MICLOUD BUSINESS VIRTUAL

DEPLOYMENT GUIDE
Release 4.2
December 2019

NOTICE

Trademarks

MiCloud Business Virtual

Deployment Guide

Release 4.2

December 2019

Table of Contents

MiCloud Business Virtual deployment

The following flowchart summarizes the process for deploying the MiCloud MLB/SMB topology. Each item in the flow chart represents a series of more detailed tasks. Follow through this guide to complete the steps needed to install and configure at each stage. Where necessary, there will be references to other documentation for specific steps, additional considerations, and engineering information needed to make decisions during the deployment.

Before beginning your deployment, review Deployment process and roles.

Workflow

Deployment Process and Roles

The installation and configuration tasks are meant to be performed by various players; these players and their roles are described in the table.

Infrastructure as a Service (IaaS) Provider	Responsible for deploying the server hardware, infrastructure networking, and VMware virtualization.
Platform as a Service (PaaS) provider	Responsible for deploying applications and configuring application networking and infrastructure networking, typically with access to virtualization tools such as vCenter and vSphere.
Software as a Service (SaaS) provider	Responsible for configuring and managing applications and providing customer services, typically without access to virtualization tools.
Reseller (VAR)	Responsible for provisioning applications and providing Customer services, typically with restricted access to system wide configuration tools.

Service providers may undertake one or more of these roles, and service provider technical staff may be responsible for one or more of these roles. To facilitate planning the deployment, the role expected to perform different steps is indicated. Prior to deployment, there are several technical and business steps required of the SaaS provider, including:

- Define the SaaS provider and customer IP addressing plans
- Determine the UCC service bundles to align with the end-user services offered by the SaaS provider
- Determine the number and type of UCC platforms required for a particular Customer

It is assumed this information will be available to the technical staff performing the deployment.

Prerequisites

- Mitel Connect is available and accessible, or the required documents have been downloaded to a local drive.
- Personnel performing the deployment have been certified on the relevant Mitel products and solutions:
- Refer to the training map, “Service Providers using MiVoice Business Virtual Platform” on the Mitel Training site: http://training.mitel.com/cw/Learning_Maps/MCLD_LM.pdf
- UCC licensing training is available. Refer to Mitel University.
- If deploying MiCollab Client Multi-tenant, training is required.
- If deploying either of the MiVoice Integrations, training is required. These integrations are built on Mitel Open Integration Gateway:
    - MiVoice Integration for Google
    - MiVoice Integration for Salesforce
- For the virtualized components, VMware training is required.
- Personnel performing the deployment have expertise in the network components and deployment configurations to meet the service provider requirements.
- Approved servers must be installed with any self-qualification tasks completed. Select servers using the MSL Qualified Server List, available on Mitel Connect.
- Network plans are complete, including logical and physical diagrams.
- Routers are installed and operational.
- Virtual clustering plan is defined.
- SIP trunk account is set up with SIP service provider.
- Internet gateway is installed and configured.
- Connections between all servers and network switches (defined in the MiCloud Business Solution Blueprint).
- VLAN programming in the network is complete, including consideration for QoS settings.
- Certificates have been ordered for MiCollab and MiVoice Border Gateway.

Step 1 Deploy Virtual infrastructure

Deploy the virtual infrastructure to build the server environment capable of running the virtual Mitel applications that are used in the MiCloud Business MLB and SMB reference architectures.

Prerequisites

- The installers are VMware certified for deploying VMware based environments. The VMware certification website http://mylearn.vmware.com/portals/certification/ describes the certification requirements and paths for obtaining certification credentials.
- The virtual infrastructure is in place, including storage.
- VMware vSphere and vCenter licenses have been purchased.
- Optional: VMware vCloud Director licenses have been purchased:
- vCloud Director is optional for VMware vCloud Networking and Security (vCNS)
- MiCloud Management Gateway (MMG) does not need vCloud Networking and Security

Deploy server hardware

Deploy server hardware to be used for installing the Mitel OVA files for Mitel virtual applications.

The server hardware must be installed and configured in the network using the instructions in the manufacturer's documentation. Servers are deployed and networked on the infrastructure network. The infrastructure LAN is independent of the management LAN.

Prerequisites

- Server hardware that complies with the VMware qualified hardware list for the intended Mitel virtual applications has been purchased and installed. The VMware tool is called the VMware Guided Search Wizard: https://www.vmware.com/resources/compatibility/wizard/request.php
- Networking, storage networks and servers configured in a VM infrastructure are available and operational.

RESOURCE	CONTENT DETAILS
Manufacturer documentation	Installation and configuration instructions for the server hardware.
VMware Product Interoperability Matrices	http://www.vmware.com/resources/compatibility/sim/interop_matrix.php
Virtual Appliance Deployment Solutions Guide	This guide, available on Mitel Connect, includes hardware requirements for Mitel virtual appliances. http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf

Deploy VMware vCenter, vSphere, and vCloud Director

To deploy the VMware infrastructure:

1. Deploy VMware vSphere on each server that will be running the Mitel applications used in the topology.
2. Set up vMotion to allow use of the VMware High Availability (HA) feature. Some restrictions and rules include:
    - The servers between vMotion VM movement will be done must be on the same layer2 broadcast domain and network, that is, in the same geographic location.
    - vMotion should be configured so that VM movement is done to a different server (anti-affinity rules).
    - See the Virtual Appliance Deployment Solutions Guide for details about setting up vMotion for Mitel Virtual Appliances.
3. Deploy VMware vCenter to run automated management of the vSphere servers the Mitel applications will reside on. vCenter is required to run VMware High Availability (HA) and MiCloud Management Portal.
4. vCloud Director is required to abstract a reseller management interface from the infrastructure provider, that is, if the reseller and infrastructure providers are not from the same organization.

Prerequisites

- Compatible server hardware is in place.
- VMware vCenter and VMware vSphere (and vCloud Director, if needed) are purchased and licensed.

NOTE: VMware vCloud Networking and Security (vCNS) deploys with a conflicting IP address on an interface. It is absolutely required that no IP address conflicts exist during vCNS deployment.

RESOURCE	CONTENT DETAILS
VMware documentation	Installation instructions for vCenter and vSphere. https://www.vmware.com/support/pubs/
Virtual Appliance Deployment Solutions Guide	On Mitel Connect: http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf

Install a DNS server on the management VLAN

The DNS server on the management VLAN will resolve management component addresses and UCC component addresses to addresses within the management VLAN associated with a 1:1 NAT device capable of accessing individual customer networks.

- Add DNS entries for MiCloud Management Portal, both LAN facing and WAN facing (portal) interfaces.
- Add MiCloud Management Portal external (Internet-facing) portal address to external and/or public DNS servers.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
Third-party DNS server documentation	Configuration instructions

Assign management plane

Use VMware vCenter to assign a management plane for use by the SaaS provider.

MiCloud Management Portal is used with networks in which the platforms (MiCollab, MiVoice Business, and MiVoice Border Gateway) are contained within a hosted virtual local area network (VLAN). The intention is to provide a 1:1 NAT at the edge of each customer network, such that the customer platforms appear as unique IP addresses within the service provider address space on the Management Plane VLAN. This, then, appears within the service provider space. To maintain isolation with other activities in the network, these connections are associated with a management VLAN, and the Management Portal connects to this management VLAN. MiCloud Management Portal also requires connection to the public network to allow over-the-top (OTT) connections from the customers to manage their configurations and end-users.

The two choices for address translation are:

- MiCloud Management Gateway (MMG). One MMG can handle 100 VLANs, with up to 10 connections per VLAN, for 1000 connections in total.
- VMware vCloud Networking and Security (vCNS). You need one vCNS for each customer.

Optional: Install MiCloud Management Gateway (MMG)

If you are using MMG (rather than vCNS), install it now. Deploy MiCloud Management Gateway on Mitel Standard Linux using the OVA deployment instructions in the Virtual Appliance Deployment Solutions Guide.

You will configure it later, in Configure 1:1 NAT with MiCloud Management Gateway**.**

Considerations:

- The DNS must be part of the management plane and associate each customer set of platforms to defined IP address on the 1:1 NAT portal.
- VMware vCloud Networking and Security (vCNS) requires the use of FQDNs. vCNS can be used with Flow Through Provisioning if FQDNs are used at the external interface and IP addresses are used internally.
- The Management Portal must use IP addresses to be able to send changes through to the MiVoice Business using Flow Through Provisioning.
- MiCloud Management Gateway (MMG) is configured with IP addresses.

NOTE: MiVoice Business does not recognize FQDNs, so communication with the Management Portal must be set up using IP addresses. Use the MiCloud Management Portal maintenance command to make the change to IP addresses.
$$UPDATE MCD CUSTOMER HOST NAME$$ <Management Host Name IP Address>, <New Customer Host Name>

MiCloud Management Portal can be deployed in the management plane configuration of the Reseller and/or Service Provider to access multiple customers, each with separate networks, accessible via a 1:1 NAT portal by use of:

- NAT between service provider management network and the customer VLAN.

NOTE: DNS in the service provider points to IP addresses within the service provider on the 1:1 NAT devices, whereas the DNS settings within each customer network point to units only within the customer network. This is also known as Split-DNS, where the same FQDN information results in different IP addresses, depending on where the information is referenced.

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

Prerequisites

- None

RESOURCE	CONTENT DETAILS
MiCloud Management Gateway Help	See the MiCloud Management Gateway Help in Mitel Standard Linux.

Step 2 Deploy MiCloud Management Portal

Create a management VLAN for MiCloud Management Portal, This VLAN needs to be separate from the VLANs used to isolate individual customer networks. This management VLAN may be combined with the service provider address space, or provided as a separate customer deployment, such as a reseller providing service on an infrastructure provider.

Prerequisites

- VMware infrastructure is in place.
- Customers are connected to the hosted infrastructure using MPLS, with a common VRF router, and isolation using VLANs.
- No end-user IP phones are registered prior to provisioning users in MiCloud Management Portal, or if there are phones registered, they are removed before provisioning. See also Bulk import end-users.

Install MiCloud Management Portal OVA

MiCloud Management Portal provides a way to manage network elements, customers, and end-users.

Install MiCloud Management Portal to create a secure management portal for end-user management. MiCloud Management Portal Virtual is deployed as a virtual machine using VMware vCenter.

MiCloud Management Portal is licensed through the Mitel Applications Management Center (AMC), as with other Mitel products.

Prerequisites

- If using MiCloud Management Gateway, external fire walls may be required for devices that require public Internet access, such as the public portal for the MiCloud Management Portal platform. If using VMware vCloud Networking and Security (vCNS), this is covered in Install and configure 1:1 NAT with VMware vCloud Networking and Security Edge.

RESOURCE	CONTENT DETAILS
MiCloud Management Portal Installation and Administration Guide	See Install Management Portal.
Virtual Appliance Deployment Solutions Guide	Covers general rules for deploying Mitel virtual appliances, plus capacity, performance, and resource requirements for individual virtual appliances.
VMware documentation	https://www.vmware.com/support/pubs/
MiCloud Management Portal Engineering Guidelines	See the “VLAN Support” section.
MiCloud Management Gateway Online Help	Available through MSL help.

Configure external access to MiCloud Management Portal

Configure a web proxy to MiCloud Management Portal to create a public IP address as a common global access point to the Management Portal for end-users, administrators, and the service provider.

You can use the MiVoice Border Gateway web proxy or a third-party firewall.

Prerequisites

- DNS must be set up with the public FQDN for MiCloud Management Portal.

RESOURCE	CONTENT DETAILS
Third-party web proxy documentation	

RESOURCE	CONTENT DETAILS
MiVoice Border Gateway Engineering Guidelines	See “Remote Proxy Services”.

Configure MiCloud Management Portal

Install and configure MiCloud Management Portal to create a secure management portal for end-user administration.

TIP: Understand the scope of all the tasks before deploying MiCloud Management Portal. Do not pre-configure settings that will be covered in future tasks during the deployment process.

MiCloud Management Portal initial programming includes:

- Administrator accounts
- Operations profiles
- Virtual Service Providers, and Value Added Resellers
- Registering the Mitel platforms
- Create test Bundles
- Assign Bundles to test Customers

The MiVoice Business instances must be in resilient clusters if end-user resiliency is required.

For every MiVoice Border Gateway cluster that the Management Portal will manage, define MBG cluster Zones in MiCloud Management Portal. The Management Portal will then display those cluster zones when creating sites in Platform Groups. The concept of Cluster Zones applies to your MiVoice Border Gateway Clusters. In an earlier step, you created a MiVoice Border Gateway Cluster for MiNet devices, and a MiVoice Border Gateway Cluster for SIP Trunks. In an upcoming step, you will create another MiVoice Border Gateway Cluster for SIP devices. These MiVoice Border Gateway Cluster Zones must be entered into the mbgZones.xml file. See the Oria 5.0 documentation for a description of how this is done.

Prerequisites

- The MBG Web Proxy services have been programmed to provide remote access to the MiCloud Management Portal.
- 1:1 NAT must be set up.

RESOURCE	CONTENT DETAILS
MiCloud Management Portal Installation and Administration Guide	For installation and configuration, see Install Management Portal.
MiCloud Management Portal Engineering Guidelines	For best performance, use the engineering guides to ensure that the configuration respects allowed capacities and limitations.

Define MiCloud Management Portal User Bundles

This step creates re-usable user bundles that define the services to be assigned to types of end-users. A User Bundle includes feature profiles. The Bundles created here are re-usable across multiple customers.

Create User Bundles to set up the feature packages for voice and unified communications to be offered to customers. Any bundles can be used with any of the customers, as long as sufficient numbers of licenses are available.

1. Log into MSL and launch MiCloud Management Portal.
2. Log in as an administrator.
3. Create Administrator Bundles and User Bundles.
    - Administrator Bundles define the features available to customer administrators.
    - User Bundles define the feature sets that will be offered to customers.
4. If you will be deploying MiCollab Clients for mobile users, you need to create a special User Bundle that includes a phone with **Phone Type** = **Next Gen Mobile SIP Softphone**.
    - Scroll to the **Softphone Settings** section. In **MBG SIP Port**, change Port **5061** to **0** (zero).

5. If you will be deploying WebRTC MiCollab Web Clients for some users, you need to use a User Bundle that includes a phone with **Phone Type** set to **PC SIP softphone**.
6. Create Feature Profiles.
7. Create Bundles. The Bundle types are **Admin Bundle**, **Basic IPT**, **Standard IPT**, **Entry**, **Standard**, and **Premium**. To create a Bundle for contact center agents:
    a. Create a Bundle with:
        - **License Type** = **Contact Center Agent**
        - **Prime Phone Type** = **ACD with Softphone.**
    b. To allow users to use the free basic MiCollab Web Client, create a user bundle that includes Basic IPT plus Desk phone.
    c. Select the Customer and **Edit**. Assign the new Bundle to the Customer.
    d. Select Hotdesk Phones. Move **PC MiNet Softphone** to the list of Selected Devices.
    e. Click **Save**.
8. When creating Premium Bundles, if you want to enable MiCollab MiTeam for users:
    a. Scroll down to **MiCollab Client Service**.
    b. Select **MiTeam**.

NOTE: For users to use MiTeam Meet, the Audio, Web and Video application must be configured and active.

After they are created, Feature Bundles are a available across the scope of the managed Service Provider, as defined in the Management Portal, and can be applied to any customer. More Feature Bundles can be created when adding customers with unified communications and additional features to the solution.

MiCloud Management Portal has three levels; each level has its own bundles, and each level can see only their own bundles:

- Service Provider
- Virtual Service Provider
- Value Added Reseller (VAR)

See also Step 7 Configure UCC platform services with MiCloud Management Portal.

Prerequisites

- At least one Feature Profile has already been created.

RESOURCE	CONTENT DETAILS
MiCloud Business for Service Providers Help	See Create and change bundles.
MiTeam for MiCollab and MiCloud Business Virtual Reference Guide	
MiCollab Client Administrator Guide	See “MiTeam Integration”.

Step 3 Deploy Mitel Performance Analytics (MPA)

Mitel Performance Analytics deployment is a relatively independent step in the process. As such, you can deploy it at this stage OR at the end of the UCC deployment.

NOTE: The SaaS provider may choose whether to use Mitel Performance Analytics. If using Mitel Performance Analytics, the SaaS Provider can choose to deploy the Mitel Performance Analytics server.

Deploy Mitel Performance Analytics to monitor core networking devices and take ongoing measurements of voice quality on customer connections. Mitel Performance Analytics is sold as “software as a service” (SaaS) that delivers fault and performance management capabilities for Mitel Unified Communication (UC) systems and the associated network infrastructure.

There are two parts to Mitel Performance Analytics; server and Probe.

- The server can be deployed with the service provider as a service with a public IP connection. It can also be hosted from a central location.
- Probes are deployed into the individual customer networks. These will register with either the service provider Mitel Performance Analytics server, or with the central hosted solution, whichever is configured.

Prerequisites

- The installer has Mitel Performance Analytics documentation on hand. It is available from Mitel Connect.
- For Mitel Performance Analytics to monitor platforms—MiVoice Business and MiVoice Border Gateway, etc.—the SNMP agent must be enabled, and community strings set for each application.

Install Mitel Performance Analytics (MPA)

Install Mitel Performance Analytics to create the server and the Probe instances used to monitor the network. The Mitel Performance Analytics server OVA must be ordered and licensed through Mitel.

NOTE: Ask your Mitel Sales Engineer for help purchasing Mitel Performance Analytics licenses and getting them added to the ULM.

The service provider version of the Mitel Performance Analytics server is provided as an OVA file that can be deployed in the VMware virtual machine. After the OVA has been deployed, it is accessible using a web portal and is ready for configuration. The Mitel Performance Analytics OVA is available in three different package sizes. Review the documentation, and consult with Mitel Professional Services to determine the correct size for your network and topology and size.

Single or multiple probes are deployed to provide monitoring information back to the server. A root certificate file must be added to the Java JRE certificates (cacerts) file on any Windows or Linux blades. There is also an embedded Probe running in the Mitel Performance Analytics server.

Use the following procedures to deploy Mitel Performance Analytics.

Download Mitel Performance Analytics OVA

Download instructions are sent after ordering a Mitel Performance Analytics OVA. The instructions include a download link with an expiration timer, and credentials.

Instance Access credentials (Both Linux Console and Mitel Performance Analytics web page).

URL: <web portal url>
Username: dftadmin
Password: **********

Deploy Mitel Performance Analytics OVA

1. Download and extract the attached Root Certificate file unto the system the probe is going to be installed on.
2. Find the location of the 32-bit Java JRE cacerts file. This is usually located in the installed directory of Java JRE.
   Example: C:\Program Files\Java\jre6\lib\security\cacerts
3. Open a command line terminal as windows Administrator.
   a. In Windows, click Start > All Programs > Accessories.
   b. Right-click **Command Prompt**.
   c. Select **Run as Administrator** to launch a DOS command line terminal.
4. Run the following command to add the Root Cert. file to Java JRE cacerts file
   keytool -importcert -keystore "<path to java jre securite cacerts>" -alias martelloCA -file "<path to the extracted Root Cert file>"
   Example command: (use the quotation marks around the file paths)
   keytool -importcert -keystore "C:\Program Files\Java\jre6\lib\security\cacerts" -alias martelloCA -file "C:\Users\rsally\Documents\martelloRootCert.crt"
5. Enter the password for the Java JRE cacerts when prompted.
   The password is: changeit
   This is default to Java JRE cacerts file and should not be changed.
   PASSWORD for Java JRE cacerts is: changeit
6. Download the MSI installer.
7. Install the probe as usual.

Install Windows root certificate file for Mitel Performance Analytics Probe

1. Download and extract the attached Root Certificate file unto the system the probe is going to be installed on.
2. Find the location of the 32-bit Java JRE cacerts file. This is usually located in the installed directory of Java JRE.
   Example: C:\Program Files\Java\jre6\lib\security\cacerts
3. Open a command line terminal as windows Administrator.
   a. In Windows, click **Start > All Programs > Accessories**.
   b. Right-click **Command Prompt**.
   c. Select **Run as Administrator** to launch a DOS command line terminal.
4. Run the following command to add the Root Cert. file to Java JRE cacerts file.
   keytool -importcert -keystore "<path to java jre securite cacerts>" -alias martelloCA -file "<path to the extracted Root Cert file>"
5. Example command: (leave the quotes around the file paths)
   keytool -importcert -keystore "C:\Program Files\Java\jre6\lib\security\cacerts" -alias martelloCA -file "C:\Users\rsally\Documents\martelloRootCert.crt"
6. Enter the password for the Java JRE cacerts when prompted.
   The password is: changeit
   This is default to Java JRE cacerts file and should not be changed.
   PASSWORD for Java JRE cacerts is: changeit
7. Download the MSI installer.
8. Install the probe as usual.

Install Linux root certificate file for Mitel Performance Analytics Probe

1. Download and extract the attached Root Certificate file unto the system the probe is going to be installed on.
2. Run the following command to find the location of Java cacerts file:
   sudo find / -name "cacerts"
   The following is an example of the expected result:
   usr/lib/jvm/java-6-sun-1.6.0.45/jre/lib/security/cacerts
3. Run the following command to add the Root Cert. file to Java JRE cacerts file:
   sudo keytool -import -keystore <path to java jre securite cacerts> -alias martelloCA -file <path to the extracted Root Cert file>
   Example command:
   sudo keytool -import -keystore /usr/lib/jvm/java-6-sun-1.6.0.45/jre/lib/security/cacerts -alias martelloCA -file /home/voipadmin/martelloRootCert.crt
4. Enter password for the Java JRE cacerts when prompted.
   The password is: changeit

This is default to Java JRE cacerts file and should not be changed
PASSWORD for Java JRE cacerts is: changeit
5. Download the RPM file.
6. Install the RPM file.

NOTE: Steps 1 through 4 apply to the MSL Blade installation.

Prerequisites

- A static public IP address has been assigned for the Mitel Performance Analytics server instance.
- A external DNS entry has been created for the Mitel Performance Analytics web portal URL.

RESOURCE	CONTENT DETAILS
Mitel Performance Analytics System Guide	See “Probe Installation and Configuration”. Also see the documentation on Mitel Connect.

Configure external access to MPA portal

Configure a web proxy to Mitel Performance Analytics to allow external connectivity to the server and to the Probe instances. This will be used by technicians who need to work remotely.

The following procedure describes how to configure a web proxy with MiVoice Border Gateway. This can also be done in MSL or with a third-party web proxy, if desired.

In the MiVoice Border Gateway user interface, create and configure a web proxy. This is done in the Remote Proxy Services panel.

1. Click **Add new LAN server proxy**.
2. In the screen that appears, there is the question: **What kind of LAN server are you configuring?** Select **MiVoice Business**.
3. In the WAN Side FQDN, enter the FQDN that resolves to the Mitel Performance Analytics IP Address on the internal DNS Server. The same FQDN must resolve to the MBG WAN IP address on the external public DNS Servers.
4. Select **Yes** for the option **Do you wish to permit remote administration access?**
5. Select the **Enable** check box.
6. Continue by creating end-users as described in the *MiVoice Border Gateway installation and Maintenance Guide*.
7. In the **Users** tab, create login credentials for a proxy account that customers will use to reach Mitel Performance Analytics. The credentials must be exactly the same Username and Password defined on the Mitel Performance Analytics server for administrator **access.**

   NOTE: MiVoice Border Gateway Remote Proxy Services programming is not auto-shared across the MBG cluster. Therefore, this programming must be duplicated on other MBG Cluster members. Program the Alias entries in the External DNS server for each MBG WAN IP address that serves as an MBG Web Proxy.

8. Test external connectivity to Mitel Performance Analytics to verify that the web proxy setup in the user MiVoice Border Gateway is working correctly. The external connections must work correctly to allow external access to the Mitel Performance Analytics server from outside the network.

Prerequisites

- None

MiVoice Border Gateway Installation and Maintenance Guide	To configure MBG to support external traffic into the service provider’s network: • “Server-Gateway Configuration on Network Edge”

Configure Mitel Performance Analytics

Configure Mitel Performance Analytics to monitor the service provider core network space for alarms and network activity. The probes installed in the customer network can monitor the devices in the customer network. Each Probe must be configured for the device it is monitoring.

Mitel Performance Analytics server:

- Deploy Mitel Performance Analytics Server using one of these options:
  - as a public service
  - provided by the service provider, along with use of MMG or vCNS, if required, along with a web proxy.
- The DNS server for each Probe must be able to resolve the Mitel Performance Analytics name within that URL, and the resolved Mitel Performance Analytics server IP Address must be reachable by the Probe across the network.

Probe:

- Deploy Probes, both at the service provider level (part of the server) and as probes deployed at the customer network with access via public network, or via the local MiCloud Management Gateway, or vCNS, ports if these are configured.
- For each Probe device created in Mitel Performance Analytics, a unique URL will be presented. Copy this URL into the Configuration panel in each individual Probe.

Prerequisites

- SNMP agent/service must be enabled in each Mitel application—MiVoice Business, Mi-Voice Border Gateway, etc.—prior to configuring Mitel Performance Analytics.

RESOURCE	CONTENT DETAILS
Mitel Performance Analytics System Guide	See “Probe Installation and Configuration”. Also see the documentation on Mitel Connect.

Step 4 Deploy UCC Platforms

Deploy UCC platforms for end-customers.

Prerequisites

- The hardware is in place, and networking is connected and tested.
- The VMware infrastructure, including vCenter, is installed and working.
- All Mitel licenses are ready in Mitel AMC.

Assign customer VLAN and VRF

Configure customer VLAN and Virtual Routing and Forwarding (VRF) using virtual routers and switches for each customer network. This step establishes the customer address space and connectivity to the customer sites. Virtual Routing and Forwarding is completed with third-party networking equipment.

- Assign VLAN - Select vCenter tab and enter:
- VLAN - enter the VLAN number
- Name - customer name

Prerequisites

- The management plane is deployed and operational.

RESOURCE	CONTENT DETAILS
Engineering Guidelines for Industry Standard Servers (ISS) and MiVoice Business Virtual	See “MiVoice Business Virtual Engineering Guidelines System Overview”.
Installation and Administration Guide for Industry Standard Servers (ISS) and MiVoice Business Virtual	See “MiVoice Business Virtual Software Installation.”
Virtual Appliance Deployment Solutions Guide	See “Networking”. http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
Router or switch supplier documentation for VRF configuration	Instructions for installation and configuration

Configure 1:1 NAT

Configure 1:1 NAT with forwarding for management access.

Use one of the following procedures:

- Configure 1:1 NAT with MiCloud Management Gateway (MMG)
- Install and configure 1:1 NAT with VMware vCloud Networking and Security

Configure 1:1 NAT with MiCloud Management Gateway (MMG)

This step sets up connectivity between the SaaS provider and multiple customer networks using MiCloud Management Gateway. MiCloud Management Gateway (MMG) is a Mitel product, delivered as an OVA. MMG is configured through Mitel Standard Linux.

Use 1:1 network address translation (NAT) to isolate the service provider from the customers, and customers from each other. This is essentially a router function—IP to IP—with 1:1 direct IP Address (NAT) translation. A connection (and management IP address) is

required for each of the Mitel virtual applications requiring management. Each MiCloud Management Gateway supports up to 100 customers.

This allows Oria to manage multiple customers with potentially overlapped IP addresses, from a separate and isolated network, the Management Plane of the Reseller/Service Provider. It also allows for re-use of customer IP addresses.

The MMG supports two types of connections: “southbound” from the service provider space into the customer space, and “northbound” from the customer space to the service provider space.

- Southbound connections: The MMG controls southbound connections from the service provider space into the customer space using Network Address Translation (NAT). MMG maintains a one-to-one mapping between unique management IP addresses on the service provider network and specific end-point addresses on the customer networks. Port translation is not performed. Before forwarding the request to the customer network, the MMG translates the source and destination addresses, with the source becoming the primary service IP address of the MMG on the specific customer network and the destination becomingthe actual endpoint address in the customer network.
- Northbound connections: The MMG can also be configured to control northbound connections from the customer space to particular TCP, UDP, and ICMP services in the service provider network. In a northbound scenario, the connection is initiated from the customer side. A customer application requests a connection to the service IP address configured on the MMG that represents the desired service. The MMG translates the request and forwards it to the appropriate service in the service provider network. The source address is translated to the management IP address assigned to the originator, and the destination address is translated to the address of the endpoint providing the service. Port translation is not performed. Before forwarding the request, the MMG translates the addresses. All ports are blocked except for those configured.

Configuring MiCloud Management Gateway:

1. Configure the MiCloud Management Gateway using the instructions in the Mitel Standard Linux (MSL) Online Help.

NOTE: Configure one or two customers and test the configuration and operation before configuring all customers. Configure all customers off-line before powering up the MiCloud Management Gateway virtual machine.

Prerequisites

- An IP address re-use plan has been created for management of the customer address spaces.
- The various edge deployment options for supporting the 1:1 NAT function have been analyzed, and a strategy has been chosen.
- MiCloud Management Gateway has been licensed for the deployment.
- The IaaS vendor has set up the VLAN trunk connector. This cannot be done in VMware vCenter.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”. http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
MSL Online Help	See the MiCloud Management Gateway configuration instructions.

Install and configure 1:1 NAT with VMware vCloud Networking and Security

This step sets up connectivity between the customer address space and the SaaS provider management address space using vCNS. One vCNS instance is needed for each customer.

Use 1:1 network address translation (NAT) to isolate the service provider from the customers, and customers from each other. This is essentially a router function—IP to IP—with 1:1 IP address direct translation.A connection (and management IP address) is required for each of the Mitel virtual applications requiring management.

This allows MiCloud Management Gateway to manage multiple tenants, and have the availability to re-use customer IP addresses. The use of 1:1 NAT allows the Management Gateway to manage multiple customers, with potentially overlapped IP addresses, from a separate and isolated network, the Management Plane of the Reseller/Service Provider.

This deployment includes:

- VMware vCloud deployment NAT from a Customer network
- VMware vCloud deployment NAT from a Reseller network
- Direct vCenter deployment with port group backed networks Important considerations and things to watch for:
- VMware vCloud Networking and Security (vCNS) deploys with a conflicting IP address on a interface. It is absolutely required that no IP address conflicts exist during vCNS deployment.
- Destination NAT rules MUST be individual entries. Range programming does not support true 1:1 NAT on the vCNS.
- Source NAT rules on the vCNS require a full vCNS reset after programming is complete to take effect.
- Split-DNS must be used to support IP address overlap between customers.
- All Mitel virtual applications being registered with Oria MUST do so using a FQDN and not a straight IP address to support the split DNS and NAT functionality.

NOTE: MiVoice Business does not recognize FQDNs, so communication with the Management Gateway must be set up using IP addresses. Use the Oria maintenance command to make the change to IP addresses.
$$UPDATE MCD CUSTOMER HOST NAME$$ <Management Host Name IP Address>, <New Customer Host Name>
See the Provision Customers in the *Management Portal Installation and Administration Guide* for instructions.

Prerequisites

- An IP address overlap plan has been created for management of the customer spaces.
- The various edge deployment options for supporting the 1:1 NAT function have been analyzed, and a strategy has been chosen.

RESOURCE	CONTENT DETAILS
MiCloud Management Portal Engineering Guidelines	See “VLAN Support”.
VMware documentation	https://www.vmware.com/support/pubs/
MiCloud Management Portal Help	Provision customers

Configure Mitel Performance Analytics Probes

Mitel Performance Analytics Probes can monitor the devices in the customer network. Each Probe must be configured for the device it is monitoring.

Deploy Probes:

- Deploy Probes, both at the service provider level (part of the server) and as probes deployed at the customer network with access via public network, or via the local MiCloud Management Gateway, or vCNS, ports if these are configured.
- For each Probe device created in Mitel Performance Analytics, a unique URL will be presented. Copy this URL into the Configuration panel in each individual Probe.

Prerequisites

- SNMP agent/service must be enabled in each Mitel application—MiVoice Business, MiVoice Border Gateway, etc.—prior to configuring Probes.

RESOURCE	CONTENT DETAILS
Mitel Performance Analytics System Guide	See “Probe Installation and Configuration”. Also see the documentation on Mitel Connect

Deploy MiVoice Business and MiCollab OVAs

Configure Remote Proxy access for configuration and management. Deploy the MiCloud Performance Analytics Probes.

Deploy the required OVAs:

1. Deploy MiCollab.
   - Deploy the MiCollab instances. Make sure they are configured for Integrated Mode. See the MiCollab installation documentation for details.
   - If you will be adding extra MiCollabs into the MiVoice Business Cluster: In the Server-Manager, navigate to **Configuration** > **MiCollab Settings** > **MiVB Sharing tab** > **Enable Multi-MiCollab** in each MiCollab that will be used in the Multi-MiCollab cluster.
2. Deploy MiVoice Business.
   - Deploy MiVoice Business instances in a cluster. Add each one as a Network Element in the same network, and follow the instructions in the System Administration Tool on-line help to cluster the instances.
   - Add one or more MiCollabs as Network Elements into the MiVoice Business Cluster. One MiCollab can serve up to 5000 users, so you may want to start with one MiCollab, and add another when you need the capacity. You add the MiCollab servers as type **MSL server (MiCollab).**
   - Perform an SDS Sync. This will synchronize the MiVoice Business instances with each other and with the MiCollab instances.
   - Install a third-party certificate, and export it for import into all of the applications.
3. Optional: Deploy Mitel Performance Analytics Probes. See Deploy Mitel Performance Analytics.

Prerequisites

- VMware vSphere is installed and configured, using VMware best practices and the Mitel resource requirements.
- VMware vCenter is installed and configured, using VMware best practices.
- The Mitel virtual appliances have been purchased and licensed in the Mitel AMC.
- MiCloud Management Gateway or VMware vCloud Networking and Security has been deployed and configured for customer isolation and 1:1 connections from the management plane VLAN.
- DNS Server and domain name are available.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
Mitel product-specific documentation, including Installation Guides and Engineering Guides	**Mitel Connect** > **eDocs** Login credentials are required for access to Mitel Connect.
VMware documentation	https://www.vmware.com/support/pubs/

Optional: Use Platform Manager to create Blueprints

You can create “Blueprints” of common customer configurations using Platform Manager.

In MSL, in the left column, click Platform Manager, and follow these steps to create new Blueprints. For detailed instructions, see the Service Provider Portal Help.

The first step is to register the Platform Manager server in MiCloud Management Portal; **System** > **Platform Manager Registration**.

General steps for creating new customers with Platform Manager:

1. In **MSL** > **Platform Manager**:
   a. Register the MiVoice Business Multi Instance server.
   b. Create MiVoice Business Multi Instance pools.
   c. Register the File Server(s).
   d. Register the AMC account.
   e. Register the MiCollab Multi-tenant servers (if any).
   f. Create Blueprints (ARID, resource, and platform) to describe platforms to deploy.
   g. Upload a golden database and the MiVoice Business Express OVA.
   h. Create inventory pool(s) of platform Blueprints describing systems that you want to provide to your Customers.

   i. Register the Blueprints with AMC license-bank-records containing enough license parts to build a quantity of platform instances. The parts list is displayed on **Platform Blueprint** > **Platform Availability**.

   NOTE: The Platform Manager server contains reference database files, in the directory /opt/dist_oria-bim-setup/reference.
2. Platform Manager creates ARIDS for the Platform instances it creates and puts everything into a ULM, including the MiCollab, if required.
3. If the Blueprint specifies the creation of resilient MiVoice Business controllers, Platform Manager creates two MiVoice Business instances and clusters them.
4. In MiCloud Management Portal, select the Blueprints to be available to Management Portal users. Only Blueprints with Platforms in the inventory pool will be visible.
5. Navigate to the **Register Platform** page. Select the Blueprint that describes the system you want to register.
6. Configure the sites and review the MiCollab configuration.

Prerequisites

- You must have connections to AMC from both MSL and MiCloud Management Portal.
- All licenses must already be available in AMC.
- You must have an MSL golden database.

RESOURCE	CONTENT DETAILS
Platform Manager Help	Platform Manager Help

Deploy UCC OVAs

Deploy Mitel OVAs. Many Mitel products are supported on VMware, and are delivered and deployed using OVA files. OVA files are archive files that contain the entire Mitel virtual appliance, including the Mitel Standard Linux (MSL) operating system.

Configure Remote Proxy access for configuration and management.

Deploy the required OVAs

1. Deploy the external MiVoice Border Gateways.
   NOTE: When deploying the MiVoice Border Gateways, both internal and external, keep in mind that the master MBGs overwrite the slave MBGs. Slave MBGs are used in the same way as for Teleworkers and SIP trunks.
   NOTE: When certificates are required, the same certificates are required on both the external and internal MBGs. If this is not done, MiCollab Client Teleworker users cannot log in.
   a. If you are deploying MiCollab soft phone resiliency, configure the MiVoice Border Gateways into a cluster and a backup cluster. DNS SRV records are used to define the MiVoice Border Gateways, their host names, their priorities and weightings, and Time To Live (TTL) for each. The Registrar/Proxy file in the MiCollab Client for Mobile soft phone lists the host names of multiple MBGs. Each soft phone can register with any of the MBGs in the list subject to the priority and weighting settings. See the *MiCollab Client for Mobile Resiliency Guide* for details and instructions.
      NOTE: During fail-over to the secondary MiVoice Border Gateway, in-progress calls are lost, and new calls are completed through the secondary MiVoice Border Gateway.
   b. From the Mitel Standard Linux Web Server panel, purchase and install a third-party certificate for use with MiContact Center Business. This can be the same certificate as you are using for MiCollab, but it must include an intermediate certificate. See the Mitel Standard Linux Online Help. “Manage Third-Party Certificates from an Alternate Certificate Authority”.
   c. Export the new certificate using the Mitel Standard Linux utility. You will later install this certificate to the MiContact Center Server when completing the instructions in Optional: Install MiContact Center Business and MiVoice Call Recording.

   NOTE: If the CSR code was not generated on the MiContact Center server, you may need to combine the CRT and KEY Files into a PFX using OpenSSL. Then apply the PFX certificate to the MiContact Center server. Otherwise use the standard method for importing a certificate to a Windows server.
2. If you are deploying WebRTC for users, complete the following steps on the external MiVoice Border Gateway. This can be the same MiVoice Border Gateway being used for MiCollab Client for Mobile users.
   a. In Mitel Standard Linux, click **Applications > MiVoice Border Gateway** in the left column.
   b. In the panel that appears, click **Service Configuration > WebRTC**.
   c. Select **Enabled** to enable WebRTC.

   d. Enter the following settings:
      - **Hosting mode**: **Host WebRTC on separate server**
      - **Mode**: **Subscriber**
      - **Anonymous WebRTC ICP**: Select the MiVoice Business controller that is hosting the WebRTC clients.
      - **WebRTC protocol security mode**: **Public Only**
   e. If you are deploying a firewall on the external network in front of the MiVoice Border Gateway, perform the steps in "Configure the firewall for the WebRTC gateway" below.
3. If you are deploying MiContact Center Business with external users, you must enable a MiVoice Border Gateway web proxy.
   a. On the MSL server, select Applications > Remote proxy services.
   b. Click Add new LAN server proxy.
   c. On the Configure Web Proxy & Remote Management Service page:
      - Select **Enabled** to enable the web proxy.
      - In **WAN-side FQDN**, enter the FQDN of the MiContact Center server.
      - Select **MiContact Center**.
4. If you are deploying MiVoice Call Recording web proxy, repeat step 3., selecting MiVoice Call Recording in place of MiContact Center, and entering the MiVoice Call Recording server FQDN.

Configure the firewall for the WebRTC gateway

1. From the Internet to the MiVoice Border Gateway server, use the following settings:
   - Allow protocol TCP, destination port 5063 for SIP over TLS
   - Allow protocol UDP, destination ports 32000 to 32500 (and return traffic) for RTP media
2. From the MiVoice Border Gateway server to the LAN (or to the 3300 ICP controllers), use the following settings:
   - Allow protocol TCP, destination port 389 for connection to LDAP database (MiVoice Business)
   - Allow protocol TCP, destination port 443 for connection to picture server (MiVoice Business)
   - Allow protocol UDP, source port 5064 for unencrypted SIP trunk connection to MiVoice Business (anonymous calls)

Prerequisites

- vSphere is installed and configured, using VMware best practices and the Mitel resource requirements.
- vCenter is installed and configured, using VMware best practices.
- The Mitel virtual appliances have been purchased and licensed in the Mitel AMC.
- MiCloud Management Gateway or VMware vCloud Networking and Security has been deployed and configured for customer isolation and 1:1 connections from the management plane VLAN.
- DNS Server and domain name are available.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See "Deploying Mitel virtual appliances in VMware". http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
Mitel product-specific documentation, including Installation Guides and Engineering Guides	**Mitel Connect** > **eDocs** Login credentials are required for access to Mitel Connect.
Mitel Border Gateway Installation and Maintenance Guide	See the "Remote Proxy Services" section
MiVoice Border Gateway Online Help	See the topics called: • "Configure LAN Servers on the Web Proxy". • "Configure WebRTC"
VMware documentation	https://www.vmware.com/support/pubs/
MiCollab Client for Mobile Resiliency Guide	To configure MiCollab soft phone resiliency.
MiCollab Client Deployment Help	See "Enterprise Tab"

Optional: Install MiContact Center Business and MiVoice Call Recording

Deploy the MiContact Center Business and MiVoice Call Recording Business Edition. Add call analytics, if desired.

Deploy the OVAs in the following order:

1. If you will be offering call recording, deploy one or more additional MiVoice Border Gateways, configured in Secure Recording Connector (SRC) mode.
   You may have to install additional MiVoice Border Gateway Secure Recording Connectors if existing capacity is insufficient.
2. Deploy the MiVoice Call Recording OVAs.
   - Connect MiVoice Call Recording to MiVoice Business (MiTAI connection).
   - Connect MiVoice Call Recording to MiVoice Border Gateway (Secure Recording Connector). MiVoice Call Recording requires an SQL database, either Standard or Express, depending on the capacity you need.

   NOTE: Contact Mitel Professional Services for help sizing and configuring storage for call recording archives.
3. Deploy MiContact Center Business.
   NOTE: MiContact Center Business will be deployed and configured in one of several different ways, depending on the whether the contact center is small and informal, or the prime business, See the Contact Center Blueprint for details.
   - Configure MiContact Center Business to point to MiVoice Call Recording, if applicable.
   - Install the certificate you exported from the MiVoice Border Gateway in Deploy UCC OVAs in the MiVoice Border Gateways installation instructions.

   NOTE: If the CSR code was not generated on the MiContact Center server, you may need to combine the CRT and KEY Files into a PFX using OpenSSL. Then apply the PFX certificate to the MiContact Center server. Otherwise use the standard method for importing a certificate to a Windows server.
4. If you will be provisioning remote agents and/or supervisors, the MBG Connector must be enabled. On the existing MiNet user MiVoice Border Gateways (or if creating new MiVoice Border Gateways):
   a. Navigate to the **Service Configuration tab > Applications Integration**, select MiContact Center connector enabled.
   b. In **MiContact Center Service hostname or IP address**, enter the FQDN of the MiContact Center server.
   c. If you are also providing integration with Salesforce, see Deploy optional OVAs.

Optional

- Deploy MiVoice for Skype for Business integration. Contact your reseller for details.
- Deploy a customer backup server.

Prerequisites

- All of the core UCC OVAs must already be in place, specifically MiVoice Business, MiCollab, and MiVoice Border Gateways.
- MiContact Center Business, MiVoice Call Recording, and MiVoice Business Reporter must be licensed, with ARIDs in place in the Mitel AMC.
- MiVoice Border Gateway SRCs must be licensed, with ARIDs in the Mitel AMC.
- MiContact Center Business and MiVoice Call Recording run on Windows platforms. The Windows platforms must be licensed with appropriate Client Access Licenses for the number of users and sessions on the Windows servers.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”. http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
MiContact Center Installation and Administration Guide	Use the instructions in the following sections: • “Enterprise Server installation” for how to download and install (MiContact Center (MiCC) Setup wizard) • “MiContact Center product registration” for how to register and set up MiContact Center on the Enterprise Server and client computers • “Remote Server Installation” for how to install and configure MiContact Center at remote sites • “Call Recording” for how to deploy MiVoice Call Recording

RESOURCE	CONTENT DETAILS
MiVoice Call Recording Installation and Configuration Guide	See “Software Installation”.
MiVoice Call Recording Administration Guide	See “Getting Started”.
MiVoice Business Integration Guide	Describes how to connect SIP Trunks via MiVoice Border Gateway Secure Recording Connector.

Optional: Deploy business analytics

Deploy one or more of these contact center reporting and business analytics solutions. Both of the following can be used with either MiContact Center Business or with the MiVoice Business built-in ACD functionality.

MiVoice Business Reporter

MiVoice Business Reporter provides data collection, analysis and storage, security, forecasting, real-time monitoring, reporting, and wall sign programming for use in managing your business. See the *MiVoice Business Reporter Installation Guide*.

MiCloud Business Analytics

MiCloud Business Analytics provides business analytics for call metrics to improve communications management and reporting. MiCloud Business Analytics is a cloud-based service with user access via a standard web browser. For instructions, see *MiCloud Business Analytics Provisioning and Ordering Process*. For assistance contact your Mitel Channel Manager.

Prerequisites

- MiCloud Business Analytics requires an SMDR server.

RESOURCE	CONTENT DETAILS
Business Reporter Installation Guide	See “Enterprise Server installation”.
MiCloud Business Analytics Provisioning and Ordering Process *MiCloud Business Analytics User Guide* *MiCloud Business Analytics Reports Catalogue*	MiCloud Business Analytics guides for installation and provisioning. Also see Mitel Business Analytics for Partners.

Deploy optional OVAs

Deploy optional OVAs.

1. Deploy Mitel Open Integration Gateway (OIG) with MiVoice Integrations.

- Optional: Configure E.164 calling directory.
- Optional: Install and configure MiVoice Integration for Google.
- Optional: Install and configure MiVoice Integration for Salesforce.
- Purchase and configure Salesforce CRM.
- Optional: Connect Salesforce to MiContact Center Business for ACD calling from Salesforce (special licensing required).

Prerequisites

- All of the core UCC OVAs must already be in place, specifically MiVoice Business, MiCollab, and MiVoice Border Gateways.

- If you are deploying MiVoice Integration for Salesforce with ACD calling, MiContact Center Business must be installed and configured.
- Mitel Open Integration Gateway, MiVoice Integrations, and Salesforce licensing (if applicable) must be in place.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
Mitel product-specific documentation, including Installation Guides and Engineering Guides	**Mitel Connect** > **eDocs**: https://connect.mitel.com/connect/ Login credentials are required for access to Mitel Connect.
VMware documentation	https://www.vmware.com/support/pubs/
Mitel OIG Installation and Maintenance Guide	To install OIG, see “Installing the Mitel OIG”. If you will be using OIG with MiContact Center Business and Salesforce, see “The Network Elements Tab”.
Mitel OIG Engineering Guidelines	Requirements and capacity
MiVoice Integration for Google Administration Guide *MiVoice Integration for Google Quick Reference Guide*	Instructions for installing and configuring MiVoice Integration for Google.
MiVoice Integration for Salesforce Administration Guide	Installing and configuring MiVoice Integration for Salesforce with OIG and MiContact Center Business.

Optional: Deploy on-site survivable gateways

The Reseller installs the MiVoice Business controller on-site. This work includes installing and configuring the power infrastructure.

Install the secondary gateway before installing the primary. In the MiVoice Business System Administration Tool, run an SDS Sync to synchronize the primary and secondary gateways. The Gateways will be configured in a later step.

Prerequisites

- Management and customer VLANs are deployed and operational.

RESOURCE	CONTENT DETAILS
3300 ICP Technician’s Handbook	Planning and performing the installation of a physical MiVoice Business controller
MiVoice Business System Administration Tool Help	See the following: • “Start Here Guide” for hardware installation and licensing. • “Installation and Programming”

Optional: Deploy Vidyo

Deploy Vidyo® functionality for MiCollab Client users.

Vidyo® is a cloud-based video collaboration service. The Vidyo service enhances MiCollab Client by adding a Vidyo icon to the MiCollab Client user interface. See the *MiCollab Vidyo Administrator Quick Reference Guide* for detailed instructions.

1. Create a Vidyo tenant on the Vidyo server.
2. On the MiCollab Administrator Portal, program the Vidyo tenant settings to establish a connection between MiCollab and the Vidyo server (Vidyo Settings page).
3. In MiCollab User and Services Provisioning (USP), enable the Vidyo service by selecting **Include Vidyo Service** on the MiCollab User template. By default, the Vidyo service is not selected. Note that the **Include Vidyo Service** option only appears on the **User** form when Vidyo has been successfully configured on the **Vidyo Settings** page.

Prerequisites

- MiCollab must be installed and configured.
- A Vidyo Portal has been licensed and deployed appropriately.

RESOURCE	CONTENT DETAILS
Vidyo documentation	Vidyo self-service portal
MiCollab Vidyo Administrator Quick Reference Guide	Follow all of the instructions in this guide.

Step 5 Configure UCC platforms

Configure the UCC platforms.

In this section, MiVoice Border Gateways are clustered together, with the MiCollab internal MiVoice Border Gateway being the “Master”. MiCloud Management Portal can be used to manage the network through its connection to the Master MiVoice Border Gateway, so if a Master MiVoice Border Gateway is out of service, the Management Portal is assumed to be unable to perform user management tasks until the Master element is brought back into service.

There are two types of configuration, based on architecture.

- MiCloud Business architecture based on MiVoice Business
- MiCloud Business architecture based on MiVoice Business Express

These two follow a similar process, with most of the steps being the same, but with some divergence based on the MiVoice Business platform.

Prerequisites

- UCC platform OVAs have been deployed

Configure AMC licensing

Create and activate licenses in the AMC for the services the service provider has purchased for use by the customer.

Create Application Record IDs (ARIDs) for the components to license the MiVoice Border Gateways, MiVoice Business controllers, MiCollab, MiCollab Client Service, and Open Integration Gateway in the architecture.

ULMs are required to deploy a MiCloud UCC solution and to use the unified communication bundles. DLMs must also be defined in order to share licenses for MiVoice Business Virtual instances, including survivable gateways, if applicable.

NOTE: Do not add MiCloud Management Portal to the ULM.

Prerequisites

- MiVoice Business scaling and cluster size has been determined.
- MiVoice Border Gateway scaling and cluster size has been determined for each specific service using the MBGs.
- Licenses have been deposited to the service provider’s account.

RESOURCE	CONTENT DETAILS
Mitel Connect	Log on at Mitel Connect and then log in to the AMC to see the licenses you have purchased.
MiCloud Business Blueprint	See the Licensing chapter.
AMC Training	UCC licensing training course at Mitel University.
Managed Service Provider Program	
MiCloud Business for Service Providers Licensing Structures	
Managed Service Provider Program Service Provider AMC Licensing Best Practices	

Synchronize to AMC

Synchronize the servers with the AMC to make sure that all of the licenses are activated and ready to assign.

On the Mitel Standard Linux (MSL) status panel:

1. Put ARIDs for each platform (each MiVoice Business, each MiCollab, and each MiVoice Border Gateway) on to the Mitel Standard Linux (MSL) status panel.
    a. Under **ServiceLink**, click **Status**.
    b. Enter the ARID.
2. Enter the IP address for the AMC so that MSL can reach the AMC. (This is probably done through a proxy, so use the proxy address).
3. Click **Activate** to synchronize the licenses with the platforms.

Prerequisites

- MSL is installed.
- ARIDs have been assigned for all the platforms to be deployed.

RESOURCE	CONTENT DETAILS
Mitel Standard Linux Installation and Administration Guide	See “Online Activation”.

Install a DNS server for the Customer management plane

A Mitel Standard Linux or third-party DNS server is used on the management VLAN to resolve management component addresses and UCC component addresses to addresses in the management VLAN. The DNS entries in this server are needed to access the management addresses for the customer platforms from within the service provider management plane that may be presented on the MMG or vCNS 1:1 NAT device being used to access the customer network.

A DNS server may also be required in the customer address space to allow installed platforms to reference each other locally.

- Add DNS entries for MiCloud Management Portal LAN facing (portal) interfaces.
- Add DNS entries for publicly accessible DNS services to allow customers to reach the external public address presented by the MiCloud Management Portal.

The external components that will act as Teleworker devices must be registered with external DNS servers to allow end-users to get to the correct unified communication and voice portals.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
Mitel Standard Linux Help	DNS Server topics
Third-party DNS server documentation	Installation and configuration instructions

Add management DNS, customer DNS, and public DNS entries

In the management DNS, add FQDNs that resolve to the customer platform management addresses mapped into the Service provider Management Plane.

- In the customer DNS, add FQDNs that map to the management addresses of the platforms in the hosted customer network.

- In external and/or public DNSs, add FQDNs and public addresses for the gateways; reaches to MiVoice Border Gateway WAN interface, but public IP address may be the MiVoice Border Gateway WAN interface or external firewall interface depending on networking.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
Third-party Windows DNS server documentation	Installation and configuration instructions

Configure UCC platforms for MiVoice Business Express (SMB architecture)

To configure UCC platforms for MiVoice Business Express, continue with these three steps before returning to the shared task flow.

- Configure and cluster external MBGs (SMB)
- Configure MiVoice Business Express
- Optional: Configure MiVoice Business resilient controller

Configure and cluster external MBGs (SMB)

This step configures MiVoice Border Gateway capabilities for customer access (including Teleworker), SIP Trunk and Web Proxy.

NOTE: There may be 0-4 MiVoice Border Gateways. If there are fewer than two MiVoice Border Gateways, clustering is not necessary (or possible).

The MiVoice Border Gateway (MBG) in the MiCollab server is clustered with the stand-alone MBG servers allowing remote management of the Teleworker service from the MiCollab server in the LAN. Both the MiCollab server and MBG server must have the Teleworker service installed. However, Teleworker phones are not supported on the LAN. You use the Teleworker service only on the MiCollab server to remotely manage the Teleworker phones on the MiVoice Border Gateway server.

NOTE: Update Emergency Location information for customer with SIP Trunk provider. Ensure that updates are passed through to the local Public Safety Answering Point (PSAP).

Example - One MBG cluster:

In the case of two external MBGs and one internal MBG (included in the MiCollab), choose the internal MBG as the primary/master and the external MBGs as the slaves. All three MBGs can be put in a cluster. MiCloud Management Portal writes only to the Master MBG.

Example - Teleworker cluster and SIP cluster:

For large deployments that split Teleworker and SIP clusters, the MiCollab internal MiVoice Border Gateway is master for the Teleworker cluster. One of the external MBGs is the master for the SIP cluster.

NOTE: MiVoice Border Gateway currently displays a warning when performing this operation. If all of the guidelines for clustering in MiCollab have been followed, the warning can be dismissed

Prerequisites

- Depending on the size of the installation, the MiVoice Border Gateways may also be used for the SIP trunks. In a large installation, Teleworker service and SIP trunks may be on separate MBGs.

RESOURCE	CONTENT DETAILS
MiCollab Engineering Guidelines	See “MiCollab with MBG Teleworker & Web Proxy Configuration”.
MiCloud Solutions Blueprint	Review the use and configuration of the MiVoice Border Gateways in the MLB and SMB topologies.

Configure MiVoice Business Express

Configure the MiVoice Business Express by following the steps in the *MiVoice Business Express Deployment Guide*, "Configure System" chapter.

The general steps to follow:

- Power on MiVoice Business Express.
- Run the initial configuration wizard.
- Perform advanced configuration.
- Configure optional standalone MBG Virtual.
- Optional: Configure external MiVoice Border Gateway for SIP Trunk proxy (not usually required)

NOTE: Skip the step, "Configure Integrated Directory Services". This step is not used when provisioning is done with MiCloud Management Portal.

Prerequisites

- MiVoice Business Express has been installed.
- Optional: External MiVoice Border Gateways have been deployed. The internal MiVoice Border Gateway is usually sufficient for SMB deployments except in cases where Traffic or deployment configurations differ from the deployment guidelines.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See "Deploying Mitel virtual appliances in VMware". http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
MiVoice Business Express Deployment Guide	See "Configure system".
MiVoice Border Gateway Installation and Maintenance Guide	See "Installing MiVoice Border Gateway software"

Optional: Configure MiVoice Business resilient controller

This is an optional step.

1. Deploy an additional MiVoice Business controller. This is usually a 3300 ICP, deployed locally. This allows continued operation in the event of WAN loss, but does require additional external trunks to be provided for external connections. See also Configure on-site survivable gateway interfaces.
2. Configure it to match the MiVoice Business controller in MiVoice Business Express to make sure that it can be used to take over if MiVoice Business Express fails, or connection to it is lost.
3. In the MiVoice Business System Administration Tool:
    a. Configure the two MiVoice Business controllers to share using SDS, and perform a Sync operation.
    b. Configure the devices to use the two MiVoice Business controllers as Primary and Secondary.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
MiVoice Business Resiliency Guidelines	See the following help topics: • "Configuring a Cluster"
MiVoice Management Portal Installation and Administration Guide	See the following help topics: • "Configuring a Cluster"

RESOURCE	CONTENT DETAILS
Using System Data Synchronization Solutions Guide	Description and instructions for System Data Synchronization (SDS) among MiVoice Business and MiCollab network elements.

Configure UCC Platforms on MiVoice Business (MLB architecture)

To configure UCC platforms for MiVoice Business Virtual, continue with these three steps before returning to the shared task flow.

- Configure MiCollab
- Configure and cluster external MBGs (MLB)
- Configure and cluster MiVoice Business instances

Configure MiCollab

License and install the MiCollab OVA.

NOTE: If you need more capacity, you can use up to 3 MiCollabs by adding them into your MiVoice Business cluster (System Administration Tool, **Network Elements** Form). For details, see the MiVoice Business System Administration Tool Help and the Multi-MiCollab Scaling instructions.

Licensing includes creating a ULM, which involves registering with a MiVoice Business instance.

Prerequisites

- MiCollab Virtual and MiVoice Business and MiVoice Business Virtual licenses have been purchased.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”. http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
MiCollab Installation and Maintenance Guide	See the following: • “UCC Licensing” • “Installing Virtual MiCollab in a VMware environment”
Multi-MiCollab Scaling	

Configure and cluster external MBGs (MLB)

This step configures MiVoice Border Gateway capabilities for customer access (including Teleworker), SIP Trunk and Web Proxy.

NOTE: There may be 0-4 MiVoice Border Gateways. If there are fewer than two MiVoice Border Gateways, clustering is not necessary (or possible).

The MiVoice Border Gateway (MBG) in the MiCollab server is clustered with the stand-alone MBG servers allowing remote management of the Teleworker service from the MiCollab server in the LAN. Both the MiCollab server and MBG server must have the Teleworker service installed. However, Teleworker phones are not supported on the LAN. You use the Teleworker service only on the MiCollab server to remotely manage the Teleworker phones on the MiVoice
Border Gateway server.

NOTE: Update Emergency Location information for customer with SIP Trunk provider. Ensure that updates are passed through to the local Public Safety Answering Point (PSAP).

Example - One MBG cluster:

In the case of two external MBGs and one internal MBG (included in the MiCollab), choose the internal MBG as the primary/master and the external MBGs as the slaves. All three MBGs can be put in a cluster. MiCloud Management Portal writes only to the Master MBG.

Example - Teleworker cluster and SIP cluster:

For large deployments that split Teleworker and SIP clusters, the MiCollab internal MiVoice Border Gateway is master for the Teleworker cluster. One of the external MBGs is the master for the SIP cluster.

NOTE: MiVoice Border Gateway currently displays a warning when performing this operation. If all of the guidelines for clustering in MiCollab have been followed, the warning can be dismissed

Prerequisites

- Depending on the size of the installation, the MiVoice Border Gateways may also be used for the SIP trunks. In a large installation, Teleworker service and SIP trunks may be on separate MBGs.

RESOURCE	CONTENT DETAILS
MiCollab Engineering Guidelines	See “MiCollab with MBG Teleworker & Web Proxy Configuration”.
MiCloud Solutions Blueprint	Review the use and configuration of the MiVoice Border Gateways in the MLB and SMB topologies.

Configure and cluster MiVoice Business instances

Configure a resilient MiVoice Business cluster. Start by establishing inter-connectivity between the MiVoice Business instances. Clustering allows sharing of configuration parameters, and telephone programming among cluster members. It also allows provision of a backup controller when service is lost on the primary MiVoice Business instance.

Install and cluster MiVoice Business instances.

Cluster the MiVoice Business instances with MiCollab to enable Flow Through Provisioning and do an SDS Sync operation. Up to three MiCollabs can be added to the cluster, if additional user capacity is needed.

Prerequisites

- MiVoice Border Gateways are already installed.

RESOURCE	CONTENT DETAILS
MiVoice Business Cluster Design and Implementation	Creating a MiVoice Business cluster is a four-step process. Use the following sections: • “Prepare elements for clustering” • “Populate the Network Elements form” • “Create the cluster” • “Start sharing data via SDS”
Using System Data Synchronization Solutions Guide	Description and instructions for System Data Synchronization (SDS) among MiVoice Business and MiCollab network elements.

Configure on-site survivable gateways as needed

Configure the interfaces for the survivable gateways.

Automatic Route Selection (ARS) for the survivable gateway

NOTE: ARS can also be used for local trunks.

In the event of a SIP Provider Service failure in the trunking survivable topology or a hosted connection failure, Emergency (E911) calls are routed through the local trunking gateway or on-premise MiVoice Business. Users typically have a CESID associated with the SIP trunks.

When end-users dial out the local trunks, their CESID is presented. It is important that the service provider recognize which PSAP the customer is associated with so that 911 calls that exist on either the local gateway, or via the central SIP trunks, go to the same PSAP, and therefore the same emergency services.

To resolve this issue, use SIP trunks that do not use registration from the same SIP carrier on both the hosted and local trunk gateway. If the hosted MiVoice Business or data connection to the hosted MiVoice Business fails, 911 calls are routed out the local gateway SIP trunks.

Emergency routes for survivable mode

Configure emergency routes for survivable mode to ensure that emergency calls from within the customers' networks reach the local Public Safety Access Point (PSAP).

Prerequisites

- The resilient MiVoice Business controllers must be deployed.

RESOURCE	CONTENT DETAILS
MiCollab Engineering Guidelines	See the considerations in "E911 Call Routing".

Optional: Deploy Open Integration Gateway instances

Install and configure the OIG Virtual. The OIG provides a platform for creating custom applications or for using MiVoice Integrations for Google or Salesforce.

NOTE: MiCloud Management Portal does not manage OIG instances, so OIG instances do not need to be registered with the Management Portal. OIG must be managed separately.

One OIG instance is generally required for each Customer. Deployments of more than 1500 end-users require multiple OIGs. See the *Open Integration Gateway Engineering Guidelines* for details.

In the OIG Server-Manager, select the Application Accounts tab. If desired, select one of the supported applications:

- MiVoice Integration for Salesforce
- MiVoice Integration for Google

Program a password for each application selected. User provisioning for these applications is done in Optional: Provision users for MiVoice Integrations**.**

In each MiVoice Business instance:

1. Add the OIG to the MiVoice Business Network Elements form as a member of the SDS Cluster.
2. Click Start Sharing and do a full SDS Synchronization. This allows end-users a simpler configuration because only the end-user DN is required.
3. The OIG then automatically finds the Call Server IP address.
4. Optional: Connect to MiContact Center Business for use with Salesforce. See the MiContact Center and Business Reporter System Engineering Guide.

Prerequisites

- Additional security programming is now required for Google integration with OIG 3.0. Pay particular attention to CA Certificate management. Refer to the OIG Resource below.
- Public Internet access is provided from the customer network.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
OIG Installation and Maintenance Guide	See “Install virtual Mitel OIG software”.

Optional: Deploy a customer backup server

Deploy a customer backup server to store backups. The backup server is an FTP server created inside the customer network space as a local machine.

Prerequisites

- A server is available for use in performing backups.

RESOURCE	CONTENT DETAILS
Third-party server documentation	
Third-party back-up software documentation	

Step 6 (Optional) Deploy CRM Integrations

If your customers will require integration of their CRM with the MiVoice Business Call Server, you can choose one of the following options:

- MiVoice Integration for Salesforce
- MiVoice Integration for Google

Prerequisites

- MiVoice Business, MiVoice Border Gateway, and Open Integration Gateway are licensed and installed.
- The Customer has a supported CRM licensed and installed.

Deploy MiVoice Integration for Google/Salesforce

Deploy Mitel Open Integration Gateway with MiVoice Integration for Google or MiVoice Integration for Salesforce.

1. Deploy Mitel Open Integration Gateway (OIG).
    - Optional: Configure E.164 calling directory.
    - Optional: Install and configure MiVoice Integration for Google.
    - Optional: Install and configure MiVoice Integration for Salesforce.
    - Purchase and configure Salesforce CRM.
    - Optional: Connect Salesforce to MiContact Center Business for ACD calling from Salesforce (special licensing required).
2. In the OIG Server-Manager, select the Application Accounts tab. If desired, select one of the supported applications:
    - MiVoice Integration for Salesforce
    - MiVoice Integration for Google
3. Program a password for each application selected. User provisioning for these applications is done in Provision users for MiVoice Integrations.
4. Configure the MiVoice Integration using the applicable guides. See table, below.

Prerequisites

- All of the core UCC OVAs must already be in place, specifically MiVoice Business, MiCollab, and MiVoice Border Gateways.
- If you are deploying MiVoice Integration for Salesforce with ACD calling, MiContact Center Business must be installed and configured.
- Mitel Open Integration Gateway, MiVoice Integrations, and Salesforce licensing (if applicable) must be in place.

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”. http://edocs.mitel.com/TechDocs/BP-Virtualization.pdf
Mitel product-specific documentation, including Installation Guides and Engineering Guides	**Mitel Connect** > **eDocs** Login credentials are required for access to Mitel Connect.
VMware documentation	https://www.vmware.com/support/pubs/
Mitel OIG Installation and Maintenance Guide	To install OIG, see “Installing the Mitel OIG”. If you will be using OIG with MiContact Center Business and Salesforce, see “The Network Elements Tab”.
Mitel OIG Engineering Guidelines	For requirements and capacity.
MiVoice Integration for Google Administration Guide *MiVoice Integration for Google Quick Reference Guide*	For instructions for installing and configuring MiVoice Integration for Google.

RESOURCE	CONTENT DETAILS
MiVoice Integration for Salesforce Administration Guide	For installing and configuring MiVoice Integration for Salesforce with OIG and MiContact Center Business.
MiVoice Integration for Salesforce Troubleshooting Guide	Troubleshooting MiVoice Integration for Salesforce
MiVoice Integration for Salesforce User Guide	User info for MiVoice Integration for Salesforce.

Step 7 Configure UCC platform services with MiCloud Management Portal

Configure customer services including:

- Feature Bundles
- Custom branding
- Emergency services access

This work was introduced in Define MiCloud Management Portal User Bundles.

Prerequisites

- Person deploying has been trained on MiCloud Management Portal.
- Customer branding components, such as logo, colors, custom banner, and browser-tab favicon have been created, and are available.
- Feature Bundles have been created in MiCloud Management Portal. See Configure external access to MiCloud Management Portal in the MiCloud Management Portal Help.

Register UCC platforms with MiCloud Management Portal

Associate a platform group to an customer to connect the MiCloud Management Portal profile of the customer with the platform group that includes the components providing the same customer's services. Use the Register Platform wizard to register MiCollab and any external MiVoice Border Gateways (MBG).

1. Register the Mitel products in MiCloud Management Portal.
    - one or more MiVoice Border Gateways
    - MiCollab
2. When registering MiCollab platforms in a Multi-MiCollab configuration, there are additional steps in the registration operation:
    a. From the **Type** drop-down list, select **MiCollab**. and enter the following information:
        i. Host Name
        ii. Public Facing FQDN/IP Address
        iii. MSL Username
        iv. MSL Password
        v. Description
    b. After registering one or more new MiCollabs, save the customer in the Management Portal **Customer Details** tab.
    c. After adding the new MiCollabs, log in to the MiVoice Business, and perform an SDS Sync with each additional MiCollab you just registered.
3. If you will be provisioning mobile users, you must include the following steps in the MiCollab registration:
    a. Select **Use Embedded MiVoice Border Gateway**.
    b. In **Public Facing FQDN of External MBG**, enter the FQDN for the Teleworker MiVoice Border Gateway.
4. Optional: To provision MiCollab MiTeam users (Premium Bundles only), include the following steps in the MiCollab registration:
    a. In **Platforms > Edit Platform > MiCollab Client Tenant** tab, select **MiTeam Services**.
    b. Click **Save.**
5. Optional: If you are enabling SIP trunking, you can both enable MiTeam and set up SIP trunking from MiCollab Client Service.
    a. Select **Configure MiCollab Client Service**, and click the **Enterprise** tab.
    b. Scroll to **MiTeam Configuration Settings**.
        i. Enable **MiTeam Configuration**.
        ii. In **Telephone Domain Configuration**, select **Custom**.
        iii. In the table that appears, enter a **Label** name (Canada, for example).
        iv. In **Number**, enter the DID number to use for the MiTeam service, (e.g. +14802409721). You can get the number that applies for your location from the Mitel Partner who is assisting with your deployment.
        v. Click **Apply**.
6. Optional: To enable the emergency call warning on SIP clients:
    a. In **Platforms > Edit Platform > MiCollab Client Tenant** tab, select **Enable emergency call warning**.

b. Click **Save**.

The warnings appears as follows:

- On mobile devices: “Emergency calls will be routed through your mobile operator.”
- On web clients: “The built-in phone application cannot be used for emergency calls. You must make alternative communication arrangements to ensure you can make emergency calls if necessary.”

NOTE: MiVoice Business instances and the embedded MiVoice Border Gateway are reached through MiCollab; they are not directly registered with MiCloud Management Portal.

7. Create Sites for the MiVoice Business controllers. All of the MiVoice Business controllers may be in one site. (**Sites** tab on the **Create Platform** page).

Prerequisites

- None

RESOURCE	CONTENT DETAILS
MiCloud Business for Service Provider Help	See Set up platform groups. When using multiple MiCollabs, see **Set up multiple MiCollab platforms within a network** in 4.0 version
MiTeam for MiCollab and MiCloud Business Virtual Reference Guide	

Create MiCloud Management Portal customer for UCC platform

Use the MiCloud Management Portal Create Customer wizard to create a customer.

- Assign bundles and licenses to the customer.
- Assign the customer's DIDs - In the Management Portal, assign the customer DIDs to configure the range or list of DIDs for the customer to use.

NOTE: This can may be done at this step or when associating a platform group with a customer.

- Assign emergency location information - Collect emergency location information to update the SIP trunk provider with all the emergency location details for the customer that could be used in emergency situations for first responders.
- Assign custom branding - Assign a custom brand for each individual customer.

  Each customer can have their management portal customized with their company logo and colors, along with a custom banner and browser-tab favicon image (tab graphic). This step assumes that this branding and logos have already been created.

NOTE: This branding refers only to MiCloud Management Portal branding. To brand other aspects of the solution (clients, for example), contact Mitel to ask about the Branding Program.

- Create an customer's user administration account - Create a customer’s user administration account. This account is used to build an administrator profile in the Management Portal for each customer for end-user administration. The customer uses the administration account to manage its own end-users. The service provider will also use this account for end-user changes when necessary.
- If the customer will have users who will use MiCollab Client on Mac computers, on the Service Bundles screen, 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**.

Prerequisites

- Calling Party Number (CPN) already exists. CPN is not enforced, but it is good practice to ensure that it is entered.
- Custom branding has been created

RESOURCE	CONTENT DETAILS
MiCloud Business for Service Providers Help	See “To assign a Platform Group to a customer”.

Assign Bundles to customer

Use the MiCloud Management Portal Create Customer wizard.

- Assign bundles and licenses to the customer.
- Assign the customer's DIDs - In MiCloud Management Portal, assign the customer DIDs to configure the range or list of DIDs for the customer to use.

NOTE: This can may be done at this step or when associating a platform group with a customer.

- Assign emergency location information - Collect emergency location information to update the SIP trunk provider with all the emergency location details for the customer that could be used in emergency situations for first responders.
- Assign custom branding - Assign a custom brand for each individual customer. Each customer can have their management portal customized with their company logo and colors, along with a custom banner and browser-tab favicon image (tab graphic). This step assumes that this branding and logos have already been created.

NOTE: This branding refers only to MiCloud Management Portal branding. To brand other aspects of the solution (clients, for example), contact Mitel to ask about the Branding Program.

- Create an customer's user administration account - Create a customer's user administration account. This account is used to build an administrator profile in the Management Portal for each customer for end-user administration. The customer uses the administration account to manage its own end-users. The service provider will also use this account for end-user changes when necessary.
- If the customer will have users who will use MiCollab Client on Mac computers, on the Service Bundles screen, 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**.

Prerequisites

- Calling Party Number (CPN) already exists. CPN is not enforced, but it is good practice to ensure that it is entered.
- Custom branding has been created and components are ready to be assigned.

RESOURCE	CONTENT DETAILS
MiCloud Business for Service Provider Help	See Set up platform groups.

Step 8 Provision UCC platform end-users

Provision UCC platform end-users with MiCloud Management Portal.

Prerequisites

- Customer is set up and configured.
- No end-user IP phones are registered prior to provisioning users in MiCloud Management Portal, or if there are phones registered, they are removed before provisioning, at all connection levels, including MiCollab, MiVoice Business and MiVoice Border Gateway.

Bulk import end-users

Bulk import end-users into MiCloud Management Portal to initially create the end-user accounts for a customer. Only the service provider can complete a bulk import of end-user profiles.

NOTE: Users can be created by the service provider, the customer, or administrator users. This Bulk import facility is available only to service providers.

Before importing the users, it is important that no users have phones registered. To prevent this, set an installer password on the MiVoice Border Gateway, but do not publish it to the end user. This will prevent the MiNet device from registering with the MiVoice Border Gateway if they plug the phone in before the Management Portal can program the MiVoice Border Gateway. After MiCloud Management Portal programs the MiVoice Border Gateway, any phones in displaying the Installer Password Prompt must be reset manually.

The following procedure adds end-users to MiCloud Management Portal and to the MiCollab; then the end-users are propagated through to the MiVoice Business instances in the network. From the MiVoice Business, users are also synchronized with MiContact Center Business to provision users there.

NOTE: Paths and groups are programmed directly on the MiVoice Business using the System Administration Tool.

NOTE: MiContact Center Business hot desk users are currently available only IPT Basic and Standard licensing; MiContact Center Business Premium licensing does not support hot desk users.

Import users using MiCloud Management Portal

NOTE: If you configure users in MiCollab, outside of Management Portal, you must also set UCC licenses and roles in MiCollab. If you set the UCC licenses and roles in Management Portal you could be charged for premium licenses through Management Portal on those users.

Prepare a MiCloud Management Portal import spreadsheet:

Use the import spreadsheet template to create a file containing the users to import. There are two ways to prepare an import spreadsheet:

1. Download the import spreadsheet template.
    a. Add the users manually or by copying from another user list.
    b. Modify the spreadsheet to add the appropriate phones to each user.
    c. Save the file.
2. Import users from an Active Directory database. If a Customer has their users in an Active Directory Database, you can do a first import of their users as part of their setup. For detailed instructions, see Map Active Directory Fields for Bulk Import in the *MiCloud Management Portal Help*.
    a. Have the customer export their users from Active Directory to an LDIF file.
    b. Log in to the Service Provider Portal as the customer (Log in As).
    c. In the Management Portal, upload the LDIF file map the LDIF attributes to import spreadsheet fields.
    d. Assign the bundles to the users.

e. Download the new import spreadsheet and edit it to remove any errors and add any phones that may be missing.
f. Save the file.

In the Service Provider Portal:

1. In the main portal of MiCloud Management Portal, click **Customers > Bulk Import**.
2. Click **Import Users**.
3. From the **Customer** pull-down menu, select the customer to add end-users and shared devices to.
4. Click the icon beside the Customer pull-down menu to get the bulk import spreadsheet template for that customer.
5. Add the new users and shared devices to the spreadsheet.
    a. For ACD soft phones, create each shared device with **Phone Type** = **PC MiNet Softphone**.
    b. Create the Softphone using the "*" format. For example, if the user extension is 1234, create a shared device 1*234.
6. Save the spreadsheet and import the file. This is done under **Step 2** of the **Import** page.
7. Click **Submit** to start the bulk import. A status bar provides a progress indication of the import process.

Adjust the ACD soft phone users/devices

1. In MiCloud Management Portal, set up the ACD paths and ACD groups for the ACD agents.
2. In the MiVoice Business, log in to the System Administration Tool, open the **User and Services Configuration** form. Edit the **Device Type** for each user; select **5020 IP**.
3. After the phones have been setup and configured as specified here, use the MiVoice Business System Administration Tool to configure any advanced paths and group options that are not configurable from MiCloud Management Portal.

Prerequisites

- No end-user IP phones are registered prior to provisioning users in MiCloud Management Portal. If there are phones registered, they must be removed before provisioning users.

Administer end-users

In MiCloud Management Portal, administer end-users to add, edit, or remove individual end-users using the customer's user administration account. User administration can be a customer, service provider, or reseller task depending on the negotiated service contract.

User administration is a manual per-user process and does not accommodate bulk change requests.

Customers also use their Customer Portal to add, provision, and delete:

- Ring groups, Hunt groups, and Pickup groups
- Group paging
- Call flows
- Auto attendants
- Voice prompts, music on hold, and auto attendant messages
- ACD groups and paths. The following forms are updated in the MiVoice Business System Administration Tool:
    - ACD Skill Group
    - ACD Path Assignment

NOTE: Customer Admins may have full or limited ACD, RAD, and MOH programming capabilities, depending on the privileges included in their Admin Bundles. This is programmed on the **Select Features** page. See Assign Customer Admin features.

Prerequisites

- Administrator access is provisioned for the customer in Oria.

RESOURCE	CONTENT DETAILS
MiCloud Business for Service Providers Help	For ring groups, hunt groups and pickup groups, auto attendant, etc.: • Configure the default database For music on hold and ACD features: • Create and change bundles

Configure telephony users

In MiCloud Management Portal, configure ring groups, hunt groups, and automatic call distribution (ACD) functions to ensure that incoming calls are appropriately distributed and assigned for the customer's business hours, location, and staffing.

ACD agents are programmed as Hot Desk agents.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
MiCloud Business for Service Providers Help	See Create and change bundles See Set Up Customer

Tune the deployment

Make required modifications to the configuration to meet any unique requirements for the deployment. There are many settings in both MiVoice Business, MiCollab, and MiVoice Border Gateway that are not available from MiCloud Management Portal.

You may have different end-user types and roles that need custom configuration, for example; settings you cannot automate, like Class of Service and Class of Restriction. You may also want to configure the applications.

NOTE: Be careful of tuning parameters that can also be set from MiCloud Management Portal, because the value or values you set could be overwritten by MiCloud Management Portal at the next update.

NOTE: Call Mitel Professional Services for any tuning in MiCloud Management Portal.

Deploy phones and clients

Deploy phones and clients to connect and activate the customer's devices on the MiCloud solution.

The customer must deploy DNS and DHCP servers, and have these programmed to the correct MiVoice Business unit and MiCollab. There may also be a requirement to program external DNS for mobile clients that need to connect via the customer MBG as Teleworker devices.

Before importing the users, it is important that no users have phones registered. To prevent this, set an installer password on the MiVoice Border Gateway, but do not publish it to the end user. This will prevent the MiNet device from registering with the MiVoice Border Gateway if they plug the phone in before MiCloud Management Portal can program the MiVoice Border Gateway.

After MiCloud Management Portal programs the MiVoice Border Gateway, any phones in displaying the Installer Password Prompt must be reset manually.

For MiContact Center Business agents that will be working remotely:

Each agent must install MBG Connector on their station.

1. Click **Start > Programs > Mitel**.
2. Enter the name and IP address of the MiVoice Border Gateway to connect to.
3. Enter the phone MAC address.
4. Optional: Enter the IP phone extension.

After the MBG Connector has connected, users can access all MiContact Center Business and MiVoice Business Reporter applications as if they were in the office.

While active, MBG Connector is visible in the Windows system tray. The current number of active number connections is displayed. Users configured as supervisors in YourSite Explorer can manage MBG connections.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
MiCloud Management Portal Installation and Administration Guide	See Users.
MiContact Center Installation and Administration Guide	See “Setting up phones for remote agents and employees”.

Optional: Prepare MiCollab Client for mobile users

This step also includes instructions for deploying MiCollab MiTeam for MiCloud Management Portal Next Gen clients (iPhone, iPad, and web client on Mac or PC).

Using the MiCollab Client Mobile simplified deployment method (Next Gen Mobile Phone), mobile users receive an e-mail with a link that allows quick and easy installation of MiCollab Client on their mobile devices.

1. Purchase and install third-party SSL certificates on MiCollab and MiVoice Border Gateway for the Service Provider and for every customer connected. See the MSL Online Help: “Manage Web Server Certificate”.
2. If you are configuring soft phone resiliency, on the Manage MiCollab Client Deployment screen, follow the instructions in the MiCollab Client for Mobile Resiliency Guide, “Configuration” section, with the following exception: **IGNORE** the section, “Specify FQDN of MBG Cluster”.
3. If users are configured to use MiTeam, ensure that the MiCollab Audio, Web and Video Conference service is running.
4. In the MiCollab Client Configuration Tab, customize the Deployment e-mail. This step customizes the message each user receives; this e-mail includes a link for downloading and installing the MiCollab Client soft phone on the user’s mobile devices. For details, see MiCollab Client Deployment Help topic, “Mobile Client Deployment Email”.
5. Apply branding (your company logo and custom colors), if required. In the **Configuration** tab, under **Branding Settings**, select **Activate Custom Branding**. Enter the **Branding ID** and **Branding Secret**. Branding can be added to the Next Gen clients. Contact your sales representative for information about creating your branding ID and password.
6. In MiCloud Management Portal, add the MiCollab Client users. See the MiCloud Business for Service Providers Help.

Prerequisites

- The base network is complete (MiVoice Business instances installed, connected and sharing using SDS, MiCollab instances installed and connected to MiVoice Business cluster using SDS, MiVoice Border Gateways installed, clustered, and connected to the network.)
- The same certificate for the external MBG is also required for the MiCollab MBG. If a certificate is required to install on the MBG, MiCollab Teleworkers will not be able to login if a certificate has not been installed on each MBG. For detailed instructions, see the MSL Online Help; search for the “Manage Web Server Certificate” topic.

RESOURCE	CONTENT DETAILS
Mitel Standard Linux (MSL) Online Help	See “Manage Web Server Certificate”.

RESOURCE	CONTENT DETAILS
MiCollab Client Deployment Help	See the following help topics: • "About MiCollab Client Deployment • "Deploy Client with MiVoice Business or MiVoice Business Express" • "Run Diagnostics" • "Mobile Client Deployment Email"
MiCollab Client for Mobile Resiliency Guide	Follow the instructions in "Configuration", with the following EXCEPTION: • IGNORE the section, "Specify FQDN of MBG Cluster".
MiCloud Management Portal Installation and Administration Guide	See the following topics: • Register MiVoice Border Gateway (See "DNS Resiliency on MiCollab Client Server for Mobile Softphones") • Add a Next Gen Mobile Softphone • Create brands
MiTeam for MiCollab and MiCloud Business Virtual Reference Guide	

Optional: Provision MiVoice Integrations users

Add users to MiVoice Integration for Salesforce and/or MiVoice Integration for Google.

Provision users for MiVoice Integration for Salesforce.

Enable Salesforce users for MiVoice Integration for Salesforce.

Administrator actions

Administrator actions are performed in Salesforce by a Salesforce Administrator.

1. In Salesforce, add the MiVoice Integration for Salesforce package.
2. Create Salesforce Call Centers and connect them to the MiVoice Integration package.
3. Associate MiVoice Integration for Salesforce with the Call Centers.
4. Associate each user with a Salesforce Call Centers.

User actions

- None

Provision users for MiVoice Integration for Google

MiVoice Integration for Google Extension must be installed by each end-user.

Administrator actions

1. Install MiVoice Integration for Google. See the *MiVoice Integration for Google Administration Guide*.
2. Create a Google integration template and obtain a list mapping of Google accounts to DN in CSV format for import to the OIG server.

3. In Mitel Standard Linux, in the OIG, import the user list (CSV file) into MiVoice Integration for Google. The user list must contain a DN for every user name for the user to use the application. See the *Open Integration Gateway Installation and Maintenance Guide* for detailed instructions.
4. Notify users that the new MiVoice Integration for Google Extension is available. Send instructions for upgrade; *MiVoice Integration for Google Quick Reference Guide* contains the instructions.

User actions

1. Each user must follow the steps in the *MiVoice Integration for Google Quick Reference Guide* to add and configure MiVoice Integration for Google.

Prerequisites

- Open Integration Gateway (OIG) is installed. The MiVoice Integrations are purchased and licensed.

RESOURCE	CONTENT DETAILS
MiVoice Integration for Salesforce Administration Guide	To install and configure MiVoice Integration for Salesforce, follow all instructions in this guide.
MiVoice Integration for Google Administration Guide	To prepare for MiVoice Integration for Google for deployment by users, follow all instructions in this guide.
MiVoice Integration for Google Quick Reference Guide	Each user must follow the instructions in this guide to add the Google Extension to their browser.
Open Integration Gateway Installation and Maintenance Guide	MiVoice Integration for Salesforce: • To connect the OIG to MiContact Center Business for integration with Salesforce, see “Network Elements Tab”.

Synchronize users with MiContact Center Business

If MiContact Center Business is installed, synchronize MiContact Center Business with MiVoice Business to provision users in MiContact Center Business. The following procedure copies users from MiVoice Business to the MiContact Center Business server.

To synchronize contacts with MiVoice Business network:

1. Log in to YourSite Explorer.
2. Under **Enterprise**, click **Media servers**.
3. Select a MiVoice Business media server from the list.
4. Click the **Telephone system** tab.
5. In the ribbon at the top of the window, specify the settings to use with synchronization. See the *MiContact Center User Guide* for details.
6. In the ribbon, select **Read/Write**.
7. Click **Run**.
8. In the Synchronization window that appears, select the media servers to synchronize.
9. Select **Full synchronization**.
10. Select the telephone system media servers and devices to include in synchronization. All media servers and devices are selected by default.
11. Select **Synchronize** to synchronize the devices programmed on the telephone system.
12. The Synchronization Report is displayed. Choose the desired options and complete the synchronization.
13. Perform manual synchronization for any items that are not synchronized automatically.

Prerequisites

- Users have been provisioned in MiCloud Management Portal, and synchronized with MiVoice Business using SDS Synchronization.
- MiContact Center Business is up and running, and connected to a MiVoice Business controller.

RESOURCE	CONTENT DETAILS
MiContact Center User Guide	See "Performing Synchronization".

Step 9 Complete the deployment

Confirm that the following operation is complete:

- A customer addition has been completed correctly and the status of the account has been moved to an operations mode for accounting and billing.

Prerequisites

- All nodes and configurations are in place.

Obtain customer sign-off

Ensure that the deployment is tested and meets the expectations of the customer. Obtain customer sign off.

Obtaining sign off after deleting a customer may also be used to confirm that the customer understands that services are torn down.

Prerequisites

- An acceptance test has been agreed upon for installation acceptance.
- A method and process for obtaining customer sign-off.

Transition deployment to Operations

Transition a deployment to operations to complete the deployment and signal the start of the services contract. A formal transition is a milestone for billing and support functions to engage the customer.

Prerequisites

- None

Step 10 De-assign platforms

When a customer or the service provider terminates the contract, customer-clearing tasks must be completed.

In MiCloud Management Portal, when you delete a customer, the following is done:

- Delete platform
- Reclaim resources

Prerequisites

- None

Delete customer's MiCloud Management Portal profile

Delete a customer's MiCloud Management Portal profile to remove the connections between the license server, the platform group, and MiCloud Management Portal for the customer.

Prerequisites

- None

Clear customer configuration

Clear a customer configuration to remove the customer from the topology components when there is no longer a services contract in place between the customer and the service provider or reseller.

The MiVoice Business instances are turned off, and any references to the customer other network components, including MiVoice Border Gateways and MiCollab Client, will be removed. Databases will be cleared.

Remove the MiContact Center and MiVoice Call Recording license assignments to reclaim the licenses.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
MiVoice Business System Administration Tool Online Help	See the help topic: "Network Elements".
MiCloud Business for Service Providers Help	See Create and change bundles, particularly the sections describing the features of Administrator Bundles.

Delete the customer OIG Virtual instances

Delete the customer OIG Virtual servers to remove any OIG resources and applications deployed for this customer.

Each MiVoice Integration application must use the Mitel OIG local password (specific to each instance of Mitel OIG) to open a communication session with the OIG. To disable running MiVoice Integrations (Salesforce and Google) on a specific OIG Virtual, the Mitel OIG Administrator can delete or change the Mitel OIG local password used by the existing MiVoice Integrations.

The administrator for the Salesforce solution can remove a MiVoice Integration for Salesforce user by changing their user account. Removing the OIG call center from their user account removes MiVoice Integration for Salesforce from that specific user's web browser.

The Mitel OIG can also be removed using from the MSL server manager blades panel.

- Deleting the OIG Virtual used for a MiVoice Integration for Google has no impact on Google accounts. The Google account will show an error when it attempts to use the MiVoice Integration for Google gadget.
- Deleting the OIG Virtual used for a MiVoice Integration for Salesforce has no impact on the Salesforce account. The Salesforce account will display an error when it attempts to connect with MiVoice Integration for Salesforce.

Prerequisites

- None

RESOURCE	CONTENT DETAILS
Mitel Standard Linux Installation and Administration Guide	See “Install, Upgrade, Cache or Remove a Blade”.

Engage Mitel for license clean up

Engage Mitel Professional Services for licensing clean up to remove any assignment of licenses to the customer and return them to the license pool for reuse by the service provider.

Prerequisites

- None

Upgrade MiCloud Business (MiVoice Business Virtual)

Use this chapter to upgrade your MiCloud Business deployment. The MiCloud Business upgrade process is designed to be performed in a series of four-hour maintenance windows. It is important to follow the correct upgrade order, both to ensure that the system continues to run as the upgrade tasks progress, and also to minimize disruption for users.

It is recommended that you provision a test customer that you can use to test service restoration after you complete the system upgrade.

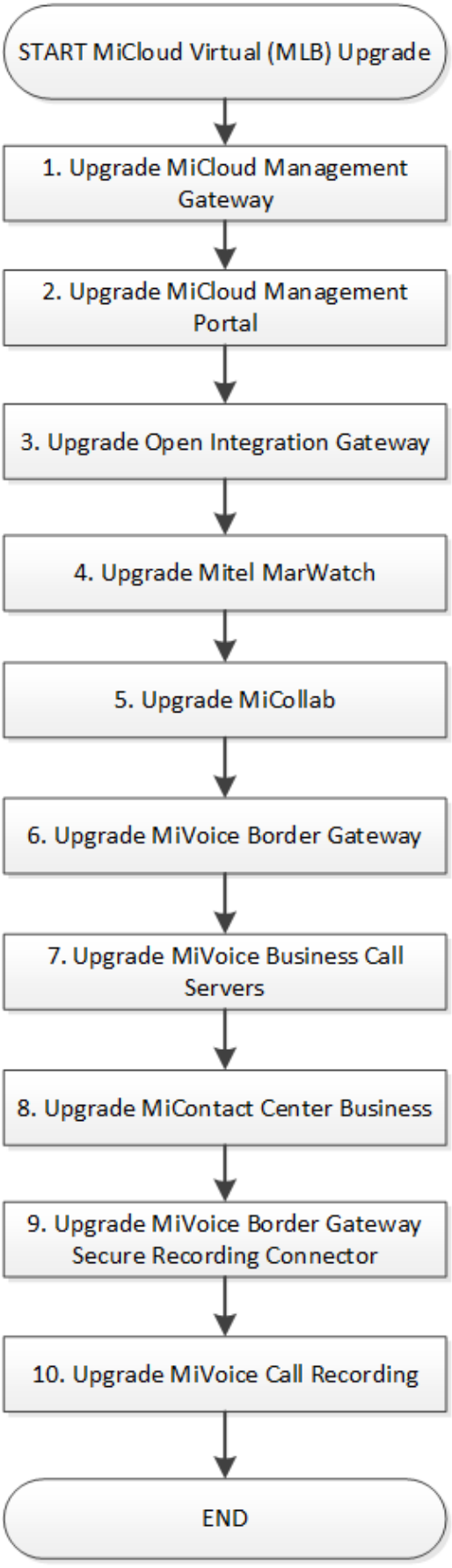
NOTE: To upgrade MiCloud Business Virtual from Release 2.0 to Release 4.1, you must perform the upgrade in two stages:

- Upgrade from MiCloud 2.0 to MiCloud 3.1: Follow the instructions in *MiCloud 3.1 Deployment Guide*.
- Upgrade from MiCloud Business 3.1+ or 4.0 to MiCloud 4.1: Follow the instructions in this guide.

CAUTION: Do not add or change users between backup and restore of any of the applications.

Prerequisites

- Prepare a full backup of every system and every database in the MiCloud system.
- Install certificates. These are needed for MiCollab and MiVoice Border Gateway for simplified mobile deployment.


START MiCloud Virtual (MLB) Upgrade
1. Upgrade MiCloud Management Gateway
2. Upgrade MiCloud Management Portal
3. Upgrade Open Integration Gateway
4. Upgrade Mitel MarWatch
5. Upgrade MiCollab
6. Upgrade MiVoice Border Gateway
7. Upgrade MiVoice Business Call Servers
8. Upgrade MiContact Center Business
9. Upgrade MiVoice Border Gateway Secure Recording Connector
10. Upgrade MiVoice Call Recording
END

1. Upgrade MiCloud Management Gateway

There are two ways to upgrade MiCloud Management Gateway (MMG).

- Install new MMG OVA.
- In MSL, use the Upgrade from Running feature to upgrade and move the database over to the new MMG. Note that you must have an extra IP address to perform the upgrade this way.

Primary resources:

- MiCloud Management Gateway Online Help (available from inside Mitel Standard Linux)
- Virtual Appliance Deployment Solutions Guide

Pre-upgrade tasks: None

		NOTES
Current Release	5.0 PR1	You may be replacing VMware vCloud Networking and Security (vCNS)
Upgrade to	5.0 PR1	
Pre-upgrade effort		
Time to upgrade (hours)	0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	All
Services available during upgrade	Admin	No management services available
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: Configure MiCloud Management Gateway interface. See MMG Online Help for instructions.

2. Upgrade MiCloud Management Portal

Primary resource: Upgrade MiCloud Management Portal in the Management Portal Help

Pre-upgrade tasks: Full MSL back-up

No administrative changes are allowed during the MiCloud Management Portal upgrade. If this is not acceptable, then create a back-up on a second machine and make your changes there. Then perform the upgrade, restore the back-up, and put the upgraded machine back into service.

		NOTES
Current Release	6.1 SP1	
Upgrade to	6.1 SP3 (6.1.xx.x)	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)	0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	All	
Services available during upgrade	None	
Services available after upgrade	All	
Services available after upgrade	All	

Post-upgrade tasks:

1. Adjust Customer Admin Bundles, if required. See Assign Customer Admin features.

    - If Customer Admin had ACD in their Bundle, then they will have the **ACD Groups** permissions and the **ACD Paths** permissions. You can add the **Advanced ACD Groups** and **Advanced ACD Paths** permissions to bundles used to create trained Customer Admins. See Assign Customer Admin features.
    - The **RAD Programming** feature is not enabled for existing Customer Admin Bundles at upgrade. You must reset the RAD source for existing customers.
2. At upgrade, Management Portal overwrites the RAD Ports, RAD indices, MOH indices.
3. After upgrade, for existing Platform Groups, the RAD group is set to None, and the RAD drop-down list will be empty.

NOTE: The Restore from Running Server option is not supported by MiCloud Management Portal.

NOTE: The 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 MiCloud Management Portal Services to start.

3. Upgrade Open Integration Gateway

Upgrade the OIG Blade from inside Mitel Standard Linux (MSL). You may also have to upgrade one or both of the MiVoice Integrations:

Primary resource:

- *Mitel Open Integration Gateway Installation and Maintenance Guide*

Upgrade tasks:

1. If MiVoice Integration for Salesforce is installed, uninstall the Salesforce blade.
2. If MiVoice Integration for Google is installed. E-mail (export) existing Google users to a CSV (which is sent to the configured e-mail address).
    - In the OIG, click the **Users** tab.
    - In **Import/Export Users**, confirm the e-mail address or configure a new one.
    - Click **Email Users**.
3. Upgrade Mitel Standard Linux to 10.5.15 or later 64 bit OS.
    - In the OIG blades panel install MSL 10.5.15+.

		NOTE
Current Release	4.0 SP1	
Upgrade to	4.1 SP3	
Pre-upgrade effort		
Time to upgrade (hours)	0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	All except for MiVoice Integrations MiVoice Integration for Salesforce: the hosted or premise-based application must be updated with a new MiVoice Integration for Salesforce package.
Services available during upgrade	Admin	All All functions of MiCloud continue operating during the OIG upgrade, except for OIG and MiVoice Integrations functions.
Services available after upgrade	User	All except for MiVoice Integrations MiVoice Integration for Google will be available to users after they are also updated to the latest version.
Services available after upgrade	Admin	All

Post-upgrade tasks:

- Upgrade Salesforce server and Google end-user extensions, if applicable. **NOTE**: The upgrade from OIG 4.0 to 4.0 SP1 does not require an upgrade of the MiVoice Integrations.
- Upgrade MiVoice Integration for Salesforce
- Upgrade MiVoice Integration for Google
- If using MiContact Center Business: After the MiContact Center Business install or upgrade, enable the OIG integration to MiContact Center Business. (MiContact Center Business must be at Release 8.0 or higher.) See the MiContact Center Installation and Administration Guide.

3a. Upgrade MiVoice Integration for Salesforce

MiVoice Integration for Salesforce (hosted or premise-based Salesforce application) must be updated with the new 2.1.6 Salesforce blade.

NOTE: The Salesforce package in the App Store does not require update.

Primary resources:

- MiVoice Integration for Salesforce Administration Guide

Pre-upgrade tasks:

- OIG is upgraded as described above.

Administrator steps for upgrade (this is done in Salesforce by a Salesforce Administrator):

NOTE: For details, see the *MiVoice Integration for Salesforce Administration Guide*.

1. In MSL, install the new MiVoice Integration for Salesforce 2.1.6 blade.
2. Make copies of all Salesforce Call Centers connected to the MiVoice Integration package you are upgrading.
3. Associate the new MiVoice Integration for Salesforce with the new copies of the Call Centers.
4. Associate each user with the new Salesforce Call Centers.

User steps for upgrade: None

		NOTES
Current Release	2.1.6	
Upgrade to	2.1.29	
Pre-upgrade effort	n/a	
Time to upgrade (hours)	Admin: 1.0 User: 0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	None
Services available during upgrade	Admin	All
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: None

3b. Upgrade MiVoice Integration for Google

MiVoice Integration for Google extensions must be uninstalled and reinstalled by each end-user.

Primary resources:

- *MiVoice Integration for Google Administration Guide*

Pre-upgrade tasks:

- OIG is upgraded as described above.
- Export or create the Google integration template and obtain a list mapping of Google accounts to DN in CSV format for import to the OIG server.

Administrator steps for upgrade:

1. Upgrade to MiVoice Integration for Google 1.1,20, if required. See the MiVoice Integration for Google Administration Guide.
2. Edit the user CSV for the new Import spreadsheet format. See the OIG 4.0 Installation and Maintenance Guide, Upgrade section, for details.
3. Import the new CSV Users file into MiVoice Integration for Google. The user list must contain a DN for every user name for the user to use the application.

User steps for upgrade: None

		NOTES
Current Release	1.1.20	
Upgrade to	1.1.20	
Pre-upgrade effort	n/a	
Time to upgrade (hours)	Admin: 0.5 User: 0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	None
Services available during upgrade	Admin	All
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: None

4. Upgrade Mitel Business Analytics

Primary resource: *Mitel Business Analytics Upgrade Guide*

Pre-upgrade tasks:

- Back-up application configurations; connections to monitored server/applications, and so on.

Mitel Performance Analytics reporting is affected by the in-progress upgrade, but MiCloud Management Portal and similar administrative services remain available.

NOTE: Probes are updated automatically after upgrade of the server.

		NOTES
Current Release	4.1	
Upgrade to	3.7	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)	1.0	
Roll-back time (hours)	1.0	
Services available during upgrade	User	All
Services available during upgrade	Admin	All
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: Check that the Mitel Performance Analytics application is running and fully functional.

5. Upgrade MiCollab

In this step, you should also upgrade MiCollab Speech Auto Attendant (SAA), if applicable.

Primary resource:

- *MiCollab Installation and Maintenance Guide*

The MiCollab MiVoice Border Gateway is the MBG cluster Master and must be upgraded before the slave MBGs are upgraded.

Ensure that Single Point Provisioning and MiCollab Client Service PBX Node Synchronization continue working through the upgrade by performing one of the following:

- Upgrade each MiCollab.
- Install a new MiVoice Business certificate on each MiCollab. Use the instructions in Mitel Knowledge Base Article 15-3829-00015_1. (MiVoice Business is upgraded in a later step, so this step is postponed until after the MiVoice Business upgrade is complete.)

NOTE: UC services including soft phones will be out-of-service during the MiCollab upgrade.

Pre-upgrade tasks:

- Request third-party certificate.

		NOTES
Current Release	8.0 SP2 FP2	
Upgrade to	9.0	
Pre-upgrade effort		
Time to upgrade (hours)	Without Speech Auto Attendant: 1.0 With Speech Auto Attendant: 2.0	
Roll-back time (hours)	1.0	
Services available during upgrade	User	Voice only: No UCC services are available during upgrade.
Services available during upgrade	Admin	None
Services available after upgrade	User	All
Services available after upgrade	Admin	All except for database changes and user provisioning

Post-upgrade tasks:

1. Apply the third-party SSL Web Server Certificate to MiCollab and to the external MiVoice Border Gateways.
2. User desktop clients will be prompted to upgrade at their next log-in.
3. Mobile clients will not receive an upgrade prompt. You must change the user bundle for the new Mobile client, and explicitly re-send the Deployment e-mail to the mobile users. Users will install the new Mobile client from the Deployment e-mail. The old Mobile client will remain on their device until they delete it. It can be deleted in the same way as any other application on the device.

6. Upgrade MiVoice Border Gateways

This procedure upgrades all MiVoice Border Gateways except for the one included in MiCollab, that is, external MiVoice Border Gateways.

NOTE: Do not do any provisioning until this upgrade step is complete.

Upgrade MiVoice Border Gateway with Teleworker desk sets

Perform this step for each external MiVoice Border Gateway.

Primary resource: MiVoice Border Gateway Installation and Maintenance Guide

Pre-upgrade tasks:

1. Full back-up
2. Ensure that the MiVoice Border Gateway databases are synchronized between MiCollab-MBG Master and external MiVoice Border Gateway slaves. This is only a check as databases would typically be synchronized.

For large sites deploying separate Teleworker and SIP trunk MiVoice Border Gateway clusters; the clusters may be upgraded independently.

		NOTES
Current Release	10.0 SP3	
Upgrade to	11.0	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)	0.5 each + 0.5 each re-balance time	
Roll-back time (hours)	0.5 each	
Services available during upgrade	User	All Non-resilient SIP devices will be out of service while their primary MiVoice Border Gateway is upgrading. MiNet phones: devices may be load balanced in clusters that are not yet. Service may be affected due to lack of licenses and/or capacity limits.
Services available during upgrade	Admin	All except for user provisioning
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks:

1. Install a third-party SSL Web Server certificate, if one is not already present.
2. Using the option in the web server panel on MSL, export the certificate. Save it for installation on the MiContact Center Business server, For more detailed instructions, see Deploy UCC OVAs.

On the MiVoice Border Gateway, use the following procedure to reset the MiNet devices.This triggers the Teleworker sets to upgrade their firmware. Hot Desk users may need to log in again.

1. Select **Service Configuration > Minet devices**.
2. Click **Bulk Edit**.
3. Click Reset.

7. Upgrade MiVoice Business

Primary resource: *MiVoice Business Migration Guidelines*, *MiVoice Business Installation and Administration Guide for Industry Standard Servers (ISS), and Virtual MiVoice Business*

Pre-upgrade tasks: Full back-up of each MiVoice Business

		NOTES
Current Release	8.0 SP3 PR2	
Upgrade to	9.0 SP3	
Pre-upgrade effort	Back-up (0.5 hours)	
Time to upgrade (hours)	1.0 each; Depends on the number of users	
Roll-back time (hours)	1.0 each	
Services available during upgrade	User	All
Services available during upgrade	Admin	
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Primary resource: *MiVoice Business Installation and Administration Guide for Industry Standard Servers (ISS) and Virtual MiVoice Business*

Pre-upgrade tasks:

- Full back-up of each MiVoice Business

8. Upgrade MiContact Center Business

Primary resources: *MiContact Center Installation and Administration Guide*

Pre-upgrade tasks: Full back-up. See Backup methods for VMware virtual applications for details.

		NOTES
Current Release	9.0 SP1	
Upgrade to	9.2	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)	2.0	
Roll-back time (hours)	up to 2.0	
Services available during upgrade	User	All UC, but no contact center features
Services available during upgrade	Admin	All UC, but no MiContact Center Business admin
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks:

1. Upgrade desk top clients.
2. Install the certificate exported from the MiVoice Border Gateway when it was upgraded.

9. Upgrade MiVoice Border Gateway Secure Recording Connector

Primary resource: *MiVoice Border Gateway Installation and Maintenance Guide*

Upgrade the MiVoice Border Gateways that are configured as Secure Recording Connectors.

You may have to install additional MiVoice Border Gateway Secure Recording Connectors if existing capacity is insufficient.

Pre-upgrade tasks: Full back-up

	NOTES
Current Release	10.0 SP3
Upgrade to	11.0
Pre-upgrade effort	Back-up
Time to upgrade (hours)	0.5 each
Roll-back time (hours)	0.5 each
Services available during upgrade	User All

		NOTES
Services available during upgrade	Admin	All
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: None

10. Upgrade MiVoice Call Recording

Following the upgrade, the system will be fully functional, recording calls and playing back calls on demand. Any clients that were running at the time of the upgrade are disconnected and automatically upgraded on the next usage.

Primary resource: *MiVoice Call Recording Installation and Configuration Guide*

Pre-upgrade tasks: None

		NOTES
Current Release	9.1 SP4	
Upgrade to	9.2	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)		
Roll-back time (hours)		
Services available during upgrade	User	All except for call recording
Services available during upgrade	Admin	All except for MiVoice Call Recording admin
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: None

Upgrade MiCloud Business (MiVoice Business Express)

The upgrade flow for MiCloud Business Virtual (SMB) is summarized in the graphic below.

It is recommended that you provision a test customer that you can use to test service restoration after you complete the system upgrade.

To upgrade from a release prior to MiVoice Business 3.1, see the following table for how to perform the complete upgrade.

IF DEPLOYMENT IS RESILIENT
(CONTAINS MIVOICE BUSINESS REMOTE SURVIVABLE GATEWAYS)

Upgrade from Rls 2.0 to Rls 3.1:	Follow the procedure in the *MiCloud Business Virtual (MLB) Release 3.1 Deployment Guide*.
Upgrade from Rls 3.1 to Rls 3.3	Follow the upgrade instructions in this chapter.

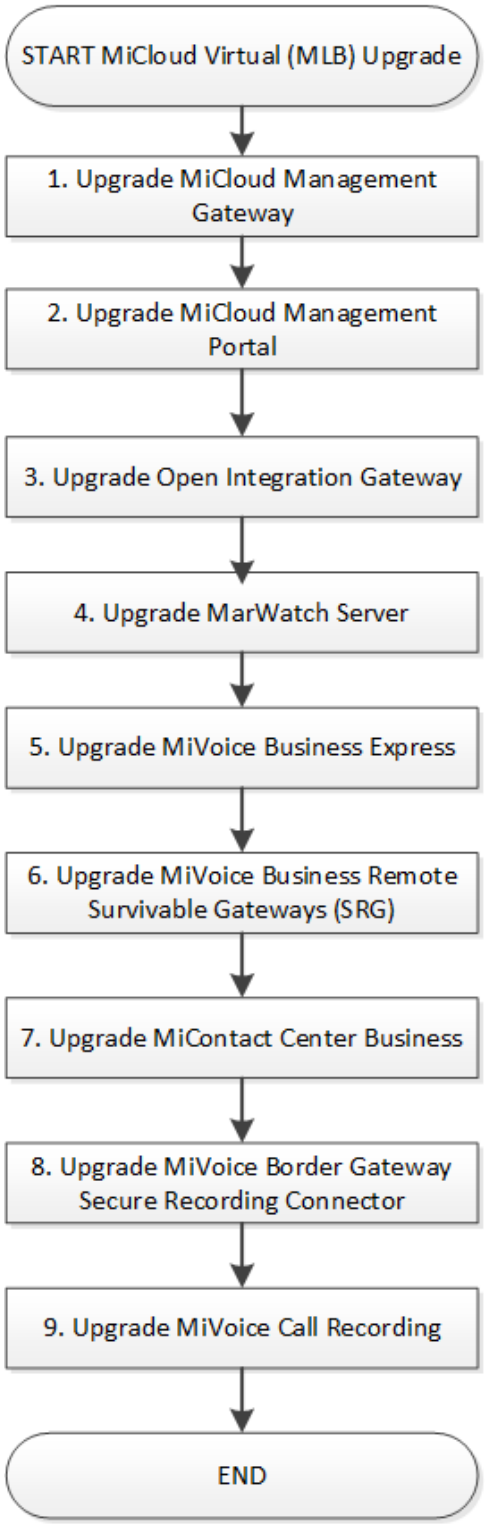
IF DEPLOYMENT IS NOT RESILIENT
(THERE ARE NO MIVOICE BUSINESS REMOTE SURVIVABLE GATEWAYS)

Upgrade from Rls 2.0 to Release 4.1	Use the upgrade order in this guide to upgrade all of the products all the way from their Rls 2.0 versions to their Rls 4.0+ versions.

Prerequisites

- Prepare a full backup of every system and every database in the MiCloud system.
- MiCollab for Mobile is a new, simplified user application for mobile devices. You must add a Web Server Certificate to the MiCollab and MiVoice Border Gateway servers before deploying the MiCollab for Mobile to end-customers. Purchase a third-party SSL Certificate and install it on the MiVoice Border Gateways on the network edge and on the MiCollab on the LAN. See the Add Web Server Certificate topic in MSL help for details.

NOTE: Only one certificate is needed for both MiCollab and the MiVoice Border Gateway (MBG) if the embedded MBG in MiVoice Business Express is used as the Network edge MBG for Mobile Client connections.



1. Upgrade MiCloud Management Gateway

Primary resources:

- MiCloud Management Gateway Online Help (available from inside Mitel Standard Linux)
- Virtual Appliance Deployment Solutions Guide

Pre-upgrade tasks: None

		NOTES
Current Release	5.0 PR1	
Upgrade to	5.0 PR1	
Pre-upgrade effort		
Time to upgrade (hours)	0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	All
Services available during upgrade	Admin	No management services
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: Configure MiCloud Management Gateway interface. See MMG Online Help.

2. Upgrade MiCloud Management Portal

Primary resource: MiCloud Business for Service Providers Help

Pre-upgrade tasks: Full back-up

No administrative changes are allowed during the MiCloud Management Portal upgrade. If this is not acceptable, then you could create a back up on a second machine. Then perform the MiCloud Management Portal upgrade and restore the back-up, and put the upgraded machine back into service.

NOTE: The 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 MiCloud Management Portal Services to start.

		NOTES
Current Release	6.1 SP1	
Upgrade to	6.1 SP3 (6.1.xxx.x)	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)	0.5	
Roll-back time (hours)	0.5	
Services Available during upgrade	User	All
Services Available during upgrade	Admin	None
Services Available after upgrade	User	All
Services Available after upgrade	Admin	All

Post-upgrade tasks:

1. Adjust Customer Admin Bundles, if required. See Assign Customer Admin features in the MiCloud Management Portal Help.
    - If Customer Admin had ACD in their Bundle, then they will have the **ACD Groups** permissions and the **ACD Paths** permissions. You can add the **Advanced ACD Groups** and **Advanced ACD Paths** permissions to bundles used to create trained Customer Admins. See Assign Customer Admin features in the Management Portal Help.
    - The **RAD Programming** feature is not enabled for existing Customer Admin Bundles at upgrade. You must reset the RAD source for existing customers.
2. At upgrade, Management Portal overwrites the RAD Ports, RAD indices, MOH indices.
3. After upgrade, for existing Platform Groups, the RAD group is set to None, and the RAD drop-down list will be empty.

3. Upgrade Open Integration Gateway

Upgrade the OIG Blade from inside Mitel Standard Linux (MSL).

NOTE: Do not attempt to restore an OIG Release 3.0 database into OIG Release 4.0. Upgrading from the MSL Blades panel allows OIG 4.0 to convert the existing MSL database so that it is usable in OIG 4.0.

Primary resource:

- *Mitel Open Integration Gateway Installation and Maintenance Guide*

Upgrade tasks:

1. Upgrade the OIG software using the **Upgrade** link in the **Blades** panel.
2. Reboot.

		NOTES
Current Release	4.0 SP1	
Upgrade to	4.1 SP3	
Pre-upgrade effort		
Time to upgrade (hours)	0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	All except for MiVoice Integrations MiVoice Integration for Salesforce: the hosted or premise-based application must be updated with a new MiVoice Integration for Salesforce package.
Services available during upgrade	Admin	All All functions of MiCloud continue operating during the OIG upgrade, except for OIG and MiVoice Integrations functions.
Services available after upgrade	User	All except for MiVoice Integrations MiVoice Integration for Salesforce: the hosted or premise-based application must be updated with a new MiVoice Integration for Salesforce package.
Services available after upgrade	Admin	All

NOTE: The OIG Release 4.0 server upgrade does not support Release 3.0 clients.

Post-upgrade tasks:

- Upgrade Salesforce server and Google end-user extensions, if applicable. **NOTE**: The upgrade from OIG 4.0 to 4.1 does not require upgrading the MiVoice Integrations.
  - 3a. Upgrade MiVoice Integration for Salesforce
  - 3b. Upgrade MiVoice Integration for Google
- If using MiContact Center Business: After the MiContact Center Business install or upgrade, enable the OIG integration to MiContact Center Business. (MiContact Center Business must be at Release 8.0 or higher.) See the *MiContact Center Installation and Administration Guide*.

3a.Upgrade MiVoice Integration for Salesforce

MiVoice Integration for Salesforce (hosted or premise-based Salesforce application) must be updated with the new Salesforce blade.

NOTE: The Salesforce package in the App Store does not require update.

Primary resources:

- MiVoice Integration for Salesforce Administration Guide

Pre-upgrade tasks:

- OIG is upgraded as described above.

Administrator steps for upgrade (this is done in Salesforce by a Salesforce Administrator):

NOTE: For details, see the MiVoice Integration for *Salesforce Administration Guide*.

1. In MSL, install the new MiVoice Integration for Salesforce 2.1.6 blade.
2. Make copies of all Salesforce Call Centers connected to the MiVoice Integration package you are upgrading.
3. Associate the new MiVoice Integration for Salesforce with the new copies of the Call Centers.
4. Associate each user with the new Salesforce Call Centers.

User steps for upgrade:

- None

		NOTES
Current Release	2.0	
Upgrade to	2.1.29	
Pre-upgrade effort	N/A	
Time to upgrade (hours)	Admin: 1.0 User: 0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	None
Services available during upgrade	Admin	All
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks:

- None

3b. Upgrade MiVoice Integration for Google

MiVoice Integration for Google extensions must be uninstalled and reinstalled by each end-user.

Primary resources:

- MiVoice Integration for Google Administration Guide
- MiVoice Integration for Google Quick Reference Guide

Pre-upgrade tasks:

- OIG is upgraded as described above.
- Export or create the Google integration template and obtain a list mapping of Google accounts to DN in CSV format for import to the OIG server.

Administrator steps for upgrade:

1. Upgrade to MiVoice Integration for Google 1.1,20, if required. See the MiVoice Integration for Google Administration Guide.

2. Edit the user CSV for the new Import spreadsheet format. See the OIG 4.0 Installation and Maintenance Guide, Upgrade section, for details.
3. Import the new CSV Users file into MiVoice Integration for Google. The user list must contain a DN for every user name for the user to use the application.

User steps for upgrade:

- None

		NOTES
Current Release	1.1	
Upgrade to	1.1.20	
Pre-upgrade effort	N/A	
Time to upgrade time (hours)	Admin: 0.5 User: 0.5	
Roll-back time (hours)	0.5	
Services available during upgrade	User	None
Services available during upgrade	Admin	All
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks:

- None

4. Upgrade Mitel Performance Analytics

Primary resource: *Mitel Performance Analytics Upgrade Guide*

Pre-upgrade tasks: None

Reporting is affected by the in-progress upgrade, but MiCloud Management Portal and similar administrative services remain available.

NOTE: Probes are updated automatically after the server is upgraded.

		NOTES
Current Release		2.3
Upgrade to		3.0
Pre-upgrade tasks		Back-up
Time to upgrade (hours)		1.0
Roll-back time (hours)		1.0
Services available during upgrade	User	All
Services available during upgrade	Admin	All
Services available -after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: None

5. Upgrade MiVoice Business controllers (Remote Survivable Gateways)

NOTE: This step is necessary only if your system is configured for resiliency and contains one or more MiVoice Business Remote Survivable Gateways.

Primary resource:

- MiVoice Business Migration Guidelines
- Mitel 3300 IP Communications Platform (ICP) Technician's Handbook
- MiVoice Business Installation and MiVoice Business System Administration Tool Help

Pre-upgrade tasks:

- Full back-up of each MiVoice Business

NOTE: Upgrade secondary controllers before upgrading primary controllers.

		NOTES
Current Release	8.0 SP3 PR2	
Upgrade to	9.0 SP2	
Pre-upgrade effort	Back-up: 0.5 hrs	
Time to upgrade (hours)	1.0 per MiVoice business controller Depends on the number of users	
Roll-back time (hours)		
Services available during upgrade	User	All
Services available during upgrade	Admin	
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks:

1. Install a third-party certificate on MiVoice Business. Export it for install to all of the applications. This will involve going back to your MiCollab and MiVoice Border Gateway installations.
2. LAN based desk sets will be automatically upgraded. Hot Desk users may need to log in again.

6. Upgrade MiVoice Business Express

There are two options for upgrading MiVoice Business Express, depending on how it was created.

- If it was created using Platform Manager, you can upgrade through Platform Manager by creating an Upgrade Blueprint and migrating to the new blueprint. See the Platform Manager help for details.
- If the instances were not created using Platform Manager, follow the instructions in this section.

Primary resource: *MiVoice Business Express Deployment Guide*

NOTE: UC services including soft phones, Teleworker phones, and SIP phones will be out-of-service during the MiCollab upgrade.

NOTE: MiVoice Business Express install includes automated SDS sync between embedded the MiVoice Business and MiCollab.

Pre-upgrade tasks: A virtual machine (VM) back-up must be available. LAN based desk sets will upgrade automatically. MiCollab desktop clients will prompt for upgrade when user logs in.

		NOTES
Current Release	8.0 SP2 FP2	
Upgrade to	8.1	
Pre-upgrade effort	Back up VM	
Time to upgrade (hours)	1.0	
Roll-back time (hours)	0.5	
Services available during upgrade	User	Voice only: Voice only through Remote Server Gateways; no Unified Communication features and no soft phones are available during upgrade. Teleworker phones and SIP phones are out of service.

		NOTES
Services available during upgrade	Admin	None
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks:

1. Request third-party Web Server certificate if one has not previously been used. Apply the certificate to MiCollab.
2. Mobile clients will not receive an upgrade prompt. You must change the user bundle for the new Mobile client, and explicitly re-send the Deployment e-mail to the mobile users. Users will install the new Mobile client from the Deployment e-mail. The old Mobile client will remain on their device until they delete it. It can be deleted in the same way as any other application on the device.
3. On the MiVoice Border Gateway, use the following procedure to reset the MiNet devices. This triggers the Teleworker sets to upgrade their firmware. Hot Desk users may need to log in again.
    - Select Service **Configuration > Minet devices**.
    - Click **Bulk Edit**.
    - Click **Reset**.

7. Upgrade MiContact Center Business (SMB)

Primary resources:

- *MiContact Center Installation and Administration Guide*
- *MiCloud Contact Center Administration Guide*

There are two types of upgrades, depending on how and whether MiContact Center Business is or will be used in a multi-tenant configuration.

- If you are upgrading MiContact Center Business single user to MiContact Center Multi Tenant, follow the instructions in the guides below.
- If you are currently managing multiple tenants using Access Control Lists (ACL):
    - For customers using MiContact Center Business Call Costing module, MiContact Center Business will continue to be used in single Tenant mode using ACL for tenant segregation.
    - After upgrade, contact Mitel Professional Services to convert to the new MiContact Center Multi Tenant deployment.

Pre-upgrade tasks: Full back-up

There are three back-up methods. See Backup methods for VMware virtual applications in MiCloud Business for Multi-Instance document for details.

		NOTES
Current Release	9.0 SP1	
Upgrade to	9.2	
Pre-upgrade effort	back-up	
Time to upgrade (hours)	2.0	
Roll-back time (hours)	from minutes up to 2 hrs	
Services available during upgrade	User	All UC, but no contact center features
Services available during upgrade	Admin	All UC, except for MiContact Center Business admin
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: Upgrade desktop clients.

8. Upgrade MiVoice Border Gateway Secure Recording Connector

Primary resource: *MiVoice Border Gateway Installation and Maintenance Guide*

Upgrade the MiVoice Border Gateways that are configured as Secure Recording Connectors.

You may have to install additional MiVoice Border Gateway Secure Recording Connectors if existing capacity is insufficient.

Pre-upgrade tasks: Full back-up

		NOTES
Current Release	10.0 SP3	
Upgrade to	11.0	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)	0.5 each	
Roll-back time (hours)	0.5 each	
Services available during upgrade	User	All
Services available during upgrade	Admin	All
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: None

9. Upgrade MiVoice Call Recording

Following the upgrade, the system will be fully functional, recording calls and playing back calls on demand. Any clients that were running at the time of the upgrade are disconnected and automatically upgraded on the next usage.

Primary resource: *MiVoice Call Recording Installation and Configuration Guide*

Pre-upgrade tasks: None

		NOTES
Current Release	9.1 SP4	
Upgrade to	9.2	
Pre-upgrade effort	Back-up	
Time to upgrade (hours)		
Roll-back time (hours)		
Services available during upgrade	User	All except for call recording
Services available during upgrade	Admin	All except for Call Recording admin
Services available after upgrade	User	All
Services available after upgrade	Admin	All

Post-upgrade tasks: None