomerSnapshot>** tag. Here are the details about each highlighted field within that tag. Note that each customer is encased in their own **<CustomerSnapshot>** tag.

Field name	Format	Description	Possible values
Account Number	<accountNumber></accountNumber>	The number assigned to the customer by the Service Provider when the customer was created.	string
Bundle List	<CustomerBundleDetails> </CustomerBundleDetails>	All bundles assigned to a customer.	This tag contains a list of customer bundles. See the Customer Bundles detail table below.
Device List	<CustomerDeviceDetails> </CustomerDeviceDetails>	All devices in use by the customer	This tag contains information regarding the devices a customer uses. See the Customer Device details table below for more information.
DID Information	<CustomerDidDetails> </CustomerDidDetails>	Information regarding the DIDs in use by the customer.	See the Customer DID Details table below.
Hot Desk Phone List	<CustomerHotDeskPhoneDetails> </CustomerHotDeskPhoneDetails>	All hot desk phones in use by the customer	See the Customer Hot Desk Phone details table below.
Site List	<CustomerSiteList> </CustomerSiteList>	All Sites used by a customer.	See the Customer Site Details table below.
User List	<CustomerUserDetails> </CustomerUserDetails>	A list of all Users for that customer.	See the Customer User Details table below.
Voice mail details	<customerVoiceMailDetails> </customerVoiceMailDetails>	Voice mail details for the customer.	See the Customer Voice Mail details table below.
Customer Name	<name></name>	The customers name	string
Reporting Status	<reportingStatus></reportingStatus>	Determines whether license reporting is enabled for this customer	• Active • Inactive
Report Generation time	<time></time>	The time the report was generated.	Time format is YYY/MM/DD - HH:MM:SS and is in 24 hour clock format

Field name	Format	Description	Possible values
Last sync Time	<synctime></synctime>	The last time this customer had a successful sync.	Time format is YYY/MM/DD - HH:MM:SS and is in 24 hour clock format

Customer Bundle Details

The list of bundles allocated to each customer. The list is bracketed by the **<BundleList>** tag. Each bundle within the list is bracketed by the **<Bundle>** tag.

Field name	Format	Description	Possible values
Customer Bundle list	<BundleList></BundleList>	The list of bundles for the customer	A list of bundles bracketed by the <Bundle> tag.
Customer Bundle	<Bundle></Bundle>	Details on a specific bundle.	See the Bundle Details section/table that describes the list of Service Provider bundles. The same information type and format will be displayed here for the customer bundles

Customer Device Details

The list of devices used by the customer. The list is bracketed by the **<DeviceList>** tag. Each device within the list is bracketed by the **<Device>** tag.

Field name	Format	Description	Possible values
Customer Device list	<DeviceList></DeviceList>	The list of customer devices	For each device type, information on that device will be contained with a <Device> tag.
Customer device	<Device></Device>	Information describing one type of device assigned to the customer.	Each tag will bracket information on a particular device
Device Identifier	<id></id>	The Mitel Identifier for a device	string

Field name	Format	Description	Possible values
Device Name	<name></name>	The device name	• 5235 IP • 5224 dual mode • 5304 IP • 5312 IP • 5320 IP • 5324 IP • 5330 IP • 5340 IP • 5360 IP • 5212 dual mode • 5215 IP • 5220 dual mode • 5320e IP • 5330e IP • 5340e IP • 5610 SIP • 5603 SIP • 5604 SIP • 5607 SIP • 5610 SIP • 5624 SIP • 612 SIP DECT • 622 SIP DECT • 632 SIP DECT • 650 SIP DECT • 6905 IP • 6910 IP • 6920 IP • 6930 IP • 6940 IP • 6970 Conference Phone • Openphone 26/26 • 112 DECT
Used Count	<numberUsed></numberUsed>	The number of devices in use by the customer	integer

Customer DID Details

Information regarding the DIDs assigned to a customer.

Field name	Format	Description	Possible values
Assigned DID count	<numberAssigned></numberAssigned>	The number of DIDs assigned to a customer	integer
Used DID Count	<numberUsed></numberUsed>	The number of DIDs in use by the customer	integer

Customer Hot Desk Phone Details

The list of hot desk phones used by the customer. The list is bracketed by the **<HotDeskPhoneList>** tag. Each device within the list is bracketed by the **<HotDeskPhone>** tag.

Field name	Format	Description	Possible values
Customer hot desk list	<HotDeskPhoneList></HotDeskPhoneList>	The list of customer hot desk phones	For each hot desk phone, information on that phone will be contained with a <HotDeskPhone> tag.
Hot desk phone	<HotDeskPhone></HotDeskPhone>	Information describing one hot desk phone	Each tag will bracket information on one hot desk phone. There will be one for each hot desk phone.

Field name	Format	Description	Possible values
Extension	<extension></extension>	The extension of the hot desk phone	string
Name	<name></name>	The name assigned to the hot desk phone	string
Device Name	<deviceName></deviceName>	The device name	• 5235 IP • 5224 dual mode • 5304 IP • 5312 IP • 5320 IP • 5324 IP • 5330 IP • 5340 IP • 5360 IP • 5212 dual mode • 5215 IP • 5220 dual mode • 5320e IP • 5330e IP • 5340e IP • 6905 IP • 6910 IP • 6920 IP • 6930 IP • 6940 IP • 6970 Conference Phone

Customer Site Details

The list of sites used by the customer. Information for each site is bracketed by the **<CustomerSite>** tag.

Field name	Format	Description	Possible values
Customer Site	<CustomerSite></CustomerSite>	Each customer site is bracketed by this tag.	Each tag will bracket information on a particular site
Primary MiVoice Business Name	<primaryMcdName> </primaryMcdName>	The name of the primary MiVoice Business for the site.	string
Secondary MiVoice Business Name	<secondaryMcdName></ secondaryMcdName>	The name of the secondary MiVoice Business for the site.	string
Site Identifier	<siteId></siteId>	The identifier assigned to the site by the service provider	string
Site In Use state	<siteInUse></siteInUse>	Will show true if at least one user or group or mailbox is using the site.	• true • false
Site Name	<siteName></siteName>	The name assigned to the Site by the Service Provider	string
Managed state	<managed></managed>	If true, the site was created and is managed by Management Portal. If false, the site was discovered during a platform sync.	• true • false

Customer User Details

The list of users for this customer are bracketed within the **<UserList>** tag. Each user's data is contained within a **<User>** tag.

Field name	Format	Description	Possible values
User's Bundle	<bundleName></bundleName>	The name of the bundle assigned to the user	string

Field name	Format	Description	Possible values
User's Device	<deviceName></deviceName>	The name of the device assigned to the user	• 5235 IP • 5224 dual mode • 5304 IP • 5312 IP • 5320 IP • 5324 IP • 5330 IP • 5340 IP • 5360 IP • 5212 dual mode • 5215 IP • 5220 dual mode • 5320e IP • 5330e IP • 5340e IP • 5610 SIP • 5603 SIP • 5604 SIP • 5607 SIP • 5610 SIP • 5624 SIP • 612 SIP DECT • 622 SIP DECT • 632 SIP DECT • 650 SIP DECT • 6905 IP • 6910 IP • 6920 IP • 6930 IP • 6940 IP • 6970 Conference Phone • Openphone 26/26 • 112 DECT
User's extension	<extension></extension>	User's assigned prime extension	string
User's first name	<firstName></firstName>	User's first name	string
User's last name	<lastName></lastName>	User's last name	string
Number of Dids.	<numberOfDids></numberOfDids>	Number of DIDs assigned to the user. This does not include any external hotdesk numbers that the user may have.	string
User's License Type	<licenseType></licenseType>	The UCC license type assigned to the user	• Basic IPT • Standard IPT • Entry UCC • Standard UCC • Premium UCC • Contact Center Agent
User's Bundle Product code	<productCode></productCode>	The product code of the user's bundle	string
User's site id	<siteId></siteId>	The Identifier of the site assigned to the user	string
User's site name	<siteName></siteName>	The name of the site assigned to the user	string
User's username	<username></username>	The user's username	string
Managed status	<managed></managed>	If true, the user was created and is managed by Management Portal. If false, the user was discovered during a platform sync.	• true • false

Customer Voicemail Details

Information about the voice mailboxes used by this customer. This data is bracketed by the **<customerVoiceMailDetails>** tag.

Field name	Format	Description	Possible values
Auto Attendant Voice mailbox count	<numberVoicemailboxesByAA> </numberVoicemailboxesByAA>	The number of mailboxes used by the auto attendant for that customer	integer
Group Voice mailbox count	<numberVoicemailboxesByGroup> </ numberVoicemailboxesByGroup>	The number of mailboxes used by the groups for that customer	integer
User Voice mailbox count	<numberVoicemailboxesByUser> </ numberVoicemailboxesByUser>	The number of mailboxes used by the users for that customer	integer
Total Voice mailbox count	<totalnumberVoicemailboxes> </totalnumberVoicemailboxes>	The total number of mailboxes for that customer	integer

Reseller Details

The reseller details will list all Value-Added Resellers and Virtual Service Providers for the Service Provider.

The list of Value-Added Resellers are bracketed within the **<ValueAddedResellerSnapshotList>** tag with data for each value added reseller bracketed by the **<ValueAddedResellerSnapshot>** tag. All data within these tags, meaning bundles, customers, etc, is formatted the same as the data is for the service provider and the description will not be duplicated here.

The list of Value-Added Resellers are bracketed within the **<VirtualServiceProviderSnapshotList>** tag with data for each value added reseller bracketed by the **<VirtualServiceProviderSnapshot>** tag. All data within these tags, meaning bundles, customers, etc, is formatted the same as the data is for the service provider and the description will not be duplicated here.

```
<Billing>

    <ServiceProviderSnapshot>

        General information ...

        <BundleDetailsList>

            Bundle details ...

        </BundleDetailsList>

        <CustomerSnapshotList>

            Customer details ...

        </CustomerSnapshotList>
        <ResellerSnapshot>
            <ValueAddedResellerSnapshotList>
                <ValueAddedResellerSnapshot>
                    All the same information and in the same format with the same tags as for a Service Provider,
                    meaning all bundles, customers, etc
                </ValueAddedResellerSnapshot>
            </ValueAddedResellerSnapshotList>
            <VirtualServiceProviderSnapshotList>
                <VirtualServiceProviderSnapshot>
                    All the same information and in the same format with the same tags as for a Service Provider,
                    meaning all bundles, customers, etc
                </VirtualServiceProviderSnapshot>
            </VirtualServiceProviderSnapshotList>
        </ResellerSnapshot>
        <ServiceProviderLicenseDetails>
            Manual License details ...
        </ServiceProviderLicenseDetails>
    </ServiceProviderSnapshot>
</Billing>
```

Manual License Details

This section of the report will list all the manually entered license information that were specified on the Edit Licensing page. The list is bracketed by the **<ManuallyEnteredLicensesList>** tag. Each license within the list is bracketed by the **<ManuallyEnteredLicensesDetails>** tag.

Field name	Format	Description	Possible values
License description	<description> </description>	Management Portal provided description of each license	• MIVOICE_SFDC_ADV • SCREEN_RECORDING • MITEL_CRM_PRO • REPORT_EXTENSION • NPM_TTS • BR_X50 • BA_PRIVATE_CLOUD • INSIGHT_EXTENSION • HOSPITALITY • OIG_GOOGLE • ACD_AGENT • NPM_SAA_CORP_DIR • MICOLLAB_PORT • OIG_SFDC • ANALOG_ONS • NPM_FAX • MIVOICE_BUSINESS_CONSOLE • BR_CLIENT_X1 • MBG_SIP_TRUNK • CALL_RECORDING • SPEECH_SEARCH • MITEL_CRM_PREMIUM • CALL_ACCT_EXTS • SRC • MICOLLAB_CONSOLE • VOICE_MAILBOX • QUALITY_MONITORING • MITEL_CRM_BASIC • IVR_STD_PORTS • MICLOUD_CC_IVR • MICLOUD_CC_AGENT • _CC_SOFTPHONE • STD_AGENTS • ADV_AGENTS • MICLOUD_CC_MULTIMEDIA_AGENT • IVR_PREM_PORTS • BASIC_AGENTS • MICLOUD_CC_MULTITENANT_AGENT • PREM_AGENTS • WFS_STANDARD_X1 • Entry UCC • Standard IPT • Basic IPT • Contact Center Agent • Premium UCC • Standard UCC • UC_TELEWORKER • Softphone • Mobile Sip
License Type	<licenseType> </licenseType>	Type of License	• MIBUSINESS • MICONTACT • M2CLOUD • UCC_LICENSE • MW_UCC_LICENSE • MW_ALACARTE

Field name	Format	Description	Possible values
Part Number	<partnumber> </partnumber>	The part number of the license	string
License count	<usageCount> </usageCount>	The total number used. This number was entered on the Edit Licensing page.	integer

Configure Reports

Choose the license model

Choose either the operating expenditure (OPEX) or capital expenditure (CAPEX) license model.

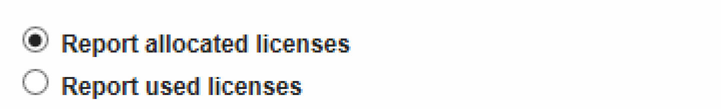
To choose the license model for reporting:

1. Click **Customers > Billing**.
2. Click **Configure**.
3. Select **Opex** or **Capex**.
4. Click **Save**.

Choose the license counts to report

You can select the type of license counts to include in reports.

Note: Because registered platform groups count the billing only, user licenses created in Management Portal are not included in the billing reports.



● Report allocated licenses

○ Report used licenses

To choose the type of license counts to report:

1. Click **Customers > Billing**.
2. Click **Configure**.
3. Select **Report allocated licenses** or **Report use licenses**.
4. Click **Save**.

Schedule reports

Schedule reports to run at specific intervals so that they are ready when you need them. After a report is run, it is available in the Download Reports tab.

To schedule a report:

1. Click **Customers > Billing > Configure**.
2. Click **Enable Scheduled Reporting**.

3. Choose the frequency, day, and start time for generating the reports.
4. Choose whether to "Perform data synchronization before report generation". If chosen, the system will synchronize data from the customer platforms before generating the report. If synchronization is performed before report generation, a sync report will be created and it can be downloaded from the "Sync Reports" tab.
5. Click **Save**.

Restart the scheduler

You can restart the billing scheduler in two ways; reconfigure the schedule for a new time or interval or restart the scheduler through a maintenance command.

Issue this maintenance command to restart the billing scheduler using the current configuration:

```
$$RESTART_BILLING_SCHEDULER$$
```

Note: If this command is run and scheduling is not enabled, the command has no effect.   You may want to use this maintenance command when the server time changes for some reason (for example, daylight savings time)

Specify a billing number for a site

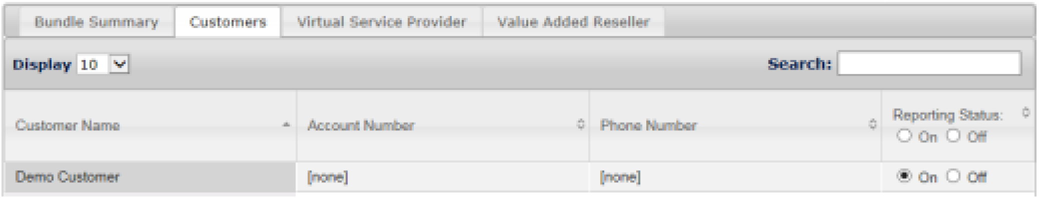
If you have multiple sites with separate billing, you can specify a billing number on a per-site basis. After you add the site billing number, it is included in billing and licensing reports.

To specify a billing number for a site:

1. Click **Platforms > Platform Groups**.
2. Select the platform group and click **Edit**.
3. Click the **Sites** tab.
4. Click the **Edit** icon for the site you want to add the billing number.
5. In the **Site ID** field, enter a number to identify the site in billing reports.
6. Click **Save**.

Turn off license reporting

Turn license reporting on or off through the Customers tab in Billing.



Customer Name	Account Number	Phone Number	Reporting Status: ○ On ○ Off
Demo Customer	[none]	[none]	● On ○ Off

To turn off license reporting for a customer:

1. Click **Customers > Billing** and then click the **Customers** tab.
2. In the table, find the customer, go to the **Reporting Status** column and select **On** or **Off**.
3. Click **Save**.

Synchronize Billing Report Data

Synchronizing data from the MLB customer platforms allows for more accurate billing counts. Synchronizing discovers bundles, devices and users that were created, modified or deleted directly on customer platforms.

There are two ways to synchronize billing report data; as part of the scheduled billing report generation or on-demand from the Billing page. The date of the last completed data synchronization is displayed on the Billing page. All billing reports generated, on-demand or scheduled, use the data from the last completed synchronization.

Data synchronization is performed in the background and is expected to take a long time if there are a lot of customers to collect data from. The "Tasks" in progress icon at the top of the page indicates when the synchronization is complete.

Each time data is synchronized a sync report is generated. This report states the time it took to perform the sync and lists any customers that Management Portal could not synchronize because the sync could not communicate with their platforms to collect data.

Bundles that are discovered as part of the sync are displayed on the Billing page in the Bundle Summary tab. Bundles, devices and users discovered as part of the sync are used in the billing reports.

On-demand Synchronization

To synchronize billing report data:

1. Click **Customers > Billing**.
2. Click the **Synchronize Now** button

Note: If there is no **Synchronize Now** button, you may see "Synchronization in progress..." instead because there is a sync in progress and only one can run at a time.

Generate reports

Service provider subscription usage report

You can generate subscription reports and system reports from the Management Portal The Service Provider Subscription Usage Report is an .xls formatted subscription report for the system. The report contains a summary of the licenses in use and the counts manually entered in the editable fields. The subscription usage report is only available for service providers and includes monthly subscription usage for:

- MiCloud Business
- MiCloud Contact Center
- Premium Software Assurance (optional)
- MiCloud Business Move2Cloud (optional)

Service provider license report

The service provider license report is an .xml formatted report that contains a summary of the system licenses in use. The license counts are derived from the Management Portal database and manually entered values.

Customer VSP and VAR allocation and usage reports

A report that provides a billing summary for Customers, Virtual Service Providers (VSP), and Value Added Resellers (VAR). It contains Customer details and a summary of their bundle allocation and usage. The billing information is downloadable in .xml format for use in a compatible billing system.

View Bundles Allocated

The portal tracks how many bundles each customer has been allocated, and of those, how many bundles are currently being used. To view the bundle usage information, follow the steps listed below.

To view how many bundles a customer is using:

1. Click the **Customers** tab.
2. Select the customer profile.
3. In the customer's popup there is a list of the bundles allocated and used by the customer.

Optional license counts for premium software assurance and Move2Cloud

The optional license counts for Premium Software Assurance and Move2Cloud are derived from the number of Core UCC license types that the service provider has in use.

Premium Software Assurance

When the Premium Software Assurance option is enabled, the system reports indicate a Premium Software Assurance license equal to the actual number of each of the Core UCC license types. For example, if a service provider has 250 Entry UCC licenses in use, there will be 250 Premium Software Assurance Entry UCC licenses reported. If Premium Software Assurance is disabled, the license count for each Premium Software Assurance license type is 0.

Move2Cloud and Core UCC Licenses

You can manually enter the number of UCC licenses to include in Mitel’s Move2Cloud promotion. The license counts for the Move2Cloud promotion are included in the system level .xls and .xml reports. To prevent double counts, the Move2Cloud licenses are subtracted from the Core UCC license counts when they are reported. So the number of Move2Cloud licenses for a given type cannot exceed the corresponding number of Core UCC licenses.

For example, Management Portal calculates that you are using 500 Standard IPT licenses. If you want 300 under the Move2Cloud promotion, enter 300 for the license count field for Move2Cloud Standard IPT field. Management Portal reports 200 Standard IPT licenses for UCC core and 300 Move2Cloud Standard IPT licenses.

Download reports

You can download generated billing reports at any time.

To download reports:

1. Click **Customers > Billing** and then click the **Download Reports** tab.
2. Click the report to download it.

Manually enter license information

You can manually enter the license counts that Management Portal does not automatically calculate in the Management Portal. The license counts that Management Portal does calculate from its database appear as read-only fields in the License Information page. Any counts that are manually entered in the editable fields are also stored in the Management Portal database.

To manually enter licensing information:

1. Select **Customers > Billing**.
2. Click the **Edit Licensing** link.
3. Edit the corresponding licenses and click **Save**.

Enable billing change notification

Billing change notification settings are available for Service Provider Administrators who hold Advanced privileges in the Service Provider Portal. The Billing Change Notification feature displays a warning message to Customer Administrators when the action they are about to take changes the Service Agreement with the Service Provider and increases billing. Billing change notification settings include a customizable default message.

When you create a new customer, billing change notification is disabled by default. When an existing customer is upgraded to Oria 5.2 and later, billing change notification is enabled by default.

Billing change notification is available for the following actions:

- Create a user
- Change a user bundle
- Create a group
- Create an auto attendant or auto attendant action
- Create a call flow
- Create a general mailbox

To set billing change notification:

1. Click **System > Advanced** and then click the **Billing Change Notification** tab.
2. Select the actions you want billing notification for.
3. Customize the billing notification message:
   a. Select the language for the message.
   b. Customize the message.
   c. Repeat **a.** and **b.** for any other language.
4. Click **Save**.

To change billing notification for a customer:

1. From the **Customers** tab, click **View Customers**.
2. Select the customer and click the **Edit** icon.
3. Click the **Service Bundles** tab.
4. Under **Billing Change Notification**, select or deselect **Customer must confirm any changes that will affect their billing**.

Maintain Management Portal

Here are the maintenance activities that need to take place on a regular basis:

- Back up and restore Management Portal
- Upgrade Management Portal
- Create a Service Provider Administrator user

Occasionally you may also need to do the following operations:

- Migrate Management Portal
- Move users from one MiCollab platform to another

Back up and restore Management Portal

There are two backup methods available to back up the Management Portal database, depending on your needs:

- MSL backup
- Management Portal backup

> **Caution**
> The above backup methods are not compatible with each other. An MSL Backup can only be restored using the MSL Restore capability. A Management Portal backup can only be restored using the Management Portal database restore capability.

Both offer complete backups but the MSL Backup offers the advantage of automated scheduled backups. The Management Portal Backup method is useful for software migrations and when a database needs to be sent to Mitel support.

MSL backup and restore

An MSL backup is a complete representation of an MSL server at the time of backup. It includes MSL and the application databases. It does not include any of the software application blades installed on MSL. This means that if a new system needs to be restored, MSL, the backup-file, and the Management Portal Blade will need to be installed. An MSL backup may be restored to an existing system without reinstalling MSL or Management Portal (restoring a database that originated or a greater version of Management Portal than the restore target will result in system failure).

To schedule automatic MSL backups:

Scheduled MSL backups use the network file server option from with the MSL Server Manager.

> ⚠ **Note**
> This procedure also backs up all application data through the MSL backup feature. Performing a separate backup of the Management Portal database may not be necessary, depending on local administration/maintenance protocols.

1. Log in to the MSL Server Manager using a supported browser with the user name and password when initially configuring the MSL server.
2. Under Administration, click **Backup**.
3. From the Select an action drop-down list, click **Configure network backup**.
   Note: Selecting the Backup to Desktop option will back up the data to the local workstation. Scheduled backups cannot be performed with this option.
4. Click **Perform**.
5. In the **Backup Server Configuration** area, configure the server where the backup file will be stored:
   In the IP Address field, enter the IP address of the file server where the backup will be stored.
   In the **Sharename** field, enter the name of the shared folder where the backup file will be stored. (For example, "Backups".) The shared folder must have permissions set to "Full Control".
   In the **Username** field, enter the username to use when connecting to the backup server.

In the **Domain or Workgroup Name** field, enter the domain or workgroup name of the server. (For example, mitel.com.)
In the **Password** field, enter the password to use when connecting to the backup server. Available storage space is displayed.

6. In the **Maximum number of backup files to keep** field, enter the maximum number of backup files to keep (1-999) on the server (default is 5). When the number of stored files reaches this maximum count, the oldest version is deleted.
7. In the **Backup Schedule** area, select the frequency with which to perform backups (Daily, Weekly, Monthly, Never). Backup file names will include timestamps in the format: mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz)
   For Daily backups, select a time of day (hour, minute, AM/PM)
   For Weekly backups, select a time of day, and day of the week
   For Monthly backups, select a time of day, and day of the month
   To disable regularly scheduled backups, click Disabled.
8. To test the backup configuration, or to run an immediate backup, click **Backup Now**.
9. Click **Save** to save the schedule information.

See the *Mitel Standard Linux Installation and Administration Guide* for additional information.

Restore the Management Portal database from an MSL backup

You need the following information and equipment to restore a database:

- Installer PC
- MSL system IP address
- MSL Server Manager username and password

There are two methods for restoring the Management Portal database from an MSL backup:

- Use the "Restore" option when re-installing MSL.
- Use the Command Line Interface by logging in to the MSL Server Console and select the "Restore from backup" option. See the Mitel Standard Linux Installation and Administration Guide for details.

Caution
You must restart the Management Portal application after restoring a database. Service will be LOST during this reboot.

To update the Management Portal database with MiCollab version using maintenance command

- Login to the Management Portal service provider portal (http://xx.xx.xx.xx/konos/sp/spLogin.do). Replace xx.xx.xx.xx with the Management Portal server IP address or FQDN.
- Enter this URL in the same active service provider browser session (https://xx.xx.xx.xx/konos/commands.jsp) Replace xx.xx.xx.xx with the Management Portal server IP address or FQDN. This will open up the Management Portal Service Provider maintenance command window.
- Run the following maintenance command:

```
updateMasVersion <host IPAddress>
```

Upgrade Management Portal

Follow these steps to upgrade from a minimum of Oria 4.0.275 to Management Portal. Make sure that you upgrade from the latest MiCloud Management Portal support build. Contact product support for the latest patch release. See the latest release notes for details. If you are upgrading from an earlier release of Management Portal, for example Oria 3.0, contact Mitel Professional Services for assistance.

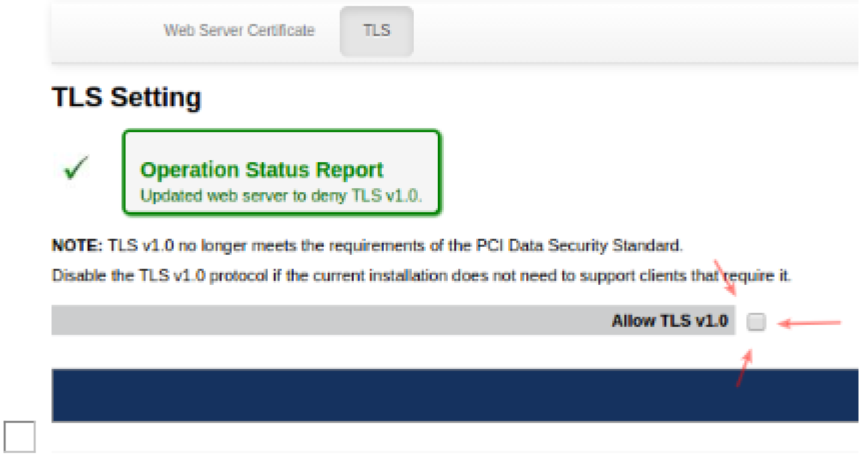
⚠ To manage the platform from Management Portal, you must first migrate the platform and users. See Migrate Management Portal.

⚠ If you are using system speed call, you must migrate to DID services using the Management Portal migration outlined in Management Portal before migrating.

Important: TLS 1.0 has been found to be vulnerable to a number of security attacks. As such, Management Portal disables support for TLS 1.0 by default. Mitel does not recommend using TLS v1.0. However, should you need to enable support for TLS v1.0, login to the MSL server manager for the server at:

[http://<address]http://<address of Oria server>/server-manager,

go to **Security > Web Server > TLS** and select **Allow TLS v1.0**.



TLS Setting

✓ Operation Status Report

Updated web server to deny TLS v1.0.

NOTE: TLS v1.0 no longer meets the requirements of the PCI Data Security Standard.

Disable the TLS v1.0 protocol if the current installation does not need to support clients that require it.

Allow TLS v1.0 □

When you upgrade to MiCloud Business 4.1, MiCollab Teleworker services are removed.

Upgrade on a Physical Server (Oria 5.0 or 5.1 or 5.2 or 5.3 to Management Portal 6.0 or 6.1)

Note: After an upgrade, all Management Portal history is removed. For example, Active Directory and Bulk Import history.

Step 1 Prepare for the upgrade:

1. Order a Management Portal license.
2. Make sure that the Management Portal server has Internet access to perform a DNS lookup and for access to port 22 of Mitel AMC.
3. Test access to AMC:
   a. ssh to the Management Portal server and login at root level using the same password as admin.
   b. Ping sync.mitel-amc.com and register.mitel-amc.com
   c. If no IP address is resolved, check the DNS.
4. When the Management Portal license is available in AMC, create a new Management Portal ARID and apply the license to it.

Step 2 Perform a Management Portal backup:

1. Log into the current Management Portal server using Server Manager.
2. Perform a backup to the desktop.
3. In the **Status** panel, register the server with the ARID created earlier.

Step 3 Upgrade the MSL blade to 10.5 or 10.6 version (see release notes for the latest compatible version):

If you want to upgrade the MSL blade to 10.5 for Management Portal 6.1, use the build 6.1.1.xx or 6.1.2.xx).
If you want to upgrade the MSL blade to 10.6 for Management Portal 6.1, use the build 6.1.3.xx or 6.1.4.xx).

1. In **Server Manager**, go to the blades **Blades** panel.
2. Upgrade the MSL blade.
3. Clear the report after the upgrade.
4. Reboot server from Reconfigure tab in Server Manager. Wait until the server is restarted.

Step 4 Upgrade Management Portal:

1. In **Server Manager**, go to the blades **Blades** panel.
2. Upgrade the Management Portal blade. Wait until the upgrade is finished.
3. Clear the report and ensure that there are no more upgrades listed.
4. Update the default Management Portal password on first access.

Upgrade on a Physical Server (Oria 4.0.275 to Management Portal 6.0 or 6.1)

Step 1 Prepare for the upgrade:

1. Order a Management Portal license.
2. Make sure that the Management Portal server has Internet access to perform a DNS lookup and for access to port 22 of Mitel AMC.
3. Test access to AMC:
   a. ssh to the Management Portal server and login at root level using the same password as admin.
   b. Ping sync.mitel-amc.com and register.mitel-amc.com
   c. If no IP address is resolved, check the DNS.
4. When the Management Portal license is available in AMC, create a new Management Portal ARID and apply the license to it.

Step 2 Perform a Management Portal backup:

1. Log into the current Management Portal server using Server Manager.
2. Perform a backup to the desktop.

Step 3 Upgrade the MSL blade to 10.5 or 10.6 version (see release notes for the latest compatible version):

> ⚠ If you want to upgrade the MSL blade to 10.5 for Management Portal 6.1, use the build 6.1.1.xx or 6.1.2.xx).
> If you want to upgrade the MSL blade to 10.6 for Management Portal 6.1, use the build 6.1.3.xx or 6.1.4.xx).

1. Place the CD in the server optical drive.
2. Boot from the appropriate drive, and select the **Upgrade** option during the installation process.

Step 4 Upgrade Management Portal:

1. Place the CD in the optical drive.
2. Login into the Server Manager using a supported browser with the user name 'admin' and the root password you gave when configuring the MSL server. The Server Manager is accessed by entering the following URL: *http://<www.hostname> OR <IP address of the MSL Server>/server-manager*.
3. Click on **Blades**, located in the left-side panel under the ServiceLink heading.
4. Click **Update List** to ensure an up-to-date listing of software blades.
5. Click the **Install** link, located beside the Management Portal blade name. It may take a few minutes for the software to install.
6. Test the installation:
7. Click Management Portal, located in the left-side panel under the **Applications** heading.
8. If Management Portal is not visible, refresh the browser.
9. Click **Launch**, located in the main window.

Step 5 Register the server with the ARID:

- In the **Status** panel, register the server with the ARID created earlier.

Step 6 Run the Management Portal post-upgrade maintenance commands:

1. Login to the Management Portal service provider portal (http://a.b.c.d/konos/sp/spLogin.do). Replace a.b.c.d with the Management Portal server IP address or FQDN.
2. Enter this URL in the same active service provider browser session (https://a.b.c.d/konos/commands.jsp) Replace a.b.c.d with the Management Portal server IP address or FQDN. This will open Management Portal Service Provider maintenance command window.
3. Run the following commands in the Management Portal Service Provider portal to enable features in the Customer Administrator portal: (run again?)
   In the command field, enter the following commands individually and click on Submit after each command. Replace custId1 with the assigned customer WebID in Management Portal.
   ```
   $$GET BUSINESS HOURS$$ custId1
   $$GET SUPERVISED TRANSFER$$ custId1
   $$SET FACS$$ custId1
   ```
   To issue the commands for multiple customers, run these commands:
   ```
   $$GET BUSINESS HOURS$$ custId1, custId2
   $$GET SUPERVISED TRANSFER$$ custId1, custId2
   $$SET FACS$$ custId1, custId2
   ```
   To apply the commands to all customers in the Management Portal database, run these commands:
   ```
   $$GET BUSINESS HOURS$$ ALL
   $$GET SUPERVISED TRANSFER$$ ALL
   $$SET FACS$$ ALL
   ```
   Any customer that is using MiVoice Business (MiVB) is upgraded as part of the MiCloud Business 3.2 to MiCloud Business 4.0 upgrade. To update MiVB versions, go to the Management Portal Service Provider maintenance command window and run the following command: `$$UPDATE MCD VERSION$$ CUSTOMER, custId`
   See the — *Migrate to MiCloud 3.2 Flow Through Provisioning* section if you upgraded from MiCloud Business 3.1 to MiCloud Business 3.2. (applies if upgrading from MiCloud Business 2.0 - include in procedure 2)

Upgrade on a Virtual Machine

For virtual deployments in a VMware environment, MSL software is packaged with the application software and delivered as an OVA file which can be installed on a vSphere client using the Deploy OVF Template wizard.

> ⚠ If you are upgrading MiCollab and Management Portal to MiCloud Business 2.0 from a previous version, feature profiles will not automatically be created on MiCollab. To create the feature profiles on MiCollab, you must edit and save the customer and Management Portal will create the Feature Profiles on the MiCollab Client.

Users are not created from the old Standard IPT bundle when you upgrade to Micollab Version 7.1 and up. To be able to add the users, you must manually update the Record ID on MiCollab in the location where IPT licenses are added.

Optionally you can follow the same upgrade process as the physical server upgrade with the following exception:

Upgrade the MVF blade after the MSL upgrade before the reboot.

> ⚠ After an upgrade, all Management Portal history is removed. For example, Active Directory and Bulk Import history.

Step 1 Back up the virtual machine instance:

1. In the vSphere client, right-click the virtual appliance name and select Shutdown Guest.
2. Click File > Export > Export OVF Template.
3. Enter the name of the OVF template file and the directory where you want to save it.
4. Select one of the following options:
   Physical Media (OVA): to export a single .ova file (recommended)
   Web: exports multiple files

5. Select one of the following Format options:
   Single File (OVA): to export a single .ova file (recommended)
   Folder of Files (OVF): exports multiple files
6. Click OK. MSL automatically configures the NIC address for the new virtual machine.

Step 2 Perform a full MSL backup:

1. Log in as "admin".
2. Access the server console from the server itself or remotely using an SSH client.
3. From the console, select the option to Perform backup.
4. Select a destination to store the backup, for example, your desktop or local network file server.
5. If backing up to a local network file server do the following:
   Enter the IP address of the file server where the backup will be stored.
   Enter the domain or workgroup name of the server. For example, mitel.com.
   Enter the name of the shared folder where the backup file will be stored. (For example, "Backups".) The shared folder must have permissions set to "Full Control".
   Enter the Optional Directory Path where the backup will be stored. If you leave this field blank, the file will be stored at the root of the shared folder.
   Enter the username to use when connecting to the backup server. Enter the password to use when connecting to the backup server. The estimated backup size and available storage space are displayed.
6. Click **Proceed**. When the backup is complete, file verification is performed automatically.
7. Click **Continue**.

Step 3 Deploy the Management Portal Virtual Appliance:

The .ova file you downloaded from **Mitel Connect** > **Downloads** contains the MSL operating system, the application software, and VMware Tools (a suite of utilities to enhance performance).

1. Launch the vSphere Client on the network PC:
   Click **Start** > **All Programs**.
   Click **VMware** > **VMware vSphere Client**.
   Enter the IP address or hostname of the Hypervisor ESX/ESXi Host server OR enter the IP address or hostname of the vCenter Server.
   Enter your username and password.
   Click **OK**.
2. In the vSphere Client application, click **File** > **Deploy OVF Template**. (The .ova file you downloaded is a template file in OVF format.)
3. In the **Deploy OVF Template** screen, specify the storage location of the .ova file you downloaded.
4. Specify the Source Location for the OVF template file (.ova file extension):
   To deploy from a file on the local PC or from a network share, click Browse and navigate to the file.
   To deploy from a URL (if the file is on the Internet or is accessible through a web browser) enter the URL of the file location.
5. Click **Next**. The OVF Template Details screen appears. The information shown is derived from the .ova file to provide a “check” for the correct application and version. Note that the Download size is only an estimate until a deployment configuration is selected later in the process.
6. Click **Next**.
7. Click **Accept** to accept the end-user license agreement, and then click **Next**.
8. Enter a meaningful name for the virtual appliance, or accept the default name, and then click **Next**.
9. Click **Next**. The following three steps are dependent on your configuration.
   If you are using the optional vCenter Server, select the appropriate Host/Cluster for this deployment and then click **Next**.
   If you are using the optional vCenter Server, select the appropriate Resource Pool for this deployment and then click **Next**.
   If multiple Datastores are available, select the Datastore for the vNuPoint instance, and then click Next.
10. In the **Disk Format** screen, select **Thick provision Lazy Zeroed**.
11. Click **Next**.
12. Configure the network mapping. (This screen is only displayed if the network defined in the OVF template does not match the name of the template on the host to which you are deploying the virtual application.) If required, contact your Data Center administrator for more details on which Network Mapping to use. The required settings are:
    Application: Select **Restore from backup**.
    LAN: Enter the IP Address, LAN Netmask, and Default Gateway Address.
    Note: If you want to use the IP Address of your existing Management Portal server, ensure that it is shut down. If not, the new

updated Management Portal server will detect an IP conflict, and disable its network interface, until the original Management Portal server is off the network.

13. Click **Next**. The Deploy OVF Template Ready to Complete screen appears.
14. Review the information and then click **Finish**.
15. When the deployment is complete, click **Close**. The new virtual machine appears in the inventory list in the left-hand pane.
16. Select the new virtual machine and power up the virtual machine.
17. Open the virtual machine console.
18. When the system prompts you with "Do you wish to restore from backup?", click **Yes**. The MSL console will present 3 choices of Upgrade. **DO NOT** choose "Restore from Running server". Choose one of the other options to retrieve your Management Portal Backup file, into this new Management Portal server. After you have restored the Management Portal MSL Backup, you will be prompted to Reboot. Again, ensure that the original Management Portal (with the same IP address as this updated Management Portal), is shut down before booting up the new restored Management Portal server.
    Note: The Management Portal Service Provider Portal may not be available immediately after the MSL Server Manager is available. It may take a few minutes for all of the Management Portal Services to start.
19. Select **Restore from Network Server**. You will be prompted to select a network interface to use for the restore (LAN or WAN), the address and netmask of the local MSL server, the address, gateway and domain name of the backup server, the folder name containing the backup file, and the username and password required to log in to the backup server.
20. Use VSphere, or VCentre to change the virtual machine memory allocation to 8GB.
21. When the restore is complete, select **Reboot**.

> ⚠ If you want to use the IP Address of your existing Management Portal server, ensure that it is shut down. If not, the new updated Management Portal server will detect an IP conflict, and disable its network interface, until the original Management Portal server is off the network.

Step 4 Apply the Management Portal ARID and sync with the AMC:

1. Make sure you have created the Management Portal ARID on the AMC.
2. Apply the Management Portal ARID in MSL Server Manager.
3. Synchronize to the AMC.

Step 5 Run the Management Portal post-upgrade maintenance commands:

1. Login to the Management Portal service provider portal (http://a.b.c.d/konos/sp/spLogin.do) <<replace a.b.c.d with the Management Portal server IP address or FQDN>>
2. Enter this URL in the same active service provider browser session (https://a.b.c.d/konos/commands.jsp) <<replace a.b.c.d with the Management Portal server IP address or FQDN>> This will open the Management Portal service provider maintenance command window.
3. In the command field, enter the following commands individually and click on Submit after each command. Replace custId1 with the assigned customer WebID in Management Portal.
   ```
   $$GET BUSINESS HOURS$$ custId1
   $$GET SUPERVISED TRANSFER$$ custId1
   $$SET FACS$$ custId1
   ```
   To issue the commands for multiple customers, run these commands:
   ```
   $$GET BUSINESS HOURS$$ custId1, custId2
   $$GET SUPERVISED TRANSFER$$ custId1, custId2
   $$SET FACS$$ custId1, custId2
   ```
   To apply the commands to all customers in the Management Portal database, run these commands:
   ```
   $$GET BUSINESS HOURS$$ ALL
   $$GET SUPERVISED TRANSFER$$ ALL
   $$SET FACS$$ ALL
   ```
4. Follow the steps in — *Migrate to MiCloud 3.2 Flow Through Provisioning* if you upgraded from MiCloud Business 2.0 to MiCloud Business 3.2.

Migrate to MiCloud 3.2 flow through provisioning

Any customer that is using MiVoice Business (MiVB) is upgraded as part of the MiCloud Business 2.0 to MiCloud Business 3.2 upgrade.

After the upgrade you may need to clear your browser cache memory for example, when performing a task such as creating or changing a bundle. To clear your browser cache do one of the following:

1. (preferred) Force reload the page (usually by pressing: CTRL + F5).
2. Clear browser cache.
3. Reboot Management Portal.

To update MiVB versions, go to the Management Portal Service Provider maintenance command window and run the following command:

```
$$UPDATE MCD VERSION$$ CUSTOMER custId
```

If you upgraded the platforms from MiCloud 2.0 to a MiCloud 3.2, run ONE of the following commands:

Note: Make sure that you run the command BEFORE switching the configuration from FQDN to IP (The FDQN is used to also update any MiVB references in corresponding MBGs). If the FQDN is changed before running the command, the administrator will have to go directly into the MBGs and change the MiVB reference from FQDN to IP.

NAT: Run the following maintenance command for moving from an FQDN to an IP address which is required with MiCloud 3.2 flow through provisioning.

- `$$UPDATE MCD CUSTOMER HOST NAME$$ <Management Host Name IP Address>, <New Customer Host Name>`

For example:

```
$$UPDATE MCD CUSTOMER HOST NAME$$ mmg.fqdn1.public.com, 192.168.20.1
```

non-NAT mode: Change the Host Name from FQDN to an IP address. In non-MMG, there is no Management and Customer Host Names, just one Host Name for the MiVB configuration (in MiVoice Business tab in the Platform Groups UI).

Use this maintenance command to change the Host Name from FQDN to an IP address:

- `$$UPDATE MCD HOST NAME$$ <Existing Host Name FQDN/IP Address>, <New Host Name>`

For example:

```
$$UPDATE MCD HOST NAME$$ fqdn1.com, 10.168.20.1
```

Verify that the command was successful by viewing the MiVoice Business tab in Platform Groups for the corresponding MiCollab platform.

Migrate Management Portal

After you upgrade Management Portal, perform the Migrate Platform task for each customer. Management Portal keeps track of the last configuration it programmed for a user. This information is used to determine whether a user's information has changed. To determine whether a user is unmanaged, Management Portal compares its view of the user with the MiCollab view of the user. The same comparison is made with partially managed users.

During the migration, Management Portal reads each user profile from MiCollab, makes a copy of the profile, uses the copy to compare it against the Platform Manager profile, and determines whether the user is unmanaged.

Because a migration involves so many steps, it may take a while to migrate all users. Make sure that you allow a maintenance window when migrating users as the process may take about 2 seconds per user.

⚠ The following tasks are performed prior to the Platform Migration:

- Run the MiCollab reconcile wizard on MiCollab.
- Ensure there are "No SDS Errors" on MiCollab platform.

To migrate Management Portal:

1. From the **Customers** tab, click **View Customers**.
2. Select the customer and click the **Edit** icon.
3. In **Customer Details > Platform migration required box**, click **Migrate Platform**.
4. Click **Save**.

Move users from one MiCollab platform to another

When a customer's business needs have grown beyond the maximum user capacity of a single MiCollab platform (Medium to Large business), you can scale up by adding more MiCollab platforms to a MiVoice Business cluster. Here are instructions on how to move users from an existing MiCollab to another MiCollab. Contact Mitel Professional Services for help in moving users from one MiCollab Platform to another.

Migrate MiVoice Business Express to MiCollab and MiVoice Business

Refer MiVoice Business Express Migration Guide to vMiVB and vMiCollab to migrate MiVoice Business Express to MiCollab and MiVoice Business.

Create a Service Provider Administrator user

You can create Service Provider Administrator in **Systems > Administrators** tab. After the Service Provider Administrator is created, you can edit and reset the password.

To reset the password

1. From the **Service Provider's Portal**, click **System** tab.
2. Select **Administrators**.
3. Click on the name of the administrator.
4. Click **Edit** icon which is on the top right.
5. Under the **Details** tab, enable the **Reset Password** checkbox.
6. Click **Save**.

⚠ The **Reset password** checkbox is not visible for default admin **SYSTEM**.

Prerequisite of using Reset password feature for Admins

To use reset password feature, create an Administrator Email template and assign the template to a new administrator.

To create an Administrator Email Template

1. From the **Service Provider's Portal**, click **System > Email Template**.
2. Click **Create Email Template**.
3. Select **Administrator Template**.
4. Click **Next**.
5. Enter the required details.

6. Click **Submit**.

To assign Administrator Email template to a new admin

1. From the **Service Provider's Portal**, click **System > Administrators**.
2. Click **Create Administrator**.
3. Enter the details in required fields.
4. Select already created template from **Welcome Email Template** drop-down box.
5. Click **Next**.
6. Click **Submit**.

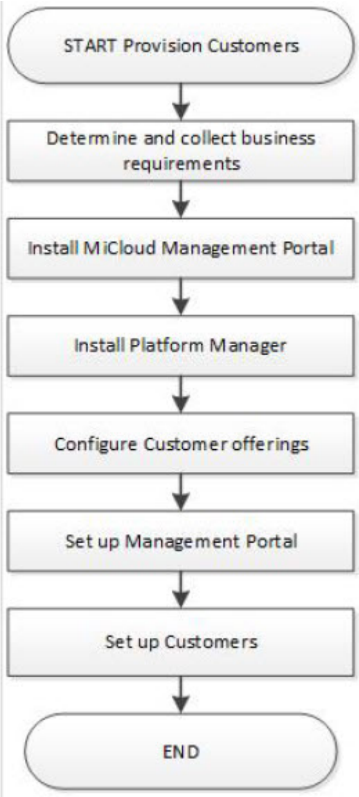
To update Administrator Email template of an existing admin

1. From the **Service Provider's Portal**, click **System > Administrators**.
2. Click on the admin name.
3. Click **Edit** icon.
4. Select the email template from **Welcome Email Template** drop-down box.
5. Click **Save**.

Provision customer site

You can use the links in the table to navigate directly to the topic you need.

Important
There are several pre-configurations that you must perform on the MiVoice Business platform before you can provision it in Management Portal. Make sure that you read the Management Portal Engineering Guidelines before you configure the MiVoice Business platform in Management Portal.

	What's New
	Virtual service providers vs value added resellers
 START Provision Customers Determine and collect business requirements Install MiCloud Management Portal Install Platform Manager Configure Customer offerings Set up Management Portal Set up Customers END	Determine and collect business requirements Install Management Portal Install Platform Manager Configure Customer Set up Management Portal Set Up Customers
	Administer Customers
	Maintain Management Portal

Mitel
Powering connections

mitel.com