

MICLOUD BUSINESS MULTI-INSTANCE FOR SERVICE PROVIDERS

DEPLOYMENT GUIDE
RELEASE 3.3

APRIL 2017

NOTICE

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

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

Trademarks

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

MiCloud Business Multi-Instance for Service Providers Deployment Guide

Release 3.3

April 2017

®,™ Trademark of Mitel Networks Corporation
© Copyright 2017, Mitel Networks Corporation
All rights reserved

CHAPTER 1: MICLOUD BUSINESS MULTI-INSTANCE DEPLOYMENT PROCESS

MiCloud Business Multi-Instance deployment process	3
MiCloud Multi-Instance deployment process and roles	5
Prerequisites	6
Multi-Instance deployment process	8

CHAPTER 2: NETWORK SERVICES CONFIGURATION

Network services configuration	11
Prerequisites	11
Network services configuration task flow	11
Create IP addressing assignment plan	12
Download current software from Mitel OnLine	13
Create a server for FTP downloads	14
Optional: Create portable media	15
Set up a DHCP server	16
Set up DNS servers	17
Set up an SMTP forwarder	18
Optional: Install SNMP server	19

CHAPTER 3: MICLOUD MULTI-INSTANCE INFRASTRUCTURE DEPLOYMENT

MiCloud infrastructure deployment for Multi-instance topology	23
Prerequisites	23
MiCloud infrastructure deployment task flow	23
Install and configure Mitel Standard Linux (MSL)	24
Configure AMC licensing	26
Synchronize to AMC	29
Deploy MiVoice Business Multi Instance	30
Deploy temporary MiVoice Business instances	31
Program internal phones for testing	33
Deploy VMware® vCenter™ and vSphere®	34

CHAPTER 4: SHARED GATEWAYS DEPLOYMENT

SIP trunk configuration	39
Prerequisites	39
SIP trunk configuration task flow	39
Deploy SIP trunk MiVoice Border Gateway cluster	40

Configure MiVoice Border Gateway for SIP trunk connection	41
Configure MiVoice Border Gateway DID/DDI routing tables	43
Configure MiVoice Business SIP routes and resiliency	44
Deploy MiVoice Border Gateway clusters for end-user MiNet devices	47
Deploy SIP and UC MiVoice Border Gateway cluster	49

CHAPTER 5: CUSTOMER ACCESS CONFIGURATION

Customer access configuration	53
Prerequisites	53
Customer Access configuration task flow	53
Configure end-user devices in the MiNet MiVoice Border Gateways	54
Configure MiNet end-user devices to MiVoice Business	55
Configure and test MiNet phones as Teleworker devices	56
Use configured phones to make a test call to the SIP trunks	58

CHAPTER 6: ORIA DEPLOYMENT

Oria deployment	61
Prerequisites	61
Oria deployment task flow	61
Prepare resilient MiVoice Business instances for management by Oria	62
Install and configure Oria	64
Configure external access to Oria	66
Register a test Platform Group	67
Create Basic IP Telephony (IPT) Oria bundles	68
Create a test customer	69
Add test users with Oria	70

CHAPTER 7: (OPTIONAL) MITEL PERFORMANCE ANALYTICS DEPLOYMENT

Optional: Mitel Performance Analytics deployment	73
Prerequisites	73
Mitel Performance Analytics deployment task flow	73
Install Mitel Performance Analytics	74
Configure Mitel Performance Analytics	75

CHAPTER 8: UC APPLICATIONS DEPLOYMENT

Unified Communications applications deployment	79
--	----

Prerequisites	79
Unified Communications applications deployment task flow	79
Deploy MiCollab	80
Configure proxy services for MiCollab Client	82
Configure MiVoice Border Gateway for WebRTC users	84
Configure MiCollab for mobile users	85
Create UC Bundles in Oria	87
Create a UC-capable test Platform Group in Oria	89
Create a UC-capable test customer and test end-users in Oria	92
Synchronize MiCollab Client and MiVoice Business	93
Register UC devices and test MiCollab Client	94
Deploy Open Integration Gateway Virtual (OIG Virtual)	95
Configure Open Integration Gateway Virtual proxy services	96
Test Open Integration Gateway configuration	97
Install MiContact Center Business and MiVoice Call Recording	98
Deploy business analytics	101
Delete the test set-up	102

CHAPTER 9: (OPTIONAL) CRM INTEGRATIONS DEPLOYMENT

Deploy Customer Relationship Management (CRM) integrations	107
Prerequisites	107
CRM deployment task flow	107
Deploy MiVoice Integration for Google, MiVoice Integration for Salesforce	108
Deploy MiCloud CRM Integrations	110

CHAPTER 10: SERVICE PROVIDER OFFER DEFINITION

Service provider offer definition	115
Prerequisites	115
Service provider offer definition task flow	115
Program Oria with service bundle definitions	116
Purchase licenses for the service provider	117

CHAPTER 11: CUSTOMER PREPARATION

Customer account preparation	121
Prerequisites	121
Customer account preparation task flow	121

Enter phone MAC addresses into the Re-Direction and Configuration Server (RCS) 122
Ship on-premise equipment to the Customer 123

CHAPTER 12: CUSTOMER DEPLOYMENT

Customer deployment. 127
Prerequisites 127
Customer deployment task flow 127
Optional: Use Oria Platform Manager to create Blueprints 128
Deploy resilient Customer MiVoice Business instances 130
Synchronize MiCollab/MiCollab Client/MiVoice Border Gateway with AMC 131
Update internal DNS server with tenant MiCollab Client and MiVoice Business FQDNs 132
Create the customer Platform Group 133
Create a Customer 134
Configure custom branding 135
Deploy Open Integration Gateway 136
Configure OIG proxy services 137
Update SIP provider with emergency location information 138

CHAPTER 13: END-USER CONFIGURATION

End-user configuration 141
Prerequisites 141
End-user configuration task flow 141
Create a Customer's user administration account 142
Bulk import end-users 143
Administer end-users 145
Configure groups 146
Configure call flows and paths, and auto attendants 147
Configure ACD functions 148
Optional: Provision users for MiVoice Integrations 149
Tune the deployment manually 151
Optional: Deploy ACD phones and clients 152
Optional: Deploy Vidyo® functionality 154

CHAPTER 14: MICONNECT CENTER BUSINESS DEPLOYMENT

Install and provision MiContact Center Business 157
Prerequisites 157

MiContact Center Business configuration task flow	157
Install MiContact Center Business and configure with MiVoice Business	158
Administer agents in Oria	159
Adjust configuration on MiVoice Business	160
Synchronize users with MiContact Center Business	161
Tune the deployment in MiVoice Business, MiCollab, and MiVoice Border Gateway (SaaS or Reseller)	163
Deploy phones and clients (Reseller)	164

CHAPTER 15: CUSTOMER DELETION

Customer deletion	167
Prerequisites	167
Customer deletion task flow	167
Delete a Customer profile	168
Delete the customer Platform Group	169
Delete the customer Open Integration Gateway instances	170
Clear the Customer configuration	171
Optional: Engage Mitel Professional Services for licensing clean up	172

CHAPTER 16: MICLOUD BUSINESS UPGRADE

Upgrading MiCloud Business Multi-Instance	175
Prerequisites	175
Upgrade MiCloud 3.0/3.1 to MiCloud 3.3	177
1. Upgrade Oria to RIs 5.3 SP1	178
2. Upgrade Open Integration Gateway (OIG) to RIs 4.0	179
3. Upgrade MarWatch server to Mitel Performance Analytics (MPA) 5.2	183
4. Upgrade MiCollab Multi-tenant to RIs 7.3 PR1	183
5. Upgrade the external MiVoice Border Gateways to RIs 9.4 PR3	184
6. Upgrade the MiVoice Business instances to RIs 8.0 PR3	185
7. Upgrade MiContact Center Business to RIs 8.1 SP1	186
8. Upgrade MiVoice Border Gateway Secure Recording Connector to RIs 9.4 PR3	187
9. Upgrade MiVoice Call Recording to 9.1	188

APPENDIX A: GLOSSARY OF ACRONYMS

Glossary of acronyms	191
----------------------------	-----

APPENDIX B: MITEL PERFORMANCE ANALYTICS PROCEDURES

Mitel Performance Analytics deployment 197

 Download Mitel Performance Analytics OVA197

 Deploy Mitel Performance Analytics OVA197

 Install Windows root certificate file for Mitel Performance Analytics Probe198

 Install Linux root certificate file for Mitel Performance Analytics Probe198

Chapter 1

MICLOUD BUSINESS MULTI-INSTANCE DEPLOYMENT PROCESS

MiCloud Business Multi-Instance deployment process

The MiCloud Business Multi-Instance deployment described in this guide is the process of installing and configuring a Unified Communications solution matching the reference architecture described in the *MiCloud Solutions Blueprint*. Completing the deployment process creates a topology that is verified as operational and ready for adding more Customers as required.

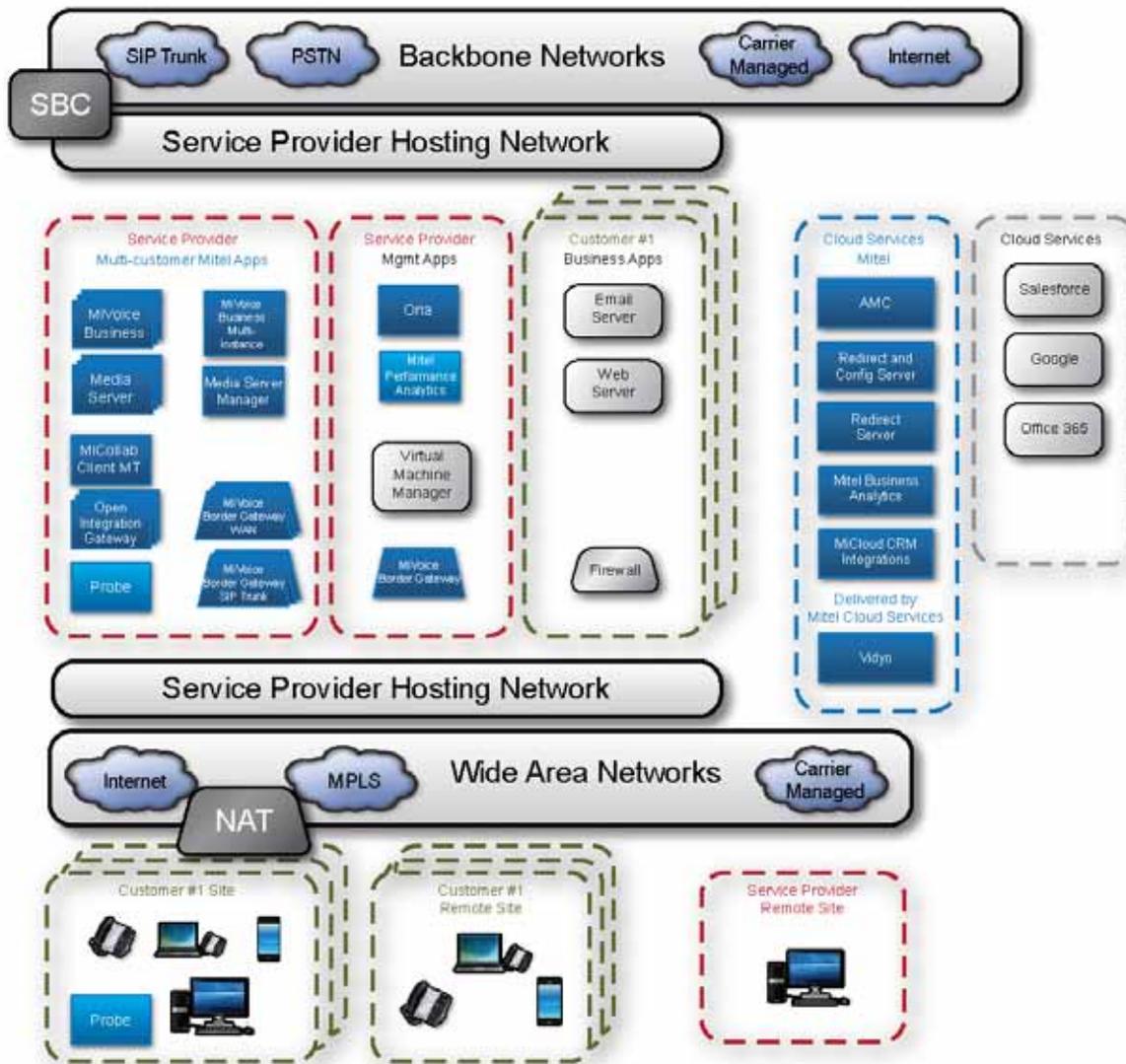
Table 1 shows the Mitel product lineup that comprises MiCloud Business Multi-Instance 3.3. See the Mitel OnLine download page to download the correct releases of these products.

Table 1: MiCloud Business 3.3 product lineup

PRODUCT NAME	RELEASE
MiVoice Business	8.0 PR3
MiVoice Business Multi Instance	2.0 SP1
MiVoice Business Express	7.3 PR1
MiCollab	7.3 PR1
MiCollab Client	7.3 PR1
MiVoice Border Gateway / Secure Recording Connector	9.4 PR3
MiContact Center Business	8.1 SP2
MiVoice Business Reporter	8.1 SP2
MiVoice Call Recording	9.1 SP1
Mitel Open Integration Gateway	4.0
MiVoice Integration for Salesforce	2.1
MiVoice Integration for Google	1.1
MiCloud Management Gateway	5.0
Oria	5.3 SP1
Redirection and Configuration Service (RCS)	1.1
Mitel Performance Analytics	2.1
MiCloud Business Analytics	3.3
MiCloud CRM Integrations	3.3

See the Release Notes for details and updates.

Figure 1: MiCloud Business Multi-Instance architecture



In this guide, the following terminology is used:

Service Provider	The Service Provider is the primary audience for this guide. The Service Provider sets up and configures a network for its Customers.
Customer, end-customer	Each Customer of the Service Provider has its own sub-network that is isolated from the Service Provider and from other Customers of the Service Provider.
System Administrator	The System Administrator is responsible for configuring system wide settings. This function is often performed by the “Software as a Service (SaaS) provider or by the Reseller. (For a definition of the SaaS role, see Table 2, “Deployment Roles,” on page 5.

Customer Administrator	The Administrator, either the Reseller or an employee of the Customer, administers the Mitel UC System for the Customer and the End-Users.
End-User	End-users are the actual phone and UC end-users, generally employees of the Customer.

Documentation and training sources

The primary documents for this MiCloud solution are:

- *MiCloud Solutions Blueprint* - contains detailed descriptions of all of the supported MiCloud topologies
- *MiCloud Engineering Guidelines* - contains engineering details and limits for all of the supported MiCloud topologies
- *Virtual Appliance Deployment Solutions Guide* - contains deployment procedures and engineering limits for all Mitel virtual appliances. Also see the VMware documentation: <https://www.vmware.com/support/pubs/>
- Mitel Performance Analytics (MPA) documentation (MPA server, Probe) - see Mitel OnLine.

Other documents needed for installation, configuration, and provisioning are listed throughout this guide, as they are needed for the procedure being performed.

For Mitel training offerings, see the training map, “Service Providers using the MiVoice Business Platform” on the Mitel Training site: http://training.mitel.com/cw/Learning_Maps/MCLD_LM.pdf.

For VMware training, see <http://www.vmwarelearning.com/>.

MiCloud Multi-Instance deployment process and roles

The MiCloud Multi-Instance deployment process summarizes the actions for deploying the Multi-Instance reference architecture. Each flowchart item links to a task flow that breaks the deployment process down into a set of tasks. Complete each task and return to the “MiCloud Business Multi-Instance deployment flowchart” on page 8 to determine the next task to be performed.

The installation and configuration tasks are meant to be performed by various players; these players are described in Table 2.

Table 2: Deployment Roles

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.

MiCloud Business Multi-Instance Deployment

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; and
- 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

- The Mitel OnLine web site 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 OnLine.
- 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.

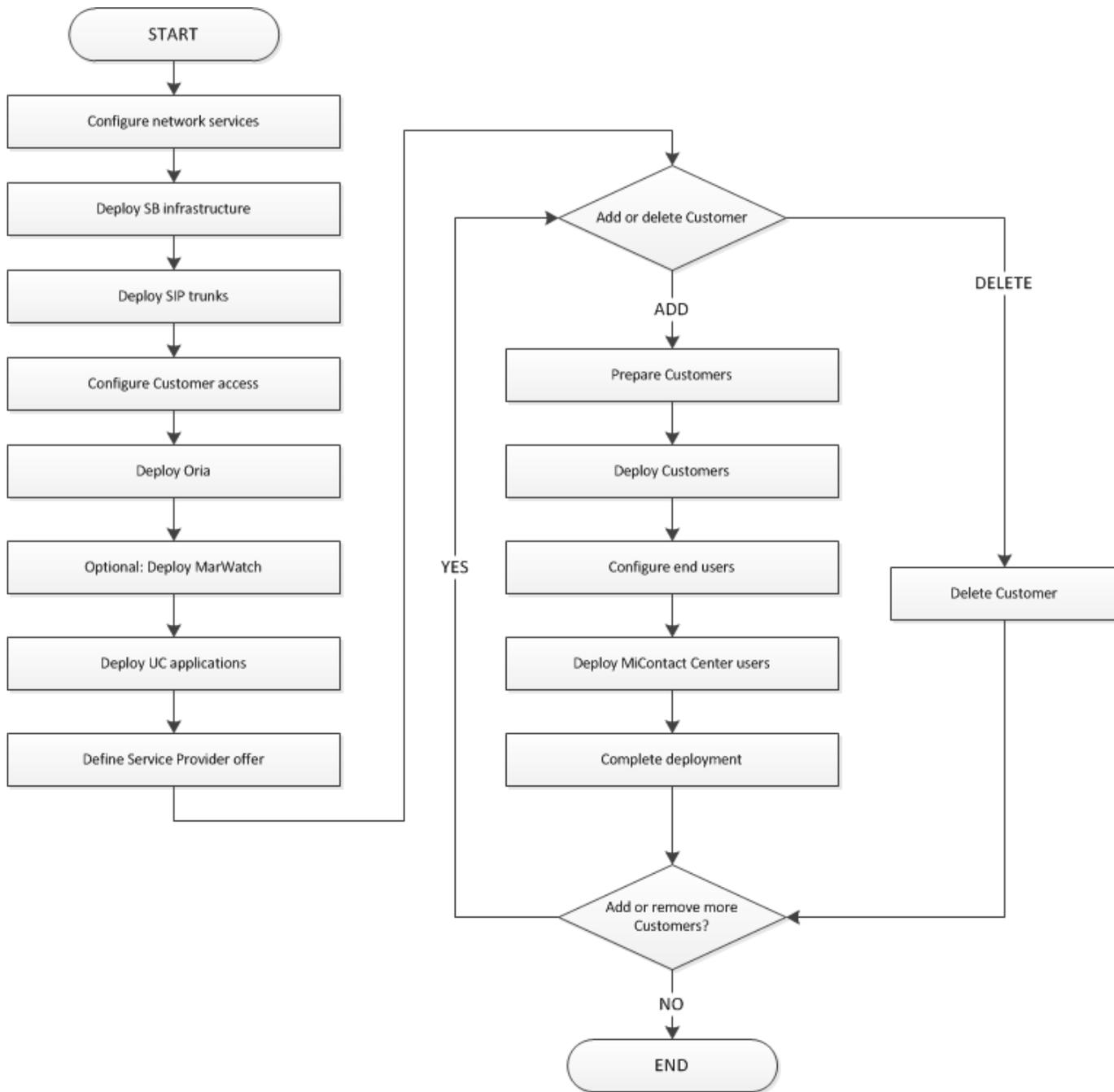
MiCloud Business Multi-Instance deployment process

- 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.

Multi-Instance deployment process

This flowchart summarizes the process for deploying the MiCloud SB 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.

Figure 2: MiCloud Business Multi-Instance deployment flowchart



Chapter 2

NETWORK SERVICES

CONFIGURATION

Network services configuration

Configure network services to build the network functions needed to support the solution deployment. Apply network addressing of the topology components, establish software delivery mechanisms, configure domain name services, enable SNMP, and set-up SMTP forwarding for e-mail services that are used when configuring, managing, and employing the topology.

Prerequisites

- The service provider must have an operational gateway to the Internet to connect to the AMC for licensing sync and to get software downloads, and to make connections for test devices.

Network services configuration task flow

These are the steps that must be performed to create the network services needed for deploying the solution.

- “Create IP addressing assignment plan” on page 12
- “Download current software from Mitel OnLine” on page 13
- “Create a server for FTP downloads” on page 14
- “Optional: Create portable media” on page 15
- “Set up a DHCP server” on page 16
- “Set up DNS servers” on page 17
- “Set up an SMTP forwarder” on page 18
- “Optional: Install SNMP server” on page 19

Create IP addressing assignment plan

Plan and assign WAN, LAN, and management access IP addresses for the topology deployment.

- WAN addressing requires public IPv4 addresses for the SIP trunk gateways, and for Tele-worker gateways for phones and UC services.
- LAN addressing requires IP addresses for creating the internal service provider routing rules and service partitions for media, call control, and management.
- Management access IP addressing requires assigning IPv4 addresses for customer management portals and service provider remote maintenance portals.

The IP address plan should include a strategy for future IP assignments as the solution grows and more Customers are added.

Prerequisites

- A network plan that shows all network elements that require IP addresses or ranges of IP addresses.

Resources

RESOURCE

CONTENT DETAILS

MiCloud Business Solution Blueprint

The Multi-Instance topology section includes the topic "Addressing considerations" for each topology.
The "Networking and Network Considerations" chapter provides details for planning and creating the network topology.

Download current software from Mitel OnLine

On the Mitel OnLine Software Downloads page, navigate to MiCloud Business 3.3. This page contains all of the product releases that comprise MiCloud Business 3.3.

Collect and store the Mitel software used in the topology. The downloaded software can be distributed using an internal FTP server or portable media.



Note: Exercise caution before updating software loads across the solution. Changing the software version of an individual product component can create unexpected problems across the entire topology. Only use software versions that are compatible with the entire solution as specified by Mitel. See “MiCloud Business 3.3 product lineup” on page 3, and the MiCloud Business 3.3 download page.

Prerequisites

- A Mitel OnLine account with credentials for downloading software.
- Licenses have already been purchased in AMC.

Resources

RESOURCE	CONTENT DETAILS
Mitel OnLine	Mitel OnLine users with MOL login credentials can download software from the Software Downloads page. Mitel.com > Technical Support > Software Downloads
Application Management Center (AMC)	Software can be downloaded directly from the AMC after the platforms are registered.
<i>Managed Service Provider Program</i>	
<i>MiCloud Business for Service Providers Licensing Structures</i>	
<i>Managed Service Provider Program Service Provider AMC Licensing Best Practices</i>	

Create a server for FTP downloads

Create a Server for FTP downloads. This will serve as an easy-to-access common place in the network for efficiently distributing software for installation of the network components. A central location facilitates controlling the software versions used in the network and helps ensure that installations are efficient and repeatable.

Prerequisites

- A list of people who have access to the FTP server and who will administer the software installed on it for download.

Resources

RESOURCE

CONTENT DETAILS

Server installation instructions

Follow the instructions for the operating system or the application to be used to provide the FTP services.

Optional: Create portable media

Create portable media, such as DVDs. This removes the need to have network connectivity for downloading and installing software to the various components in the topology.

Portable media increases the risk of using incorrect software versions, but avoids delays due to network connectivity issues. Having the software on portable media helps in case of disaster recovery or Internet lock-down.

Portable media is also an option for delivering the initial software to the FTP server.

Prerequisites

- Assign a portable media librarian to control the location and versioning of the portable media to prevent stale versions from being used for new installations.

Resources

RESOURCE

CONTENT DETAILS

Media burning software

Media burning software is provided by third-party suppliers.
Follow the instructions for the application to be used to burn the portable media.

Set up a DHCP server

Set up a DHCP server to provide addresses for components that require dynamic address assignment, and for general purpose use by the Service provider. DHCP assignments are typically used for test and maintenance PCs and phones.

Most of the servers in the topology use statically assigned IP addresses.



Note: DHCP may also be provided in some Mitel products. Decide which DHCP will be used and disable any that will not be deployed.

Prerequisites

- The range of addresses set up for assignment by the DHCP server must comply with the IP address plan created in “Create IP addressing assignment plan” on page 12.



Note: Each Customer also needs their own DHCP server, installed at their own business site.

Typically, a small site would employ the embedded DHCP Server running in the Firewall or NAT Router on the site.

Resources

RESOURCE

CONTENT DETAILS

MSL Online Help

MSL includes an embedded DHCP Server. See the MSL Online Help in the DHCP Service panel.

MSL specifically supports Mitel phone options, and can be deployed at any time.

Set up DNS servers

Set up DNS servers for internal and external domain name look-ups. Pay particular attention in planning the setup of DNS server records. This is a critical component to the proper operation of all applications and services in the MiCloud offering.

MiCollab Client connections and MiVoice Border Gateway connections use internal DNS. External DNS is available when local DNS does not have the required information.

The internal DNS server is used by applications within the service provider network to locate and connect with each other.

External DNS is required by the end-users or customers to locate the IP address of the external gateway, such as MBG, application portals, or management portals. Note that the term “External DNS” server may also refer to the Public Internet DNS Servers, and those of your customer’s Internet Service Provider.

The topology components must be registered with external DNS servers to allow end-users to get to the correct Unified Communication and voice portals.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
MiVoice Business System Administration Tool Online Help	<p>Help Topics:</p> <ul style="list-style-type: none"> • “Configuring the DNS Server” - instructions for changing the DNS server configuration on the DNS Server Configuration window. • “DNS Server Form” - use for setting up primary and secondary DNS servers on MiVoice Business controllers.
<i>MiCollab Engineering Guidelines</i>	Use this guide, if needed, to configure a web proxy for the DNS server.
<i>MiCollab Client Engineering Guidelines</i>	<p>Use this guide, if needed, to configure a web proxy for the DNS server.</p> <ul style="list-style-type: none"> • “DNS Configuration with web proxy”
<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	<p>Use this guide to program the IP address of the internal DNS server into the Corporate DNS Settings on the Domains page of the MiVoice Border Gateway server.</p> <p>This also applies to MiVoice Business Multi Instance, MiCollab, and any other of the Mitel platforms that run on MSL.</p>
<i>Mitel Standard Linux Installation and Administration Guide</i>	<p>Although it would be unusual to use the MSL server as the DNS server, this guide contains the instructions. See the topic “Configure DNS”.</p> <p>This guide contains instructions for configuring the server to forward DNS to another DNS server. See the topic “DNS Forwarder”.</p>

Set up an SMTP forwarder

Set up an SMTP forwarder to forward internally generated e-mails to a public SMTP forwarder. The SMTP forwarder sends alarm messages to the appropriate maintenance personnel. SMTP forwarding can also be used to alert end-users during UC account initialization and for sending bulk update messages.

All MSL boxes provide e-mail settings to send system alarm e-mails to the target outbound SMTP server. MiVoice Business also provides **Alarms Email Notification** services.

Prerequisites

- A plan is in place for generation and protocol for Service Provider and customer alerts.

Resources

RESOURCE	CONTENT DETAILS
SMTP forwarder configuration instructions	An SMTP forwarder is a third-party product. Follow instructions for the SMTP forwarding application being used.
SMTP settings	The SMTP forwarder may need different settings for each individual customer.
<i>Mitel Standard Linux Installation and Administration Guide</i>	Refer to the section called "Email Settings".
MiVoice Business System Administration Tool Help	Refer to the following help topics: <ul style="list-style-type: none">• "Alarms Email Notifications"• "Obtaining Email Notifications of Alarms and Scheduled Software Upgrade Events"

Optional: Install SNMP server



Note: This step is not required if Mitel Performance Analytics is being used. Any SNMP server can be used.

Install and prepare an SNMP management server and set up the network manager.

For information about deploying Mitel Performance Analytics, see:

- “Optional: Mitel Performance Analytics deployment” on page 73
- “Mitel Performance Analytics procedures” on page 195

The SNMP settings and device IP addresses need to be configured into the Mitel Performance Analytics Probe, if used, in order to be able to read SNMP MIB information or to receive SNMP traps, MiVoice Business also provides SNMP configuration settings.

All MSL boxes provide SNMP settings to send system traps to the target SNMP Management server (such as Mitel Performance Analytics). Applications like MiVoice Business and MiCollab also provide SNMP information.

Remember to also include the network infrastructure equipment in the provisioning, router alarms, for example.



Note: SNMP Agent and SNMP Service must be enabled in MiVoice Business and MiVoice Border Gateway, respectively, prior deploying Mitel Performance Analytics. Program an SNMP community string that is common across all platforms to allow these to be monitored. Choose a community string that is different than the default, and disable the default setting.

Prerequisites

- A plan is in place for to install SNMP, and the configuration options required.
- The Management Information Bases (MIB) of the Network devices have been compiled into the Network Management System (NMS) so that it properly interprets SNMP information from the network components. The MIB has been designed to generate alerts on actions and events important for the network.

Resources

RESOURCE	CONTENT DETAILS
Mitel Performance Analytics documentation	Mitel OnLine
SNMP configuration instruction	Configure SNMP using the instructions for the SNMP application chosen.
<i>Mitel Standard Linux Installation and Administration Guide</i>	Refer to the section called “Simple Network Management Protocol (SNMP)”.

Chapter 3

MICLOUD MULTI-INSTANCE

INFRASTRUCTURE DEPLOYMENT

MiCloud infrastructure deployment for Multi-instance topology

Install and configure the core voice components, following the design topology considerations in the appropriate MiCloud Blueprint

Install VMware vSphere and vCenter, if the network will include virtualized components.

After the core voice components are installed and configured, it is recommended to test the deployment by adding internal phones and making calls between them. Instructions for setting up this testing are included in this chapter.

Prerequisites

- The software and hardware, both Mitel and third-party, has been purchased and licensed. Use UCC and IPT licensing for test purposes.
- The servers have been installed in a suitable physical environment.
- Installation and configuration documentation is available and on-hand.
- IP address ranges have been planned and documented.
- User names and passwords have been chosen and documented for each installation procedure that requires them.
- A MiVoice Business call controller is available; including a Golden database plus customizations. A Golden database will not be ready the first time through, and will be created from the first configurations.

MiCloud infrastructure deployment task flow

This following list shows the sequence of tasks that must be performed to deploy the core architecture components needed for deploying the topology.

- “Install and configure Mitel Standard Linux (MSL)” on page 24
- “Configure AMC licensing” on page 26
- “Synchronize to AMC” on page 29
- “Deploy MiVoice Business Multi Instance” on page 30
- “Deploy temporary MiVoice Business instances” on page 31
- “Program internal phones for testing” on page 33
- “Deploy VMware® vCenter™ and vSphere®” on page 34

Install and configure Mitel Standard Linux (MSL)

Install and configure the MSL operating system on the servers that will host the Mitel components.

MSL is needed for some of the Mitel components, but not all. Virtualized components, including MiCollab Multi-tenant, do not require MSL.

Table 3: MSL required for...

MITEL COMPONENT	DELIVERY TYPE	MSL REQUIRED?
MiVoice Business	Industry Standard Server (ISS)	Yes
	OVA	No
MiCollab Multi Tenant	always virtualized	No
MiVoice Border Gateway	ISS	Yes
Oria	ISS	Yes
	OVA	No
Oria Platform Manager	CD	Yes
Oria File Server		
All	on Linux servers	Yes
All	non-virtualized	Yes
MiContact Center Business	delivered only on Microsoft Windows	No
MiVoice Business Reporter	delivered only on Microsoft Windows	No
MiVoice Call Recording		No

The MSL installation includes configuration of the parameters in the following table.

CONFIGURE...	MSL SETTING NAME
Local networks	Configuration - Networks
Remote access	Configuration - Remote Access
Domains	Configuration - Domains
Time	Configuration - Date and Time
SNMP	Configuration - SNMP
E-mail addresses	Configuration - Email Settings

An ARID can be entered in the Administration Console when completing the MSL IP addressing configuration.

Prerequisites

- The MSL Qualified Hardware List has been consulted to confirm that the intended MSL version is compatible with the intended components for each server. The MSL Qualified Hardware List is available on Mitel OnLine.

Any servers NOT in the MSL Qualified Hardware list must carry out self-qualification testing prior to obtaining Mitel service provider certification.

- The MSL packages are ready for download onto portable media or an FTP server.

Resources

RESOURCE	CONTENT DETAILS
<i>Mitel Standard Linux Installation and Administration Guide</i>	Use the standard MSL installation process, "Install MSL Software". Also see the topic called "BIOS settings for RAID".
Mitel Standard Linux System Administration Help	Help topic, "Configure the Server Settings".
MSL Qualified Hardware List	Ensure that the BIOS settings have been set correctly for the server being used.
Oria Service Provider Help and Installation Guide	Instructions for installing Oria Platform Manager and the HTTP File Server

Configure AMC licensing

Connect to the Applications Management Center (AMC) license server to create and manage the licenses for the service provider and for the Customers. Connecting to the AMC allows the license details to be provided to the Mitel applications, and establishes a source for software downloads and upgrades.

In MiCloud, end-users are provisioned through Oria with MiCollab using UCC licensing on MiVoice Business. However, Oria is not able to provision a user until the MiVoice Business administrator makes these licenses **Locally Allocated. (License and Option Selection form > Multi-device Users)**. The SB topology uses Basic IPT, Standard IPT, and UCC Entry SB only,



Note: When UCC v4 Entry, Standard, and Premium licenses are allocated to a ULM containing both a MiVoice Business and MiCollab (if applicable*), AMC allocates MiVoice Business Enterprise Multi-device User Licenses to the MiVoice Business.

*If MiCollab advanced functionality is not being used, then it is not necessary to include the MiCollab in the ULM.

Create and activate application record IDs (ARIDs) to license the Mitel network components, including:

- MiVoice Business Multi Instance server
- Oria
- MiVoice Border Gateway (MBG) servers
- MiCollab
- Mitel Open Integration Gateway (OIG)

MiContact Center Business, MiVoice Business Reporter, and MiVoice Call Recording have ARIDs, and they are now managed in AMC. Contact your Reseller for details.

Networks of MiVoice Business systems should be grouped together in a Designated License Manager (DLM) group. DLM group licensing saves time by allowing movement of licenses from one MiVoice Business platform to another within a network of MiVoice Business systems without having to make changes to the individual application records on the AMC for each MiVoice Business. Both DLM and ULM are types of Group Application Record IDs, or GARIDs. The core topology components are licensed to the service provider and are not linked to any specific customer.

For a MiCloud solution that includes UC functionality, UCC License Manager (ULM) Groups must be used. A ULM can contain one MiCollab system, one MiVoice Business or multiple DLMs, and optional MiVoice Border Gateways. For the SB topology:

- One ULM must be associated with one MiCollab running the MiCollab Client Service.
- Multiple ULMs are needed for multiple MiCollab deployments, one per platform.
- Do not add Oria to the ULM.

The DLM Group ARID (GARID) is associated with the ULM GARID for distributing licenses to the MiVoice Business instances. Typically one ULM GARID is associated with a single MiCollab Client server, and with multiple DLM GARIDs. The DLM manages a Customer's clustered tenants.

It is possible to have one MiCollab and multiple MiVoice Business instances, MiVoice Border Gateways, and Open Integration Gateways (OIG) in the ULM. This supports a deployment that includes MiCollab Client Service Multi-Tenant features.



Note: When deploying MiCollab Client Multi-Tenant, you must install MiCollab Client in Co-located Mode. Do not run the Install Wizard.

In MiCloud SB, there is typically one DLM per Customer. For example, if there are ten Customers, there will be ten DLMs under the Service Provider ULM.

Prerequisites

- The service provider must have an AMC account and the login credentials must be available. UCC licensing training is available through Mitel University.
- Technicians have AMC training, and have referred to the AMC section of the *MiCloud Business for Service Providers Licensing Structures* (available from Mitel Managed Service Provider Program).
- The Mitel Configure Price Quote was used by Service Providers or Mitel Sales Engineering to determine license and part number requirements.
- A service provider purchase order must be in place for purchasing licenses.
- 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.

Resources

RESOURCE	CONTENT DETAILS
Mitel Application Center Manager Online Help	Refer to the following help topics: <ul style="list-style-type: none"> • “Creating Application Record IDs for Customer Products” • “Create and manage accounts”
AMC account support	amccounts@mitel.com
<i>MiCollab Installation and Administration Guide</i>	When implementing MiCollab Client Multi-Tenant, see “MiCollab Multi-Tenanting”.
<i>MiCollab Engineering Guidelines</i>	When implementing MiCollab Multi-Tenant, see “Multi-Tenanting”.
<i>MiCloud Business for Service Providers Licensing Structures</i>	Available from the Mitel Managed Service Provider Program.
<i>MiCloud Business Solution Blueprint</i>	Topology/architecture details and licensing.
<i>Mitel Standard Linux Installation and Administration Guide</i>	
Mitel Standard Linux Online Help	For DLMs, see “Creating License Management Groups”.

MiCloud Business Multi-Instance Deployment

RESOURCE

CONTENT DETAILS

*Managed Service Provider
Program*

*MiCloud Business for
Service Providers
Licensing Structures*

Synchronize to AMC

The AMC synchronization succeeds if the networking configuration is correct. Repeat this on all of the servers that will host the Mitel components.

This synchronization must be repeated whenever new ARIDs are created.

Prerequisites

- Proper ARIDs have been created in the AMC account.
- An AMC connection has been created for software downloads and upgrades.

Resources

RESOURCE

CONTENT DETAILS

*Mitel Standard Linux
Installation and
Administration Guide*

See the *MSL Installation and Administration Guide*, "About the Applications Management Center".

Deploy MiVoice Business Multi Instance

Download, install, and configure the MiVoice Business Multi Instance on the assigned servers. Deploying MiVoice Business Multi Instance includes installing the MiVoice Business Multi Instance Manager blade and the Media Server Manager blade on separate physical servers.

The MiVoice Business Multi Instance platform provides the multiple MiVoice Business instances required for Customers.

There may be more than one MiVoice Business Multi Instance. All are deployed in non-VLAN mode and enabled for SNMP.



Note: Refer to the *Multi Instance Communications Director Engineering Guidelines* for installation options and scaling considerations. This guide is available on Mitel OnLine.

In MiVoice Business Multi-Instance Media Server Manager (MSM), create an MSM instance for each MiVoice Business tenant. Program each MSM instance with the IP address of the MiVoice Business tenant it will service.

In “Deploy temporary MiVoice Business instances” on page 31, you will create two new MiVoice Business instances to be used for test purposes as part of the MiCloud Business Multi-Instance deployment.

Prerequisites

- The appropriate software packages are ready for download on portable media, an FTP server, or the AMC.
- Servers being used are on the MSL Qualified Hardware List.

Any servers NOT in the MSL Qualified Hardware List must carry out self-qualification testing prior to obtaining Mitel service provider certification.

Resources

RESOURCE

CONTENT DETAILS

MiVoice Business Multi Instance Installation and Administration Guide

- Follow the procedure in “Install the software blades”. This section describes installing the MiVoice Business Multi Instance blade and the Media Server Manager.
- The Media Server Manager must be installed using the directions in “Installing Media Server Manager”.

Deploy temporary MiVoice Business instances

Deploy temporary MiVoice Business instances to create a set-up for testing the core voice components. Create two MiVoice Business instances and configure them in a cluster with resiliency.



Note: Install a third-party certificate on each MiVoice Business. Export it for later installation on all applications.

Configure a resilient MiVoice Business cluster. Start by establishing interconnectivity between the two test 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.

Use the MiVoice Business Multi-Instance GUI to create and license new Customers, including restoring a Golden database.



Note: There are two ways to create the new database:

1. Restore the Golden database, and then fix the IP address to avoid conflicts.
2. Set up the IP addresses, and then import the database info using CSV import files.

See the MiVoice Business documentation for details.

The temporary MiVoice Business instances will be removed after deploying and testing the Teleworker configuration.



Note: Although these MiVoice Business instances may be considered temporary, AMC licenses and valid ARIDs are required.

Prerequisites

- The appropriate software packages are ready for download on portable media, an FTP server, or the AMC.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Business Cluster Design and Implementation</i>	Creating a MiVoice Business cluster is a four-step process. <ul style="list-style-type: none"> • “Prepare elements for clustering” • “Populate the Network Elements form” • “Create the cluster” • “Start sharing data via SDS”
MiVoice Business Multi Instance Manager Administrator Online Help	Configure a MiVoice Business Instance; see “MiVoice Business Instance Detail”. See “Install the MiVoice Business instance software” to deploy the software on the MiVoice Business Multi Instance needed for adding MiVoice Business instances <ul style="list-style-type: none"> • Rather than using the default database, load the Golden database. • If MiVoice Business is in a DLM cluster, ensure that the end-user licenses are allocated among Admin group members.

RESOURCE

CONTENT DETAILS

MiVoice Business Multi Instance Engineering Guidelines

See "SIP Trunking".

Program internal phones for testing

Create and program at least two extensions, Test calls between extensions will verify that the MiVoice Business Multi Instance and MiVoice Business instances are operational. These test phones are attached directly to the internal Service Provider network, (they are not Teleworker phones yet).

Make internal test calls to confirm that voice connections can be properly made between at least two internal extensions. Successful test calls confirm that the core voice components are correctly deployed. This is the first set of test calls made during the MiCloud deployment.



Note: The MiVoice Border Gateways are in place, but not fully configured, so if the phone calls fail, then the call problem is isolated to the MiVoice Business and the MiVoice Business Multi Instance.

Prerequisites

- The phones have been programmed with Static IP addresses on the Service Provider network, or there is an active DHCP server with the necessary option already programmed.
- A test plan has been created to define the tests that are to be performed and the criteria for measuring that the system performs correctly.

Resources

RESOURCE	CONTENT DETAILS
MiVoice System Administrator Online Help	<p>Create end-user extensions on the MiVoice Business controllers.</p> <ul style="list-style-type: none"> • “Adding users and services” <p>Add the physical phones to the MiVoice Business system.</p> <ul style="list-style-type: none"> • “Program single line IP telephones” • “Program multiline IP telephones”
Installation guides for end-user devices	<p>The installation documentation for all Mitel end-user devices is found here: http://edocs.mitel.com/Installation%20Guides/index.html.</p>

Deploy VMware® vCenter™ and vSphere®

If virtualized UC components are planned in the network, OIG/MiVoice Integration Virtual, or virtualized MiCollab Client Service Multi-Tenant for example, VMware vSphere and vCenter must be installed on dedicated servers. VMware may also be needed for MiVoice Border Gateway Virtual instances for MiCollab, or if the Service Provider needs VMware High Availability (HA) for the virtual applications.

Deploy the virtual infrastructure to build the server environment capable of running the virtualized Mitel applications used in the MiCloud SB reference architecture.

Deploying 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. Ensure sufficient numbers of servers for the following applications, taking into account those that can share servers, and those that must have dedicated servers:

- MiCollab
- MiVoice Border Gateways
- Oria
- Mitel Open Integration Gateway
- MiContact Center Business

Install vCenter and vSphere

Deploy VMware vSphere to set up the servers that will be running the Mitel applications used in the topology. Deploy VMware vCenter to easily manage the vSphere servers that the Mitel applications will reside on. Deploying vCenter also allows automated VMware High Availability (HA) capability.

Prerequisites

- Server hardware that complies with the VMware Compatibility Guide for the intended Mitel virtual applications has been purchased and installed.
<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=io>
- VMware vSphere and VMware vCenter have been purchased and licensed.
- VMware Service Provider licenses have been obtained.
- 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. Alternatively, engage Mitel Professional Services to complete the installation.

Resources

RESOURCE	CONTENT DETAILS
Manufacturer docs	Installation and configuration instructions for the server hardware.
VMware Product Interoperability Matrixes	http://www.vmware.com/resources/compatibility/sim/interop_matrix.php
VMware documentation	Installation instructions for vCenter and vSphere. https://www.vmware.com/support/pubs/
<i>Virtual Appliance Deployment Solutions Guide</i>	This guide, available on Mitel OnLine, includes hardware requirements for Mitel virtual appliances. http://edocs.mitel.com/TechDocs/Solutions-Guides/BP-Virtualization.pdf

Chapter 4

SHARED GATEWAYS DEPLOYMENT

SIP trunk configuration

Configure SIP trunks to connect to the voice services offered by the SIP trunk service provider. The SIP trunk MiVoice Border Gateway cluster and the MiVoice Business cluster are configured with the appropriate access credentials, DID numbers, and incoming call routing.

Deployment success is verified by testing the configuration by making and receiving external calls.

Prerequisites

- SIP Trunk licenses must be available in MiVoice Business.
- The appropriate software packages are ready for download on portable media, an FTP server, or the AMC.
- Configuration already includes:
 - the SIP Service Provider details, including IP addresses
 - SIP Trunks have been purchased
 - there have been successful test calls on the MiVoice Business instances.

SIP trunk configuration task flow

This topics list shows the sequence of tasks that must be performed to configure the SIP trunks needed for deploying the topology.

- “Deploy SIP trunk MiVoice Border Gateway cluster” on page 40
- “Configure MiVoice Border Gateway for SIP trunk connection” on page 41
- “Configure MiVoice Border Gateway DID/DDI routing tables” on page 43
- “Configure MiVoice Business SIP routes and resiliency” on page 44
- “Deploy MiVoice Border Gateway clusters for end-user MiNet devices” on page 47
- “Deploy SIP and UC MiVoice Border Gateway cluster” on page 49

Deploy SIP trunk MiVoice Border Gateway cluster

Download, install, and configure the cluster of MiVoice Border Gateways (MBG) to provide a resilient gateway between the service provider network and the SIP trunk provider. The MiVoice Border Gateways are configured to provide incoming DID/DDI redirection.

If you are using MiVoice Border Gateways on Industry Standard Servers (ISS) follow these instructions:



Note: If you are installing MiVoice Border Gateway Virtual, skip these steps and deploy the OVA. See the *Virtual Appliance Deployment Solutions Guide* for details.

1. “Install and configure Mitel Standard Linux (MSL)” on page 24
2. “Synchronize to AMC” on page 29

SIP trunk connections are completed after the core voice services (that is, the MiVoice Business Multi Instance instances) have been set up and verified as working.

The number of MiVoice Border Gateways in the cluster is based on the immediate scaling requirements of the topology.

Create additional MiVoice Business instance entries on the MiVoice Border Gateway for test purposes.

Prerequisites

- The number of MiVoice Border Gateways in the cluster must be determined using the scaling information provided in the *MiCloud Business Solution Blueprint*.
- The appropriate software packages are ready for download on portable media, an FTP server, or the AMC.
- Hardware servers have been deployed and configured.

Resources

RESOURCE

CONTENT DETAILS

<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	Refer to the following sections of this guide: <ul style="list-style-type: none">• “Configure SIP Trunking”• “Install MBG Software on an Online System”• “Install MBG Software on an Offline System” for the MBG installation steps, based on network connectivity.
MiVoice Border Gateway Online Help	See the topic “Configure a Cluster”.
MiVoice Business System Administration Tool / System Administration Tool Online Help	Create MiVoice Border Gateway Network Element, configure Class of Service, and configure as described above. Also refer to “Programming SIP Trunks”.

Configure MiVoice Border Gateway for SIP trunk connection

Set up a connection between the SIP trunk service provider and the clustered SIP trunk MiVoice Border Gateway. The MiVoice Border Gateway configuration includes configuring the outgoing proxy and the incoming DID/DDI routing rules.

- In the MSL **Administration** panel, ensure that MiVoice Border Gateway Web Services is running with Oria.
- In the MiVoice Border Gateway Blade, set **SIP Support** to **Enabled (MBG > Configuration > Settings)**.
- Ensure that the designated DNS server for the MiVoice Border Gateway has FQDN entries for the MiVoice Business instance host names, that will be added to MiVoice Border Gateway “ICPs Listing”. This is set in the MBG **Configuration** tab, under **ICPs**. Oria creates ICP entries in the **MBG Configuration** tab, under **ICPs**.
- Set the **Network Profile** to **Server-Gateway on Network Edge**. Then in the **Status** tab, click **Start the MBG**.
- Create the SIP Trunks in the MiVoice Border Gateway cluster. Each SIP Trunk needs an initial “dummy” ICP value, for MiVoice Border Gateway to complete the trunk creation. Trunks must exist in the MiVoice Border Gateway first; otherwise Oria will fail to create new DID entries for new Customers.
- To maintain the availability of SIP trunks, configure MiVoice Border Gateway to keep the connection active by pinging the ICPs. For each SIP trunk, access the SIP trunking screen and program the following:
 - Set **Options Keepalives** to Always.
 - Set **Options Interval** to 20.



Note: Ensure that this configuration is implemented for a resilient trunk configuration. Otherwise, in the event that an ICP becomes unavailable, the secondary connection may not be active and calls may fail.

- Enter the SIP Service Provider IP address or FQDN in the **Remote trunk endpoint** field.
- Enter the password in **Authentication Username/Password**.
- For this test trunk, set the wild card DID filter in the **Routing Rules** to the test MiVoice Business instance.
- On the **Clustering** tab, Set the **Cluster weight of current node** field for both Master and Slave to 50, for even load balancing between the two nodes. One strategy is to put each MiVoice Border Gateway into its own Cluster Zone, defined in the Clustering tab.

Prerequisites

- Physical and network connections exist
- The DID/DDI numbers are known
- The SIP Trunk provider is known, the SBC addresses are known, and there is agreement on user name and password for access.

Resources

RESOURCE

CONTENT DETAILS

*MiVoice Border Gateway
Installation and
Maintenance Guide*

- Configure the SIP trunk gateway using the instructions in “Adding a SIP Trunk to MBG”.
- “Configure DID Routing Rules for SIP Trunking” explains the DID configuration requirements for SIP trunks.

Configure MiVoice Border Gateway DID/DDI routing tables

Configure the MiVoice Border Gateway DID/DDI routing tables to route incoming DID/DDI numbers to the appropriate MiVoice Business controllers running on the MiVoice Business Multi Instance.

DID	Direct Inward Dialing	North American terminology
DDI	Direct Dial-in	European terminology

Prerequisites

- Each SIP trunk requires a dummy SIP trunk (the wild card DID filter can be used) already in place. Without this, Oria will fail to create new DID entries.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	The section called "Configure DID Routing Rules for SIP Trunking" explains the DID configuration requirements for SIP trunks.
MiVoice Border Gateway Online Help	Refer to the "SIP Trunk Routing by DID" help topic.

Configure MiVoice Business SIP routes and resiliency

Configure MiVoice Business SIP routes and resiliency to handle primary and secondary connections. Primary routes are created via the SIP trunk MiVoice Border Gateways. Secondary routes use the alternative MiVoice Business unit in the MiVoice Business cluster before connecting to the SIP trunk through the SIP trunk MiVoice Border Gateways.

On MiVoice Business, in the System Administration Tool:

1. In the **Network Elements** form, create a network element for the MiVoice Border Gateway, and assign it to the **Outbound Proxy Type**. Refer to the instructions in the *MiVoice Border Gateway Installation and Maintenance Guide*, in the section called “Configuring the MiVoice Business (3300 Controller) to Support SIP Trunks”.
 - In the **System IP Properties** form, ensure that **Host Name** matches the value in the **Name** field in the **Network Elements** form. This is necessary for the SIP Trunks to work.
 2. In the **Class of Service** form for the SIP Trunk Attributes, set the following parameters to **Yes**:
 - **Public Network Access via DPNSS**
 - **Public Network To Public Network Connection Allowed**
 - **Public Trunk**
 3. In the **Trunk Attributes** form, associate this CoS with the SIP trunk.
 4. In the **Network Elements** form, create an entry for the SIP Service Provider, and assign the **Type** to **Other**. Enter the IP address or FQDN of the SIP Service Provider.
 5. Create a SIP Peer Profile for the SIP Service Provider. Follow the instructions in the MiVoice Business System Administrator Tool Help.
 6. Complete the ARS programming to route phone calls out to the SIP network.
 7. If you are deploying MiTeam: For the generic instructions, see the MiVoice Business Administration Tool Help,
 - a. In the **Network Elements** form, add a network element for the MiTeam SIP Trunk.
 - Set **Type** to **Other**.
 - If you will need access for external guests, in **FQDN or IP Address**, enter the FQDN for the MiTeam service. Do not enter the IP address. Choose the MiTeam service from the following list, based on shortest, path, latency, and data sovereignty priorities. The four data centers listed are all cross-linked, so media is re-directed, if necessary.

california.miteamsip.mitel.com

ireland.miteamsip.mitel.com

brazil.miteamsip.mitel.com

singapore.miteamsip.mitel.com
- Select **SIP Peer**.
 - Fill in the **SIP Peer Port**.

- Set **SIP Peer Status** to **Auto-Detect/Normal**.



Note: You must already have an outbound proxy for inbound and outbound PSTN calls.

- b. In the SIP Peer Profile you created for the MiTeam SIP provider, click **Add**.
 - In **Network Element**, select the MiTeam element created earlier.
 - In **Alternate Destination**, enter the Trunk Service number (**Trunk Attributes** form) where the COS/COR and incoming call handling are set.
 - In **Domain FQDN or IP Address**, enter the IP address of the alternate destination domain.
 - In **Trunk Service**, enter the Trunk Service number (**Trunk Attributes** form) where the COS/COR and incoming call handling are set.
 - Set **Maximum Simultaneous Calls**. For help with this calculation, see your Mitel engineer.
 - Set **Minimum Reserved Call Licenses**. For help with this calculation, see your Mitel engineer.
 - In **Outbound Proxy Server** enter the IP address or FQDN for the MiVoice Border Gateway.
 - The rest of the fields can remain at their default values.
- c. Add the SIP trunk MiVoice Border Gateway for the MiTeam service.
 - Log in to MSL for the SIP trunk, and edit the MiVoice Border Gateway. Navigate to **Configure > SIP Trunking**.
 - Click **Add**.
 - Create a new SIP Trunk for the MiTeam service.
 - In **Remote trunk endpoint address**, enter the FQDN for the MiTeam service.
- d. In the **SIP Peer Profile Assignment by Incoming DID** form, program the MiTeam number provided by the Mitel team. This is necessary because there are two SIP trunks using the same MiVoice Border Gateway.
- e. In the MiVoice Business System Administration tool:
 - In the **ARS Routes** form, program the **Route Number** (8, e.g.), the **Routing Medium** (SIP Trunk), **SIP Peer Profile** (MiTeam), and Digit Modification Number (use 250 to prevent any digit stripping).
 - In **ARS Digits Dialed**, Set **Digits Dialed** to the MiTeam number, including area code and country code; for example, **14802409721**. Set **Number of Digits to Follow** (0) and **Termination Type** (**Route=8**, e.g., to match the **Route Number** in the **ARS Routes** form).

Continue the SIP trunk configuration. In the Trunk Attributes form:

1. Define Answer Points for Non-Dial-In (attendant-handled) trunks under the three modes of service: Day, Night 1 and Night 2.
2. Define Digit Modification plans for Dial-In trunks.

3. Enable Call Recognition Service on trunks used to handle calls for External Hot Desk Users.
4. Enable the Direct Inward Dialing (DID) Service feature on specified trunks.

In the System Access Points form:

- Set the **Hot Desking Access Number**.

Prerequisites

- The MiVoice Border Gateway instances have been installed.
- The MiVoice Business instances are installed and working.
- SIP Trunk Service Provider addresses are known.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	Use this guide for details about programming the SIP Outbound Proxy for MiVoice Business tenants. See “Configure SIP Trunking”. This also requires careful configuration on the MiVoice Business controller.
MiVoice Business System Administration Tool Online Help	Relevant help topics: <ul style="list-style-type: none"> • “Programming SIP trunks” provides the process and considerations for configuring the MiVoice Business SIP routes. • The Forms topics provide help for completing the configuration for dialing configurations and trunks. • System Features topics provide guidance on configuring all MiVoice business features, including inward dialing, outward dialing, and trunks.
MiVoice Business System Administration Tool	Direct Inward Dialing (DID) Service form: Use this form to configure a pool of external DID numbers mapped to their destination numbers (that is, internal directory numbers or other answer points on the system). Trunk Attributes form: The Trunk Attributes form is used to assign a Class of Service, Class of Restriction, Baud Rate, Intercept Numbers and a Trunk Label to all trunks.

Deploy MiVoice Border Gateway clusters for end-user MiNet devices

Download, install, and configure the cluster of MiVoice Border Gateways required for the service provider to Customer network connection used for MiNet services. The voice traffic for end-users with MiNet services will be carried through this MiVoice Border Gateway cluster.

Download, install, configure, and license the MiVoice Border Gateways before clustering them together for MiNet services.

On the MiVoice Border Gateway:

1. In the MSL **Administration** > **Web Services**, ensure that MiVoice Border Gateway Web Services is running with Oria.
2. In the MiVoice Border Gateway blade, enable SIP protocols to be supported (**Applications** > **MBG** > **System configuration** > **Settings**).
3. Ensure that the designated DNS server for the MiVoice Border Gateway has FQDN entries for the MiVoice Business Multi Instance host names, that will be added to MiVoice Border Gateway "ICPs Listing". This is set in the MiVoice Border Gateway: **Applications** > **MBG** > **Service configuration** > **ICPs**.
4. Set the **Network Profile** to **Server-Gateway on Network Edge**. Then in **Applications** > **MBG** > **System configuration** > **Network profiles**, click **Start the MBG**.
5. On the **Clustering** tab, Set the **Cluster weight of current node** field for both Master and Slave to 50, for even load balancing between the two nodes. One strategy is to put each MiVoice Border Gateway into its own **Cluster Zone**, defined in the **Clustering** tab.
6. Purchase and install third-party SSL certificates on MiCollab and MiVoice Border Gateway for the Service Provider and for every server.
 - See MSL Online Help: "Manage Web Server Certificate" and "Manage Third-Party Certificates from an Alternate Certificate Authority".
 - This exported third-party certificate will be installed on the MiContact Center Business server when you install MiContact Center Business; "Install MiContact Center Business and MiVoice Call Recording" on page 98.



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.



Note: Create separate MiVoice Border Gateway clusters; one for MiNet devices (this step), and one for SIP devices (this will be done in a future step).

Prerequisites

- The number of MiVoice Border Gateways in the cluster must be determined using the scaling information provided in the MiCloud Blueprint.
- The appropriate software packages are ready for download on portable media, an FTP server, or the AMC.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	<ul style="list-style-type: none">• Follow the steps in “Install MBG Software on an Online System” or “Install MBG Software on an Offline System,” based on the network connectivity.• Use “Server-Gateway Configuration on Network Edge” to configure the MiVoice Border Gateway to support MiNet traffic from the Customer into the service provider’s network.

Deploy SIP and UC MiVoice Border Gateway cluster

Download, install, and configure the cluster of MiVoice Border Gateways required to connect the Customer's network to the service provider's network for SIP and UC services. UC services and the voice traffic for end-users with SIP services are routed through this MiVoice Border Gateway cluster.

Prerequisites

- The appropriate software packages are ready for download on portable media, an FTP server, or the AMC.
- The number of MiVoice Border Gateways in the cluster must be determined using the scaling information provided in the MiCloud Blueprint and the *MiVoice Business Engineering Guidelines*.
- See also "Deploy MiVoice Border Gateway clusters for end-user MiNet devices" on page 47.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	Deploy MiVoice Border Gateway instances. <ul style="list-style-type: none"> • "Installing in a virtual environment" Configure the MiVoice Border Gateway to support SIP and UC traffic from the Customer into the service provider's network. <ul style="list-style-type: none"> • "Server-Gateway Configuration on Network Edge"

Chapter 5

CUSTOMER ACCESS CONFIGURATION

Customer access configuration

Configure customer access devices and connections. Verify the configuration by making and receiving calls with the Teleworker devices.

Prerequisites

- MiVoice Border Gateway instances are in place.

Customer Access configuration task flow

This is the sequence of tasks that must be performed to configure the topology for Teleworker clients.

- “Configure end-user devices in the MiNet MiVoice Border Gateways” on page 54
- “Configure MiNet end-user devices to MiVoice Business” on page 55
- “Configure and test MiNet phones as Teleworker devices” on page 56
- “Use configured phones to make a test call to the SIP trunks” on page 58

Configure end-user devices in the MiNet MiVoice Border Gateways

In this step, configure a couple of test device accounts in the MiNet MiVoice Business Gateway Cluster provisioned earlier.

Configure the end-user devices in the MiNet MiVoice Border Gateways to grant them external access to the internal service provider network.

- The MAC address is used for MiNet-based phones.
- For each end-user phone, choose the MiVoice Business test instance as the target MiVoice Business.
- Configure the MiVoice Border Gateway to support Teleworker devices. For the first pass, set up a Teleworker device as unrestricted by de-selecting the **Restrict MiNet devices** option. This will allow installation without the **ICP Installer Password**.

Later, it will be possible to enable **Restrict MiNet** devices, and register a Teleworker phone against the ICP with the Installer password.

Prerequisites

- MAC addresses for the deployed phones are known and can be pre-programmed in the MiVoice Border Gateway cluster.

Resources

RESOURCE

CONTENT DETAILS

*MiVoice Border Gateway
Installation and
Maintenance Guide*

See "Configure Teleworker Service".

*Remote IP Phone
Configuration Guide*

This book describes considerations for configuration at the end-point device to support teleworking.

Configure MiNet end-user devices to MiVoice Business

In this step, program a couple of test telephone entries in the resilient pair of MiVoice Business instances created earlier.

Configure end-user devices in MiVoice Business to specify the MiNet end-user devices with the MAC addresses already programmed in the MiVoice Border Gateway.

Connect the MiVoice Business and the MiNet MiVoice Border Gateways to allow the MiNet Teleworker devices to connect to the MiVoice Business. The MiVoice Border Gateway uses the IP address or the FQDN in DNS of the MiVoice Business to pass the end-user device connections to the MiVoice Business system.

Prerequisites

- Equipment is installed and operational.
- DNS servers are available internally, and programmed.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	Refer to: <ul style="list-style-type: none"> • “Provisioning MiNet Devices” for instructions. • “Configuring the Teleworker Service on MBG” for instructions.
<i>MiVoice Border Gateway Engineering Guidelines</i>	See “MBG Capacities – Device (MiNet & SIP) and Trunking (SIP)”.

Configure and test MiNet phones as Teleworker devices

Configure MiNet phones as Teleworker devices and specify the public IP address of the MiVoice Border Gateway that the devices use for connecting to and registering as extensions.

This is the third set of test calls being made during the MiCloud deployment— test calls using Teleworker phones. These phones are attached to an external network, (such as a sample remote Customer network), to target the MiVoice Border Gateway WAN interface.

Do this in two stages to allow intermediate testing:

- Configure the phones as Teleworker devices with the MiVoice Border Gateway IP address. Make a test call, to make sure the MiVoice Border Gateways are working.
- Delete any entries or restore the phone to factory defaults. Then, using the Mitel Redirection and Configuration Server (RCS), create IP Phone profiles in the Zero Touch Provisioning account at rcs.aastra.com. (The IP Phone needs at least firmware version MAIN 6.0.2.6.)

Power up the phones from Factory Default. They will contact the RCS server to determine the MiVoice Border Gateway public address. They will register automatically with the appropriate MiVoice Business through the targeted MiVoice Border Gateway.

Prerequisites

- Each phone must have an IP address, which can be pre-programmed statically, or provided by a local DHCP server.
- The location of the appropriate MiVoice Border Gateway to use. This can be provided using one of these methods:
 - Using Mitel-specific options programmed in the DHCP server
 - Pre-programmed MiVoice Border Gateway information in the RCS.



Note: Many simpler DHCP servers provide only base level options and may not be able to programmed with other standard options, including the Mitel vendor specific options. In this case the RCS can be used to redirect the phone to the appropriate gateway.



Note: Do not program the DHCP vendor-specific options if the RCS is to be used for deployment. The service provider must program the RCS.

- The RCS is pre-programmed to recognize the phone MAC address and direct this to the appropriate MiVoice Border Gateway.

Resources

RESOURCE

CONTENT DETAILS

MiVoice Border Gateway Installation and Maintenance Guide See “Configure Teleworker Service”.

RESOURCE

CONTENT DETAILS

*Redirection and
Configuration
Service (RCS) User Guide*

See "IP Phone Redirection".

Use configured phones to make a test call to the SIP trunks

This is the second set of test calls being made during the MiCloud deployment.

Make test calls to confirm that voice connections can be properly made between an internal extension and external phones in the public network. Successful test calls confirm that the core voice components and SIP trunking are correctly deployed.

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Chapter 6

ORIA DEPLOYMENT

Oria deployment

Install and configure Oria as a management tool for the network. The first MiVoice Business instances that could be allocated to a real Customer are created here, but these are used to test Oria. You have the option of deleting these instances after testing is completed, if desired. These instances use a fresh Golden database.

Testing will confirm Oria's success in configuring the topology, and the suitability of the standard templates.

Prerequisites

- Default databases on all instances of MiVoice Business
- Site administrators must have taken the Mitel Oria training.
- Any licensing restrictions are known.
- Ensure that the extension range set up for Oria is different from the range used for the testing.

Oria deployment task flow

This shows the sequence of tasks that must be performed to deploy Oria.

- "Prepare resilient MiVoice Business instances for management by Oria" on page 62
- "Install and configure Oria" on page 64
- "Configure external access to Oria" on page 66
- "Register a test Platform Group" on page 67
- "Create Basic IP Telephony (IPT) Oria bundles" on page 68
- "Create a test customer" on page 69
- "Add test users with Oria" on page 70

Prepare resilient MiVoice Business instances for management by Oria

Using the two instances of MiVoice Business with a default database created when testing SIP trunks, test Oria by provisioning the first test customer.



Note: The resilient MiVoice Business configuration is highly recommended, but not mandatory.

Prepare the MiVoice Business instances for management by Oria. At a minimum, the target MiVoice Business instances need to have Embedded Voice mail Messaging (EMEM) running. They must be in resilient clusters if end-user resiliency is required.

Prerequisites

- MiVoice Business instances are all running an Golden database. Refer to the Oria documentation for a description of the MiVoice Business programming needed to represent a valid Golden database.
- MiVoice Business licensed ARIDs have been prepared in AMC.
- The MiVoice Border Gateways have been installed and are operational.
- You have the details about the customers the system will be serving.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Business Multi Instance Installation and Administration Guide</i>	Build the temporary instances for testing the topology configuration. <ul style="list-style-type: none"> • “Add MiVoice Business Instances”
MiVoice Business Multi Instance Manager Administrator Online Help	Configure a MiVoice Business Instance. <ul style="list-style-type: none"> • “MiVoice Business Instance Detail”. This help topic includes a description of the parameters that can be configured for the MiVoice Business instances.
<i>MiVoice Business Clustering Design and Implementation</i>	Creating a MiVoice Business cluster is a four-step process. Use the following procedures to cluster the MiVoice Business instances: <ul style="list-style-type: none"> • “Prepare elements for clustering” • “Populate the Network Elements form” • “Create the cluster” • “Start sharing data via SDS”
<i>MiVoice Business Resiliency Guidelines</i>	See “Resilient system elements and interactions”.
MiVoice Business System Administration Tool Online Help	See “Configuring a cluster”.
<i>Oria Installation and Administration Guide</i>	Configure MiVoice Business for using Oria: <ul style="list-style-type: none"> • “Determine and Collect the Business Requirements” • “Register Platforms Groups in Oria” • “Configure the Default Platform Database”

RESOURCE

CONTENT DETAILS

*Oria Engineering
Guidelines*

See "MiVoice Business Default Database".

Install and configure Oria

Install and configure Oria to create a secure management portal for end-user administration.

If you will be using Oria Platform Manager (OPM), log in to MSL, and install the following Oria features from CD:

- Oria Platform Manager
- Oria File Server

For best performance, install these on two separate servers.



Tip: Understand the scope of all the tasks described in this guide before deploying Oria. Do not pre-configure settings that will be covered in future tasks during the deployment process.

Oria initial programming includes:

- Administrator accounts
- Operations profiles
- Virtual Service Providers, and Value Added Resellers
- Registering the MiVoice Border Gateways and MiCollab Client Server
- Create test Bundles
- In the MSL Server-Manager console of Oria, enter your SMTP Server IP Address into the **E-mail Settings** panel under **Configuration**. This is required for Oria to send Welcome e-mails to new users.

Program the MiVoice Border Gateway Web Proxy services to provide remote access to Oria Portal. (next section).



Note: A single cluster will be associated with a single customer. Therefore multiple instances of MiVoice Business will be configured in multiple independent clusters, one cluster per customer. One cluster may include multiple instances.

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 Oria mbgZones.xml file. See the Oria 5.0 documentation for a description of how this is done.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
<i>Oria Installation and Administration Guide</i>	Oria installation. <ul style="list-style-type: none">• “Installation overview” Guidance for configuring Oria. <ul style="list-style-type: none">• Initial system configuration”
Oria Service Provider Portal Help	Install Oria Platform Manager (OPM) and Oria File Server (OFS).
<i>Oria Engineering Guidelines</i>	For best performance, use the engineering guidelines to ensure that the configuration respects allowed capacities and limitations. See “Managing MiVoice Border Gateway Cluster Zones”.

Configure external access to Oria

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

In Mitel Standard Linux, use the MiVoice Border Gateway user interface to create and configure a web proxy.

1. On the MSL server, select **Applications > Remote proxy services**.
2. Click **Add new LAN server proxy**.
3. On the **Configure Web Proxy & Remote Management Service** page:
 - a. Select **Enabled** to enable the web proxy.
 - b. In **WAN-side FQDN**, enter the FQDN that resolves to the Oria IP Address on the internal DNS Server. The same FQDN must resolve to the MiVoice Border Gateway WAN IP address, on the external public DNS Servers.
 - c. Select **Oria**.



Note: MiVoice Border Gateway **Remote Proxy Services** programming is not auto-shared across the MiVoice Border Gateway cluster. Therefore, this programming must be duplicated on other MiVoice Border Gateway Cluster members when there is a need to have High Availability access to Oria.



Note: Program the **Alias** entries in the External DNS server for each MiVoice Border Gateway WAN IP address that serves as an MiVoice Border Gateway Web Proxy. This is for back-up access to Oria, in case of an MiVoice Border Gateway proxy server failure.

4. Test external connectivity to Oria to verify that the web proxy setup in the user MiVoice Border Gateway is working correctly. The external connections must work correctly to allow global access to Oria for end-users, administrators, and the service provider.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

MiVoice Border Gateway Installation and Maintenance Guide

MiVoice Border Gateway web proxies and how to create and manage them; see “Remote proxy services”

Register a test Platform Group

Register a test Platform Group and the resilient MiVoice Businesses and MiNet MiVoice Border Gateways and add them to a Platform Group in Oria. The Platform Group includes the MiVoice Business, MiVoice Gateway, and (further below) the MiCollab Client components for a customer.

This test Platform Group will be deleted after the Oria deployment has been validated.

Another Oria task associates the Platform Group to a customer and end-users. See “Install and configure Oria” on page 64.

Prerequisites

- The MiVoice Business instances are configured before creating the Oria Platform Group.

Resources

RESOURCE

Oria Installation and Administration Guide

CONTENT DETAILS

Follow the instructions in:

- “Register Mitel Border Gateway” (now called MiVoice Border Gateway)
- “Register Platform Groups in Oria”

Create Basic IP Telephony (IPT) Oria bundles

Create Basic IP Telephony (IPT) Oria license bundles to set up the basic feature packages for voice services. In a future step, you will test that the Oria configuration is correct by assigning the feature bundles to end-users and validating that they function properly.

Feature bundles are available across the solution and are applicable to any customer. More bundles are created when adding customers with UC and additional features to the solution.

Prerequisites

- Basic IPT license has been applied to the MiVoice Business ARID.

Resources

RESOURCE	CONTENT DETAILS
<i>Oria Installation and Administration Guide</i>	See "Create bundles".
Oria training	http://mitel.ca/product-service/mitel-training

Create a test customer

Create a test customer to verify that Oria is configuring end-users and customers correctly using the feature bundles that are installed. Assign the test Platform Group and the Basic IPT feature bundles to the test customer.

To create a new Customer in Oria:

1. Enter details in the following fields:

• Customer Address	• Phone Number
• Web ID	• Platform Group
• Dial Plans	• Key Templates
• CPN Number (from Site)	• CESID Locations (Network Zone from Site)
• Brand select	• Time Zone
• DID Ranges (for additional Ranges beyond those already there from the Platform Group)	• Extension Length

2. Select the number of Bundles and the Phone Devices.

3. Select Language.

4. Create an Admin User and Login.

5. Assign the Admin Bundle.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

<i>Oria Engineering Guidelines</i>	See "New customer setup".
Oria Online Help	In Oria, select Customers > View Customers and click Show Help to display help topics for creating and managing customers in Oria.

Add test users with Oria

Add test users to verify that Oria and the topology components are correctly installed. End-users can then be assigned to customers with the Basic IPT feature bundles using Oria. This is the fourth set of test calls being made during the MiCloud deployment.

The MiVoice Business native management interface is not needed for adding the end-users. Oria manages users and devices directly on the MiVoice Business instances. The MiVoice Business System Administration Tool is used only to verify that the end-users configured through Oria appear in the MiVoice Business configuration with the same settings used in Oria.

Register test phones on MiVoice Business and make calls to test and verify that the telephony configuration operates correctly for end-users and components that have been configured using Oria.

Prerequisites

- MiVoice Business instances must already be running a golden database. This includes licenses, a System Applications Account, Embedded Voice mail Messaging, and CoS and CoR settings, and so on.

Resources

RESOURCE

CONTENT DETAILS

Oria Online Help	In Oria, select a customer from the Customers > View Customers tab and log in as the customer administrator. Select the Users tab and click Show Help to display help topics for creating and managing end-users.
System Administration Tool Online Help	Verify the end-user configurations in MiVoice Business. <ul style="list-style-type: none">• See the Forms topic “User and Device Configuration”.

Chapter 7

(OPTIONAL) MITEL PERFORMANCE

ANALYTICS DEPLOYMENT

OPTIONAL: MITEL PERFORMANCE ANALYTICS DEPLOYMENT

Mitel Performance Analytics is available as a Software as a Service (SaaS) and links to customer probes deployed on site, or in the service provider network. This installation considers a deployment where the service provider includes a Mitel Performance Analytics server within their own network.

Contact Mitel Cloud Services for licensing details.

Prerequisites

- The installer has Mitel Performance Analytics documentation on hand. It is available on Mitel OnLine.

Mitel Performance Analytics deployment task flow

This is the sequence of tasks that must be performed to configure Mitel Performance Analytics monitoring of the topology:

- “Install Mitel Performance Analytics” on page 74
- “Configure Mitel Performance Analytics” on page 75

Install Mitel Performance Analytics

Install the Mitel Performance Analytics server and the probe instances used to monitor the network. The Mitel Performance Analytics server OVA must be licensed. Contact Mitel Cloud Services for details.

The on-premise version of the Mitel Performance Analytics server is provided as an OVA file that can be deployed in a 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 server OVA is available in three different package sizes. Review the documentation, and consult with Mitel Professional Services to determine the correct size for the network.

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.

Prerequisites

- A static IP has been assigned for the Mitel Performance Analytics server instance. Access to premise Mitel Performance Analytics will be gained “Over-the-Top” via the Service Provider’s existing proxy/firewall.
- An external DNS entry has been created for the Mitel Performance Analytics web portal URL.

Resources

RESOURCE	CONTENT DETAILS
This guide: Appendix	See “Mitel Performance Analytics deployment” on page 197.
<i>Mitel Performance Analytics System Guide</i>	The Mitel Performance Analytics System Guide includes a section describing “Mar probe Installation and Configuration”. Also refer to the documentation on Mitel OnLine.

Configure Mitel Performance Analytics

Configure Mitel Performance Analytics to monitor the service provider core network space for alarms and network activity. Mitel Performance Analytics 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.

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.

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.

Prerequisites

- Enable SNMP on the customer devices that the Probe will be monitoring and configure the community string. Do not use the default community string value, but pick an alternative value that is unique to the customer.

Resources

RESOURCE

CONTENT DETAILS

Mitel Performance Analytics System Guide

The Mitel Performance Analytics System Guide includes a section describing "Probe Installation and Configuration".

Chapter 8

UC APPLICATIONS DEPLOYMENT

Unified Communications applications deployment

Create the MiCollab server (virtual or physical), MiVoice Border Gateway Virtual, and feature bundles required for providing UC and SIP services to Customers.

Deploying UC may also include installing and configuring the OIG Virtual for Salesforce integration, Google integration, or custom applications.

In this section, MiVoice Border Gateways may be clustered together, with one MiVoice Border Gateway being the “Master” of its cluster. There can be a number of clusters. The same is true of MiVoice Business controllers. Oria can be used to manage the network through its connection to the Master elements, so if a Master MiVoice Border Gateway or a Master MiVoice Business controller is out of service, Oria will not be able to perform user management tasks until the Master element is brought back into service.

Prerequisites

- The physical network and licensing is in place.
- Licensing ULM and DLM have been defined and configured in Mitel AMC.

Unified Communications applications deployment task flow

The sequence of tasks to perform to deploy and test the UC services is described here.



Note: The applications described in this chapter can be assumed to be optional.

- “Deploy MiCollab” on page 80
- “Configure proxy services for MiCollab Client” on page 82
- “Configure MiVoice Border Gateway for WebRTC users” on page 84
- “Configure MiCollab for mobile users” on page 85
- “Create UC Bundles in Oria” on page 87
- “Create a UC-capable test Platform Group in Oria” on page 89
- “Create a UC-capable test customer and test end-users in Oria” on page 92
- “Synchronize MiCollab Client and MiVoice Business” on page 93
- “Register UC devices and test MiCollab Client” on page 94
- “Deploy Open Integration Gateway Virtual (OIG Virtual)” on page 95
- “Configure Open Integration Gateway Virtual proxy services” on page 96
- “Test Open Integration Gateway configuration” on page 97
- “Install MiContact Center Business and MiVoice Call Recording” on page 98
- “Deploy business analytics” on page 101
- “Delete the test set-up” on page 102

Deploy MiCollab

Install and configure the MiCollab application for creating tenanted MiCollab Client Server. Each MiCollab Client tenant provides light UC capabilities to many customer enterprises. See the *MiCollab Client Engineering Guidelines* for the latest capacity numbers. A Service Provider network may include a number of MiCollab Client servers. License the MiCollab using a Unified License Manager (ULM) in the AMC.



Note: When deploying MiCollab Client Multi-Tenant, you must install MiCollab Client in Co-located Mode. DO NOT run the Install Wizard.

MiCollab can be installed in physical or virtual form. To deploy MiCollab in Multi-tenant mode, set the MiCollab Client service to **Co-located Mode** at time of install.

After installing MiCollab, do the following on each MiCollab server:

1. Access the MiCollab command line using PuTTY and the MiCollab IP address to log in to the server.
2. Execute the following command to enable the enterprise configuration.
`signal-event ucserver-enable-enterprise-configuration`
3. The MiCollab Client Service restarts. Wait until the MiCollab Client Service status returns to ACTIVE.

When using MiCollab in a Multi-Tenant configuration with Oria:

- All tenants are configured on the same MiCollab Client, with unique Enterprises per Tenant.
- When a Platform Group is created, it creates the Enterprise on the MiCollab server.
- MiCollab is installed as a single-application server, meaning that only MiCollab Client is licensed and configured.
- When users are created, they are grouped with their corresponding Tenant Enterprise.
- When Bundles are created, and users created within the bundles, all MiCollab Client Deployment Profiles are created in the same Deployment Profile “pool”.
- For the multi-tenant MiCollab case, Oria provides a capability in the **Platform** tab to define an Enterprise per Platform. For Enterprises on the same MiCollab host, it is expected that the host name and public FQDN will be the same for all those Enterprises.
- To scale higher than 150 Tenants/Enterprises, you may require more than one MiCollab Client server. In that case, Service Providers must add new DNS entries into external DNS server, whose FQDNs resolve to the WAN of the new MiVoice Border Gateway cluster. Recall that MiVoice Border Gateway can target only one MiCollab.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
Application Management Center Online Help	See: <ul style="list-style-type: none"> • “MiCollab Virtual Appliance (vMiCollab)” • “Installing Virtual MiCollab in a VMware Environment”
MiCollab Client Deployment Help	See: <ul style="list-style-type: none"> • “Adding and Editing Feature Profiles” • “Enterprise Tab”
<i>Virtual Appliance Deployment Solutions Guide</i>	Available on Mitel OnLine: http://edocs.mitel.com/TechDocs/Solutions-Guides/BP-Virtualization.pdf
<i>Oria Installation and Administration Guide</i>	See “MiCollab Client Multi-Tenant”.

Configure proxy services for MiCollab Client

Configure proxy services for MiCollab Client to set up routes through the MiVoice Border Gateway instances to the MiCollab Client Service for external connectivity to the UC services.

On the existing SIP user MiVoice Border Gateways (or if creating new MiVoice Border Gateways), program MiVoice Border Gateway Application Integration to enable the MiCollab Client Connector, and point at the MiCollab Client Service FQDN: **Service Configuration** tab > **Applications Integration**

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

1. Program MiVoice Border Gateway Remote Proxy Services with a new entry.
2. Click **Add new LAN server proxy**.
3. In the screen that appears, there is the question: “**What kind of LAN server are you configuring?**” Select **MiCollab**.
4. Answer the question, “**Which user interfaces would you like to enable access to?**”. Select **MiCollab Client**, and also **Deployment Unit**.
5. In the **WAN Side FQDN**, enter the FQDN that resolves to the MiCollab Client Service IP address.
6. Do not select the option **Do you wish to permit remote administration access?**
7. Select the top **Enabled** check box.



Note: MiVoice Border Gateway **Remote Proxy Services** programming is not auto-shared across the MiVoice Border Gateway cluster, so this programming must be duplicated on other MiVoice Border Gateway Cluster members to maintain high availability of the connections.

Program the **Alias** entries in the External DNS server for each MiVoice Border Gateway WAN IP address that serves as an MiVoice Border Gateway Web Proxy.

8. Test external connectivity to MiCollab Client to verify that the web proxy setup in the user MiVoice Border Gateway is working correctly.



Note: MiCollab Client connections connect through the SIP MiVoice Border Gateway cluster associated with the MiCollab Server the user is assigned to. This may result in a SIP MiVoice Border Gateway cluster per MiCollab Server, with a common MiVoice Border Gateway cluster for all MiNet devices.

Prerequisites

- FQDN - DNS entries are required in the Service Provider's internal DNS server. Create a DNS record for the MiCollab Client Service FQDN, mentioned above.
- DNS entries are needed in the external DNS service that will allow appropriate soft phones and MiCollab Client users to locate the correct MiVoice Border Gateway, web proxy and MiCollab Client service.
- To support the Next Gen Mobile SIP Softphone resiliency capability, the external DNS server must include special DNS entries called SRV Records, which resolve to MiVoice Border

Gateway WAN IP. Refer to the MiCollab Client Deployment documentation for this discussion.

Resources

RESOURCE

CONTENT DETAILS

<i>MiVoice Border Gateway Installation and Maintenance Guide</i>	See "Remote Proxy Services".
--	------------------------------

Configure MiVoice Border Gateway for WebRTC users

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.

1. In Mitel Standard Linux, click **Applications > MiVoice Border Gateway** in the left column.
2. In the panel that appears, click **Service Configuration > WebRTC**.
3. Select **Enabled** to enable WebRTC.
4. 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**
5. 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” on page 84.

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

-

Resources

RESOURCE

CONTENT DETAILS

*Mitel Border Gateway
Online Help*

See the topic: “Configuring WebRTC”

Configure MiCollab for mobile users

Using this new MiCollab Client Mobile deployment method, mobile users receive an e-mail with a link that allows quick and easy installation of MiCollab Client on their mobile devices.



Note: Third-party certificates are **REQUIRED** for Service Providers deploying the MiCollab Client. Individual certificates are not required for every customer connected to the Service Provider; just one certificate on each Service Provider server from which MiCollab Mobile Clients are being deployed.

1. In Oria: In **Public Facing FQDN/IP Address**, enter the FQDN of the MiVoice Border Gateway.
2. If you are configuring soft phone resiliency, 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”.



Note: The *MiCollab Client for Mobile Resiliency Guide* assumes that DNS SRV is already set up with primary and secondary hosts. This guide explains how to add DNS SRV into the MiVoice Border Gateway **Allowed URIs** field.

3. In the MiCollab Client **Deployment 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 the MiCollab Client Deployment Help, “Mobile Client Deployment Email”.

4. 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**.



Note: This branding refers only to Oria branding.

To brand other aspects of the solution (clients, for example), contact Mitel to ask about the Branding Program.

Please contact your sales representative for information about creating your branding ID and password.

5. In Oria, add the MiCollab Client users.

Prerequisites

- The base network is complete (MiVoice Business instances installed, MiCollab instances installed, MiVoice Border Gateways installed, clustered, and connected to the network.)
- The same certificate for the external MiVoice Border Gateway is also required for the MiCollab Client Server. A certificate must be installed on the MiVoice Border Gateway and MiCollab server; otherwise Teleworker mobile soft phones will not be able to log in. For detailed instructions, see the MSL Online Help; the **Manage Web Server Certificate** topic and the *MiCollab Client Deployment Guide*.
- Licenses must include the “Mobile Client w/ SIP Softphone” licenses.

MiCloud Business Multi-Instance Deployment

- The Oria Bundle include the “Next Gen Mobile SIP Softphone” Phone selection. These Oria Bundles also include the “Next Gen Mobile SIP Phone Settings” parameters.

Resources

RESOURCE	CONTENT DETAILS
Mitel Standard Linux (MSL) Online Help	See the help topic: “Manage Web Server Certificate”.
MiCollab Client Online Help	See the help topic: “About MiCollab Client Deployment”.
MiCollab Client Deployment Blade Online Help	See the following help topics: <ul style="list-style-type: none">• “Deploy Client with MiVoice Business or MiVoice Business Express”• “Run Diagnostics”
<i>MiCollab Client for Mobile Resiliency Guide</i>	Follow the instructions in “Configuration”, with the following EXCEPTION: <ul style="list-style-type: none">• IGNORE the section, “Specify FQDN of MBG Cluster”.
<i>Oria Installation and Administration Guide</i>	See the following topics: <ul style="list-style-type: none">• “DNS Resiliency ON MiCollab Client Server for Mobile Softphones (Register MBG)”• “Add a Next Gen Mobile Softphone”• “Create Brands”

Create UC Bundles in Oria

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 that include Class of Service (CoS). The Bundles created here are re-usable across multiple Customers.

Any UC features and à la carte licenses that are part of the service provider offering can be configured in the bundles.

Create Oria User Bundles to set up the feature packages for voice, Unified Communications, and voice mail 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 Oria.
2. Log in to Oria as an Administrator.
3. Create **Administrator Bundles** and **User Bundles**.
 - **Administrator Bundles** define the features available to Service Provider 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 of type **Next Gen Mobile SIP Softphone**.
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 an Administrator in the **System Tab** of Oria.
7. Create an **Operational Profile**.
8. Optional: Create **Key Templates**.
9. Create **Dialing Privileges**.
10. Create **Feature Profiles**.
11. Create **Bundles**. Possible Bundle types are:
 - Admin Bundle
 - User Bundle (Basic IPT, Standard IPT, and UCC Entry)
12. 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. Select the Customer and Edit. Assign the new Bundle to the Customer.
 - c. Select **Hotdesk Phones**. Move **PC MiNet Softphone** to the list of **Selected Devices**.
 - d. Click **Save**.
13. When creating UCC Entry Bundles, if you want to enable MiCollab MiTeam for users:
 - a. Scroll down to **MiCollab Client Service**.

b. Select MiTeam.

After they are created, Feature Bundles are available across the solution and can be applied to any customer. More bundles can be created when adding customers with Unified Communications and additional features to the solution.

Prerequisites

- At least one Feature Profile has already been created.
- UCC licenses must be available and added to the ULM first: UCC Entry.

Resources

RESOURCE	CONTENT DETAILS
<i>Oria Installation and Administration Guide</i>	Create and configure an Oria bundle. <ul style="list-style-type: none">• “Create bundles”
<i>MiCollab Client Administrator Guide</i>	See “MiTeam Integration”.
<i>MiTeam for MiCloud Business Multi-Instance Reference Guide</i>	

Create a UC-capable test Platform Group in Oria

Identify all of the topology components required for providing light UC and SIP services in a virtual Oria group for testing. A UC-capable Platform Group includes a customer's enterprise name, in addition to the MiVoice Businesses, MiVoice Border Gateway, and the MiCollab Client tenant.

This test Platform Group is deleted after deploying and validating the applications.

Register Platforms in Oria:

1. On the **Platforms** tab in Oria, register all MiVoice Border Gateway servers with Oria, using the **MiVoice Border Gateways** form.



Note: The concept of Cluster Zones applies to the 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 Oria mbgZones.xml file.

See the *Oria Installation and Configuration Guide* for Oria Release 5.0 for detailed instructions.

2. The Oria **Platform Group Type** is **MiVoice Business**.
3. In the **Type** field in the new **Platform Group**, enter the IP Address or FQDN of the Primary MiVoice Business instance.
4. Enter the MiVoice Business authorization credentials
5. Click **Save**. The MiVoice Business Primary and Secondary call servers are now listed in the **MiVoice** tab of the new **Platform Group**.
6. Open the **MiCollab Client Tenant** tab, and enter the customer enterprise name, the FQDN of the MiCollab Client Server, and its authorization credentials.
7. In the **Sites** tab, add new Sites, and complete the selection of MiVoice Business instances and MiVoice Border Gateway clusters. This services Teleworkers and UC end-points at each location (Site), where this customer supports end-users.
8. If you will be provisioning MiCollab MiTeam users (UCC Entry Bundles), you must include the following steps in the MiCollab registration:
 - a. In the **MiCollab Client Tenant** tab, select **MiTeam Services**.
 - b. Click **Save**.



Note: This step applies to Multi-Tenant mode. When deploying MiCollab Client Multi-Tenant, you must install MiCollab Client in Co-located Mode. Do not run the Install Wizard.

To enable MiTeam on the MiCollab Client Service UI:

1. The web page of the MiCollab Client Service now displays the new customer enterprise. The display shows the Primary and Secondary MiVoice call servers.

2. For the new Enterprise, program the following general parameters, applicable to the Customer and its end-users. These parameters include:
 - Favorite URLs that point to MiCollab Web Client.
 - Default News RSS URL.
 - Welcome E-mail template.
3. Select **Configure MiCollab Client Service**, and click the **Enterprise** tab.
4. Scroll to **MiTeam Configuration Settings**.
 - a. Enable **MiTeam Configuration**.
 - b. In **Telephone Domain Configuration**, select **Custom**.
 - c. In the table that appears, enter a **Label** name (Canada, for example).
 - d. In **Number**, enter the DID number for the MiTeam service for your area. You can get this number from the Mitel Partner who is assisting with your deployment.
 - e. Click **Apply**.

MiTeam Configuration Settings

MiTeam Configuration

Primary ***** Show

Guest ***** Show

Data Center Locations US Configured Location US

Telephony Domain Configuration

None Custom

[\[Add\]](#) [\[Delete\]](#)

<input type="checkbox"/> Label	Number
<input type="checkbox"/> Canada	+14802409721

Email Notification Settings

Apply Reset

Another Oria task associates the Platform Group to a Customer and users

To configure MiTeam on the MiVoice Business System Administration Tool:

1. For the tenant MiVoice Business, open the **Direct Inward Dialing Service** form.
2. Edit the **Destination Number** for MiTeam to exactly match the number you entered in "To enable MiTeam on the MiCollab Client Service UI:" on page 89, Step 4.

Tenant029

Direct Inward Dialing Service on **Tenant029** DN to search Show form on Tenant029

Direct Inward Dialing Service Search:

Find a field named: Primary Node Id (PNI) that has a value of: Search

Add Change Delete Print... Import... Export...

<< < > >>

Direct Inward Dialing Service

DID Number	Primary Node Id (PNI)	Destination Number	DID
4802409721	929	14802409721	Star
6160294008	929	4008	Star
6160294009	929	4009	Star
6160294010	929	4010	Star

Prerequisites

- There is a full list of the components in the service provider network.
- All of the MiCloud SB component servers must have FQDN entries in the DNS server being used by Oria.

Resources

RESOURCE

Oria Installation and Administration Guide

MiTeam for MiCloud Business Multi-Instance Reference Guide

CONTENT DETAILS

- Create and save an Oria Platform Group.
- “Register Platform Groups in Oria”

Create a UC-capable test customer and test end-users in Oria

Create a UC-capable test customer to verify that Oria is configuring end-users and customers correctly using the Entry UCC and Standard IPT feature bundles. Assign the test Platform Group and the Entry UCC and Standard IPT feature bundles to the test customer. MiCloud Business Multi-Instance supports

- Basic IPT
- Standard IPT
- UCC Entry users
- À la carte add-on feature licenses

Add test end-users with Oria to verify that an end-user can be defined as an Entry UCC or a Standard IPT user with MiNet or SIP devices. Oria, the topology components, and the applications must be correctly installed to create UC-capable end-users. When you add a new customer user, a Welcome e-mail is sent automatically.

Test the customer and end-users for correct operation.

Customer programming includes a Key Template for UC end-point devices that includes a Multicall Key (discussed later in this guide).

Prerequisites

- MiCollab Client desk phones and soft phones require the Class of Service (COS) options below to be properly set, that is, they must match the IDs defined earlier, in “Create UC Bundles in Oria” on page 87. In the MiVoice Business instances, use the System Manager to configure the following fields and options on the **Class of Service Options** form:
 - **Group Presence Control**
 - **Group Presence Third Party Control**
 - **HCI/CTI Call Control Allowed**
 - **HCI/CTI Monitor Allowed**
 - **Display Caller ID on multicall/keylines**
 - **Voice Mail Softkey Allowed:** Make sure this is set to **No**. (If set to Yes, end-users will not be able to hang up from their voice mail box when using MiCollab Client.)

Resources

RESOURCE

CONTENT DETAILS

Oria Engineering Guidelines

Create a customer in a service provider environment.

- “New customer setup”

Synchronize MiCollab Client and MiVoice Business

There are two types of synchronization between MiCollab Client and MiVoice Business:

- Automatic: 24-hour cycle to synchronize between MiCollab Client and MiVoice Business.
- Manual: Select MiVoice Business system in Synchronization tab and click **Sync**.

In the case where the Administrator imports users into Oria (**Import Users**), Oria automatically executes a PBX sync immediately. After that, the automatic 24-hour synchronization takes over.

A manual real-time PBX sync is required after Oria updates of the following on the MiVoice Business controller:

- Addition or deletion of soft phones in a user account
- Addition or change of a hand-off FAC
- Addition or deletion of a ring or hunt group on the MiVoice Business
- Addition or deletion of a member of a ring or hunt group on the MiVoice Business

To complete the MiCollab provisioning of the new end-users, log in to the MiCollab Server Manager, and navigate to the MiCollab Client panel. Open the new Enterprise. In the **ICPs** tab, perform a manual Sync of MiVoice Business instances.

Inspect the MiCollab Client Enterprise accounts to see that the phones are listed. The account phones listed there will vary, depending upon the UCC v4 Licenses contained in the Oria Bundle assigned to each account.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
MiCollab Online Help	Enter and synchronize end-users. <ul style="list-style-type: none"> • “Enter User Information” • “Synchronization Tab”
MiCollab Client Online Help	Synchronize end-users: <ul style="list-style-type: none"> • “Synchronization Tab”

Register UC devices and test MiCollab Client

Register UC devices and test MiCollab Client to validate the deployment of the application server and MiVoice Border Gateway Virtual proxies to the MiCollab Client. Use PC soft phones, internal phones, and mobile phones to test a variety of situations for calls using UC applications.

This is the fifth test connection being made during the MiCloud deployment.

For device registration, the MiCollab Client proxy must be set up in the MiVoice Border Gateway web proxy.

For MiCollab Client application access, the MiVoice Border Gateway **Application Integration** connector must enable MiCollab Client access:

1. Register the Basic IPT phone that created in Oria. If the phone has a profile on the RCS Server, boot the phone from Factory Defaults.
2. In Oria, perform a manual Sync. Navigate to **Advanced > Synchronize Platforms**.
3. On the end-user PC, download the MiCollab Client application by browsing to:
<https://<uca-server FQDN>/ucs/dl/UnifiedCommunicatorAdvanced.msi>
4. Install and run the application.
5. Log in to a MiCollab account using the end-user credentials created earlier through Oria, and sent to the User in the Welcome e-mail.

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Deploy Open Integration Gateway Virtual (OIG Virtual)

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



Note: Oria does not manage OIG instances, so OIG instances do not need to be registered with Oria. OIG must be managed separately.

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

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. The OIG then automatically finds the Call Server IP address.

This allows end-users a simpler configuration because only the end-user DN is required.

3. Optional: Connect to MiContact Center Business for use with Salesforce. See the *MiContact Center Business 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.
- OIG licensing has been purchased for OIG and for the MiVoice Integrations.

Resources

RESOURCE	CONTENT DETAILS
<i>Virtual Appliance Deployment Solutions Guide</i>	See "Deploying Mitel OVAs".
<i>Open Integration Gateway (OIG) Installation and Maintenance Guide</i>	Install an OIG as a virtual appliance. <ul style="list-style-type: none"> • "Install virtual Mitel OIG software" Add MiContact Center to OIG network elements. See "Network Elements Tab".

Configure Open Integration Gateway Virtual proxy services

Configure OIG Virtual proxy services to create the proxy services on the MiVoice Border Gateway Virtual instances that allow external connections to the OIG Virtual instances.

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

1. Program MiVoice Border Gateway Remote Proxy Services with a new entry.
2. Click **Add new LAN server proxy**.
3. In the screen that appears, there is the question: “**What kind of LAN server are you configuring?**” Select **Open Integration Gateway**.
4. In the **WAN Side FQDN**, enter the FQDN that resolves to the Open Integration Gateway IP address.
5. Do not select the option **Do you wish to permit remote administration access?**
6. Select the top **Enabled** check box.



Note: MiVoice Border Gateway **Remote Proxy Services** programming is not auto-shared across the MiVoice Border Gateway cluster, so this programming must be duplicated on other MiVoice Border Gateway Cluster members to maintain High Availability connections.

Program the **Alias** entries in the External DNS server for each MiVoice Border Gateway WAN IP address that serves as an MiVoice Border Gateway Web Proxy.

Test external connectivity to the OIG to verify that the web proxy setup in the user MiVoice Border Gateway is working correctly.

Prerequisites

- Internal DNS and potentially external DNS servers are in place and operational.

Resources

RESOURCE

CONTENT DETAILS

MiVoice Border Gateway Installation and Maintenance Guide

Configure the MiVoice Border Gateway to support external traffic into the service provider’s network to the OIG.

- “Server-Gateway Configuration on Network Edge”

Test Open Integration Gateway configuration

Test the OIG configuration to validate that the OIG and MiVoice Border Gateway Virtual MiVoice Border Gateway configurations are correct and that they allow for end-users to access applications that are interacting with MiVoice Business. OIG may be installed in physical or virtual form.

This is the sixth test connection being made during the MiCloud deployment.

The OIG deployment can be tested with custom applications or with Mitel applications, such as MiVoice Integration for Google or MiVoice Integration for Salesforce.

Prerequisites

- Licenses have been obtained for MiVoice Integrations.
- A Google Mail (GMail) account is available MiVoice Integration for Google.
- Active Salesforce administration and user accounts are required for MiVoice Integration for Salesforce.

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Integration for Salesforce Administration Guide</i>	Install and set up the MiVoice Integration for Salesforce.
<i>MiVoice Integration for Salesforce User Guide</i>	How to use the MiVoice Integration for Salesforce.
<i>MiVoice Integration for Google Administration Guide</i>	Install and setup the MiVoice Integration for Google and import users.
<i>MiVoice Integration for Google Quick Reference Guide</i>	How to install the Google Extension and use the MiVoice Integration for Google user interface.

Install MiContact Center Business and MiVoice Call Recording

Deploy the MiContact Center in multi-tenant mode and MiVoice Call Recording. Add call analytics (MiVoice Business Reporter or MiCloud Business Analytics), if required.

MiCloud Contact Center uses a site-based security model to isolate customer data. In a multi-tenant deployment, each site in the Enterprise represents a “tenant”. Supervisors see only configuration data specific to their site when they log in to any of the MiContact Center Business applications to run reports—Contact Center Client and CCMWeb.



Note: The SB topology provides a multi-tenant voice-only contact center; multi-media features are not available.

The system automatically filters data based on the user’s site association, such that agents, supervisors, and administrators have no view of data or devices outside their sites. Only supervisors can run reports, and only on devices associated with their own site. Similarly, when creating groups, only those users belonging to the specific site are available for membership.

Limitations and restrictions

This is a partial list; for the full list, see the *MiContact Center Site-Based Security (Multi-tenant) Administration Guide*.

- Each tenant/customer can have exactly one site. Multiple sites per tenant are not supported.
- Sites cannot be backed up individually. Backup and restore are system-wide operations. There is a single backup containing all tenant sites.
- Employee names must be unique across the entire system. It is recommended to use user e-mail addresses to provide a unique user name for each user.
- The Enterprise Server time zone is applied to all sites, regardless of their location.
- The multi-tenant deployment of MiContact Center Business does not support Oria integration for agent and supervisor provisioning and must be provisioned manually. Agents on the MiVoice Business must be provisioned via Oria, and then synchronized to MiContact Center Business.

Deploy the OVAs in the following order:

1. If you will be offering call recording, deploy an additional MiVoice Border Gateway, configured in Secure Recording Connector (SRC) mode.
2. Deploy the MiVoice Call Recording OVA.
 - a. Connect MiVoice Call Recording to MiVoice Business (MiTAI connection).
 - b. Connect and configure MiVoice Call Recording to MiVoice Border Gateway (Secure Recording Connector).
 - c. On the MiVoice Border Gateway, accept the MiVoice Call Recording certificate.
 - d. Provision users and extensions.

3. Deploy MiContact Center Business using the MiContact Center Setup wizard, following the steps in the *MiContact Center Installation and Administration Guide* and the *MiContact Center Site-Based Security (Multi-tenant) Administration Guide*.
 - In the **Enable Features** page, enable **Site Based Security**.
 - Install the exported third-party certificate created in “Deploy MiVoice Border Gateway clusters for end-user MiNet devices” on page 47 to the MiContact Center Business server.



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. Follow the instructions in the *MiContact Center Site-Based Security (Multi-tenant) Administration Guide*; the section called “Configuring the Multi-tenant System”.
 - a. Create a site for each tenant.
 - b. Select the first site and click **Manage this Site** (in the **Tools** ribbon) and add at least one media server.
 - c. Create security roles for Service Provider administrators, supervisors, agents, and local administrators.
 - d. Add the first employee and assign the security role created for local administration. This will be the Local Admin for the site/tenant.
5. Configure MiContact Center Business to point to MiVoice Call Recording, if MiVoice Call Recording is being used.
6. If you are also providing integration with Salesforce, see “Deploy Open Integration Gateway Virtual (OIG Virtual)” on page 95.

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, and ARIDs must be in place in the Mitel AMC.

Resources

RESOURCE	CONTENT DETAILS
<i>Virtual Appliance Deployment Solutions Guide</i>	Covers OVA deployment procedures, general rules for deploying Mitel virtual appliances, plus capacity, performance, and resource requirements for individual virtual appliances. This guide is available on Mitel OnLine: http://edocs.mitel.com/TechDocs/Solutions-Guides/BP-Virtualization.pdf
VMware documentation	https://www.vmware.com/support/pubs/
<i>MiVoice Call Recording Installation and Configuration Guide</i>	

RESOURCE	CONTENT DETAILS
<i>MiVoice Business Integration Guide (9.1)</i>	Describes how to connect SIP Trunks via MiVoice Border Gateway Secure Recording Connector.
<i>MiVoice Call Recording Administration Guide</i>	
<i>MiContact Center Installation and Administration Guide</i>	Use the instructions in the following sections: <ul style="list-style-type: none">• how to download and install (MiContact Center Business Setup wizard)• how to register and set up MiContact Center Business on the Enterprise Server and client computers• how to install and configure MiContact Center Business at remote sites• how to install and deploy MiVoice Call Recording
<i>MiContact Center Site-Based Security (Multi-tenant) Administration Guide</i>	Set up Multi-tenant contact center.

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 *Business Reporter Installation Guide*.



Note: While MiContact Center supports multi-tenant deployment, a separate Business Reporter must be installed for each MiContact Center tenant.

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.

Resources

RESOURCE	CONTENT DETAILS
<i>Business Reporter Installation Guide</i>	See “Enterprise Server installation”.
<i>MiCloud Business Analytics Provisioning and Ordering Process</i>	MiCloud Business Analytics guides for installation and provisioning.
<i>MiCloud Business Analytics User Guide</i>	
<i>MiCloud Business Analytics Reports Catalogue</i>	

Delete the test set-up

Most of this step is optional, and you may choose to keep most of the test set-up as an ongoing staging or sandbox area. Items that must be removed/deleted at this stage are the following:

- Any devices added from MiVoice Business must be deleted; that is, any devices not added from Oria.

Remove the test customer

Remove the customer and Platform Group association from Oria and return the resources used for testing. Deleting the customer also deletes all the end-users configured for the customer.

Removing the customer does not delete the Entry UCC and Standard IPT licenses that were used.

The test devices are deleted from the MiVoice Business instances, but the MiVoice Business instances themselves still exist in the MiVoice Business Multi-Instance server. You can log in to the MiVoice Business System Administration tool to confirm—using the **User and Device Configuration** form—that the test sets have been removed by Oria. You may then also use MiVoice Business Multi-Instance Server-Manager to delete the test MiVoice Business instances. Remember to clear hardware IDs in the ARIDs in the AMC.

The test devices are deleted from the MiVoice Border Gateway servers, but the 3300 ICP list entries still exist in the MiVoice Border Gateway. You can log in to the MiVoice Border Gateway Server-Manager tool to confirm that the test devices have been removed by Oria. You may then also use the MiVoice Border Gateway Server-Manager to delete the test ICP entries from the ICPs list.

The test accounts are deleted from the MiCollab Client Server, as well as from the test 3300 ICP controllers, and enterprises are cleared from MiCollab.

Remove the test Platform Group

Delete the test Platform Group to remove the virtual association of the topology components, making them available for other Customers.

Removing the test Platform Group does not remove the Entry UCC or Standard IPT feature bundles that were added.

Remove the test OIG Virtual

Remove the OIG Virtual resource and any applications.

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 the MiVoice Integration for Salesforce plug-in.



Tip: Maintaining the test customer, test Platform Group, and test OIG Virtual creates a sandbox environment for customer demonstrations and trials. Remember that the sandbox environment consumes resources and licenses.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

Oria Online Help

In Oria, select **Platforms > Platform Groups**. Select the Platform Group and click the trash icon to delete it.

Chapter 9

(OPTIONAL) CRM INTEGRATIONS

DEPLOYMENT

Deploy Customer Relationship Management (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
- MiCloud CRM Integrations

Prerequisites

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

CRM deployment task flow

Follow the instructions for either:

- “Deploy MiVoice Integration for Google, MiVoice Integration for Salesforce” on page 108
- OR
- “Deploy MiCloud CRM Integrations” on page 110

Deploy MiVoice Integration for Google, MiVoice Integration for Salesforce

Deploy Mitel Open Integration Gateway with MiVoice Integrations.

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 “Optional: Provision users for MiVoice Integrations” on page 149.
4. Configure the MiVoice Integration using the applicable guides:
 - MiVoice Integration for Salesforce:
 - *MiVoice Integration for Salesforce Administration Guide*
 - *MiVoice Integration for Salesforce User Guide*
 - MiVoice Integration for Google
 - *MiVoice Integration for Google Administration Guide*
 - *MiVoice Integration for Google Quick Reference Guide*

Prerequisite

- 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.

Resources

RESOURCE

*Virtual Appliance
Deployment Solutions
Guide*

CONTENT DETAILS

See “Deploying Mitel virtual appliances in VMware”.

RESOURCE	CONTENT DETAILS
Mitel product-specific documentation, including Installation Guides and Engineering Guides	Mitel OnLine: http://portal.mitel.com/wps/myportal/MOLHome Note: Login credentials are required for access to Mitel OnLine.
VMware documentation	https://www.vmware.com/support/pubs/
<i>Mitel OIG Installation and Maintenance Guide</i>	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”.
<i>Mitel OIG Engineering Guidelines</i>	For requirements and capacity.
<i>MiVoice Integration for Google Administration Guide</i> <i>MiVoice Integration for Google Quick Reference Guide</i>	For instructions for installing and configuring MiVoice Integration for Google.
<i>MiVoice Integration for Salesforce Administration Guide</i>	For installing and configuring MiVoice Integration for Salesforce with OIG and MiContact Center Business.

Deploy MiCloud CRM Integrations

Complete deployment instructions are contained in the *MiCloud CRM Integrations Administration Guide*.

The high level steps are:

1. In MiVoice Business System Administration Tool, set up sharing between MiVoice Border Gateway, Open Integration Gateway, and MiVoice Business.
2. If there is a Reseller or Partner who will be working with Customers and their users: create the Reseller/Partner administrator account in the MiCloud CRM Integrations Administrator Portal.
3. Either the Service Provider or the Reseller/Partner sets up the Customer:
 - a. Perform a Customer site survey for the following information:
 - CRM type and log in credentials
 - List of CRM users' user IDs and DNs (phone extensions)
 - b. Create the Customer account in the MiCloud CRM Integrations Admin Portal.
 - c. Connect the Customer MiCloud CRM Integrations account to the Customer CRM.
 - d. Create all of the Customer's CRM users in the MiCloud CRM Integrations Admin Portal.
 - e. Train Customer's CRM users and provide the *MiCloud CRM Integrations User Guide*.

Prerequisites

- The MiCloud CRM Integrations license has been purchased and activated by Mitel (PN 51305714). Mitel has set up an administrator account in the MiCloud CRM Integrations Admin Portal.
- Open Integration Gateway (OIG) is purchased. Each OIG is licensed with the Subscription/CapEx Base Kit, with an added Advanced Control Server license if you need to support ACD Agent Monitoring. One OIG is required for each customer. See the *MiCloud CRM Integrations Administration Guide* for details, including part numbers.
- Oria, MiVoice Business, and MiVoice Border Gateway are installed and operational.
- The Customer has a CRM purchased and installed, and an installed user base.

Resources

RESOURCE

CONTENT DETAILS

MiVoice Business System Administration Tool Online Help	See the help topic: "Network Elements".
---	---

Open Integration Gateway Installation Guide

MiCloud CRM Integrations Administration Guide

RESOURCE

CONTENT DETAILS

*MiCloud CRM Integrations
User Guide*

Chapter 10

SERVICE PROVIDER OFFER

DEFINITION

Service provider offer definition

Create and configure the basic profiles and bundles used to offer services to potential Customers. Defining the service provider's offer allows the service provider to be in a "ready to deploy" state for any new customer. A pool of licenses can be purchased and configured under the service provider's account.

Prerequisites

- The Service Provider must have worked through their market offer.

Service provider offer definition task flow

This list describes the sequence of tasks that must be performed to define and deploy the service provider offer for the deployment.

- "Program Oria with service bundle definitions" on page 116
- "Purchase licenses for the service provider" on page 117

Program Oria with service bundle definitions

Program Oria with service bundle definitions to create the service bundles that the service provider will sell and assign to Customers.

Create Bundles for Customer Administrators in Oria.

For MiCloud SB Bundles, in **Service Type**, select **MiVoice Business Multi-Instance**. Then in **License Type**, select one of **Basic IPT**, **Standard IPT**, or **Entry UCC**, depending on the intended use for the Bundle. Some of the Optional Features are then selected automatically.

If you will be deploying MiCollab Client to mobile phones, create a new User bundle that includes a phone with **Phone Type** set to **Next Gen Mobile SIP Softphone**.

Prerequisites

- An evaluation has been done to determine the scale of the solution, based on the services to be deployed to end-users.

Resources

RESOURCE	CONTENT DETAILS
<i>Oria Installation and Administration Guide</i>	Create and configure an Oria bundle <ul style="list-style-type: none">• "Create bundles"
Oria Online Help	In Oria, select the Bundles tab and click Show Help to display help topics for creating bundles.

Purchase licenses for the service provider

Purchase licenses for the service provider to create a pool of licenses that the service provider can apply to Customers.

Purchase orders must be completed and part numbers must be assigned to their relative license bundles, with the associated ARIDs generated for all the components and services that will be deployed to each Customer. The details of the license configurations needed are explained in “Configure AMC licensing” on page 26.

Types of MiCloud licenses:

- Basic IPT (IP Telephony)
- Standard IPT (IP Telephony)
- UCC Entry

Plus optional à la carte licenses:

- PC SIP Softphone
- Mobile SIP Softphone
- MiVoice for Skype for Business

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

*MiCloud Business for
Service Providers
Licensing Structures*

Available from the Mitel Managed Service Provider Program.

Chapter 11

CUSTOMER PREPARATION

Customer account preparation

Prepare the Customer account to start the process of adding a new Customer. Feature bundles are common across all customers, but licenses, purchase orders, and desktop client configurations are unique to each customer.

Prerequisites

- The customer requirements must be known: Number of users, number of sites, features and applications required, etc.

Customer account preparation task flow

This is the list of tasks that must be performed to create a new account for a Customer and to start the customer's deployment.

- "Enter phone MAC addresses into the Re-Direction and Configuration Server (RCS)" on page 122
- "Ship on-premise equipment to the Customer" on page 123

Enter phone MAC addresses into the Re-Direction and Configuration Server (RCS)

Enter phone MAC addresses into the RCS to enable it to recognize the Customer phones for direction to the appropriate MiVoice Border Gateway and to the UC MiVoice Border Gateway user portal (Zero-touch Provisioning).

Create a Server entry that corresponds to the public IP address of the appropriate MiVoice Border Gateway.

Create a Phone entry for each of the Teleworker Devices that includes the device MAC Address. Note that the RCS server can upgrade firmware to the Mitel phones.



Note: RCS: A public Internet accessible server that allows simple deployment of phones for OTT deployments by providing redirection information to the service provider user gateway.

Prerequisites

- Mitel MiNet phones must be running version 6.2.0.6 firmware, at minimum.
- Service provider licensing is complete.

Resources

RESOURCE

CONTENT DETAILS

*Redirection and
Configuration Service
(RCS) User Guide*

Ship on-premise equipment to the Customer

Ship equipment to the Customer to install all the phones, peripherals, and accessories on-site before attempting to cut over to the hosted solution.

Do not attach the new phones to the network, until the User programming in Oria is complete.

Prerequisites

- The Customer site requires the firewall or NAT router to be network-reachable to the Customer Access/Teleworker MiVoice Border Gateway WAN interfaces and RCS.
- The Customer site requires DHCP services (usually via the NAT router).
- The Customer site may provide access to DNS services that resolve FQDN requests to the IP address of the MiVoice Border Gateway WAN.

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Chapter 12

CUSTOMER DEPLOYMENT

Customer deployment

Create the components and accounts required to provide the hosted services to individual customers.

Prerequisites

- The Customer's DID is configured with the SIP trunk service provider.
- The Customer must have a good data connection, and the connection must be verified before the customer is added.

Customer deployment task flow

These steps list the sequence of tasks that must be performed to deploy the hosted services for a new Customer:

- "Optional: Use Oria Platform Manager to create Blueprints" on page 128
- "Deploy resilient Customer MiVoice Business instances" on page 130
- "Synchronize MiCollab/MiCollab Client/MiVoice Border Gateway with AMC" on page 131
- "Update internal DNS server with tenant MiCollab Client and MiVoice Business FQDNs" on page 132
- "Create the customer Platform Group" on page 133
- "Create a Customer" on page 134
- "Configure custom branding" on page 135
- "Deploy Open Integration Gateway" on page 136
- "Configure OIG proxy services" on page 137
- "Update SIP provider with emergency location information" on page 138

Optional: Use Oria Platform Manager to create Blueprints

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

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

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

General steps for creating new customers with Oria Platform Manager:

1. In MSL > **Oria Platform Manager**:
 - a. Register the MiVoice Business Multi Instance server.
 - b. Create MiVoice Business Multi Instance pools.
 - c. Register the Oria 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 software image files.
-  **Note:** The Platform Manager server contains reference MiVoice Business database files, in the directory /opt/dist_oria-bim-setup/reference.
- 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**.
2. Oria 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, Oria Platform Manager creates two MiVoice Business instances and clusters them.
4. In Oria, select the Blueprints to be available to Oria 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 Oria.
- All licenses must already be available in AMC.

- You must have a MiVoice Business golden database.

Resources

RESOURCE

CONTENT DETAILS

Oria Service Provider
Portal Help

Navigate to: **Set Up Customers > Register Platform Groups > Configure Blueprints.**

Deploy resilient Customer MiVoice Business instances



Note: If you are using Oria Platform Manger, the MiVoice Business instances are already created.

Deploy resilient Customer MiVoice Business instances. A minimum of two MiVoice Businesses must be created to support resiliency.

Use the MiVoice Business Multi-Instance GUI to create and license new instances, including restoring a Golden database.

If the MiVoice Business instances are clustered and have been licensed under a Group ARID, ensure that the licenses have been allocated down to each cluster member.

The MiVoice Businesses are set up as described in the Oria basic configuration guidelines on the MiVoice Business Multi Instance.

Call center without MiContact Center Business

If you are not planning to install MiContact Center Business, but you will have a small number of agents doing call center activities, you can use the ACD and Music On Hold (MOH) functionality built into MiVoice Business.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
<i>MiVoice Business Multi Instance Installation and Administration Guide</i>	Follow the procedure in “Add MiVoice Business Instances” to build all of the MiVoice business instances required to support the scale of the customer’s topology.
MiVoice Business Multi Instance Manager Administrator Online Help	To configure a MiVoice Business Instance, refer to the “MiVoice Business Instance Detail” topic. It describes all of the parameters that can be configured for the MiVoice Business instances.
<i>MiVoice Business Cluster Design and Implementation</i>	Creating a MiVoice Business cluster is a four-step process. Use the following procedures to interconnect the MiVoice Business instances: <ul style="list-style-type: none"> • “Prepare elements for clustering” • “Populate the Network Elements form” • “Create the cluster” • “Start sharing data via SDS”
<i>MiVoice Business Resiliency Guidelines</i>	See “Resilient System Elements and Interactions”.

Synchronize MiCollab/MiCollab Client/MiVoice Border Gateway with AMC

Synchronize MiCollab/MiCollab Client with AMC to pick up any à la carte licenses that have been created for the Customer's deployment.

Synchronize the Master member of each MiVoice Border Gateway cluster with the AMC to pick up any à la carte licenses that have been created for the Customer deployment.

Pick up any additional licenses on any of the platforms, such as MiContact Center Business, and so on.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
AMC Online Help	Refer to the help topic called "AMC Licensing Steps".
Mitel University	UCC Licensing Training

Update internal DNS server with tenant MiCollab Client and MiVoice Business FQDNs

Update the Service Provider internal DNS server, with MiCollab Client FQDN(s) to allow the MiVoice Border Gateway to connect to the unique MiCollab Client tenant instance for each customer.

Update the SP internal DNS Server with FQDN entries for the MiVoice Business controller Host names. Oria may use these FQDNs during creation of Platform Groups for Customers. These may also be listed in the MiVoice Border Gateway ICP list.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

Windows DNS Manager documentation and Help

Windows documentation, if using the Windows DNS Server.
Otherwise, refer to the documentation for the DNS Server being used.

Create the customer Platform Group

Create the customer's Platform Group to include all of the topology components required to provide the hosted services in Oria. The Platform Group includes a customer's enterprise name, along with the MiVoice Businesses, MiVoice Border Gateway, and MiCollab Client service required to provide the hosted UC and voice services.

Configure Platform Group before registering it in Oria.

In Oria, set up the range or list of DIDs/DDIs for the customer. Oria automatically adds Customer DIDs into MiVoice and into the MiVoice Border Gateway SIP Trunk.

If you will be provisioning MiCollab Client for mobile users for the Customer, in Oria, scroll to the **Softphone Settings** section. In the **MBG SIP Port** field, change Port 5061 to 0 (zero).

Optional: To enable the emergency call warning on SIP clients, navigate to **Platforms > Edit Platform > MiCollab Client Tenant**. Select **Enable emergency call warning**. The warnings will appear 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."

Another Oria task associates the Platform Group to a customer and end-users.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

Oria Installation and Administration Guide

Follow the instructions in the following sections:

- "Register Mitel Border Gateway"
- "Register Platform Groups in Oria"

Create a Customer

Create a voice-capable Customer. Assign the Platform Group and the Basic IPT feature bundles to the customer.

To create a new Customer in Oria:

1. Enter values for the following fields:

• Customer Address	• Phone Number
• Web ID	• Platform Group
• Dial Plans	• Key Templates
• Brand select	• Extension Length
• DID Ranges (for additional Ranges beyond those already there from the Platform Group)	• CPN Number (from Site)
• CESID Locations (Network Zone from Site)	• Time Zone

2. Select the number of Bundles and the Phone Devices.

3. Select Language.

4. If the customer will have users who will use MiCollab Client on Mac computers, on the **Service Bundles** screen, select **Enable deployment for a MAC Client when at least one bundle contains a PC SIP Softphone and MiCollab's version is 7.1 or higher.**

5. Create an Admin User and log in.

6. Assign the Admin Bundle.

Prerequisites

- Oria has been programmed with service bundle definitions that the service provider will sell and assign to Customers.

Resources

RESOURCE	CONTENT DETAILS
<i>Oria Engineering Guidelines</i>	Create a customer in a service provider environment. <ul style="list-style-type: none"> • "New customer setup"
Oria Online Help	In Oria, select Customers > View Customers and click Show Help to display help topics for creating and managing customers in Oria.

Configure custom branding

In Oria, run the brand creation wizard to create a customized brand to be assigned to one or more customers. Users will see the images and colors associated with the brand assigned to their company while logged into the portal.

Oria provides the capability to modify the color scheme and images displayed throughout the portal to match a corporate brand or other desired customized brand. Multiple brands can be created on the system, which allows different service provider customers to have different portal branding schemes assigned to them. The modifiable branding options available include:

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

Prerequisites

- The custom branding components and files have been created, and are available in the correct formats for use.

Resources

RESOURCE

CONTENT DETAILS

Oria Installation and Administration Guide

Create custom branding for individual customers.

- “Brands” to create custom branding.

Deploy Open Integration Gateway

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

Most deployments require only a single OIG instance. Larger deployments may require multiple OIGs. See the *OIG Engineering Guidelines* for guidance.

Mitel offers OIG-based applications that integrate MiVoice with Salesforce and Google. Customers using the MiVoice Integrations require additional configuration and licensing before enabling the MiVoice Integration for Google or MiVoice Integration for Salesforce.

In each MiVoice Business tenant:

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 user DN is required.

3. The OIG then automatically finds the Call Server IP address.

Prerequisites

- MiVoice Integrations are licensed (purchased from Mitel).
- MiVoice Integration for Google requires a Google Mail (GMail) account.
- MiVoice Integration for Salesforce requires active Salesforce administration and end-user accounts.

Resources

RESOURCE	CONTENT DETAILS
<i>OIG Installation and Maintenance Guide</i>	See "Installing the Mitel OIG".
<i>Virtual Appliance Deployment Solutions Guide</i>	See "Installing Mitel virtual appliances and applications".
<i>MiVoice Integration for Salesforce Administration Guide</i>	This guide describes how to install and set up the MiVoice Integration for Salesforce.
<i>MiVoice Integration for Salesforce User Guide</i>	This guide describes how to use the MiVoice Integration for Salesforce.
<i>MiVoice Integration for Google Administration Guide</i>	This guide describes how to install and set up the MiVoice Integration for Google.
<i>MiVoice Integration for Google Quick Reference Guide</i>	This guide describes how to use the MiVoice Integration for Google.

Configure OIG proxy services

Create and configure the OIG proxy services on the MiVoice Border Gateway instances to allow external connections to the customer's OIG instances.

Prerequisites

- The steps in “Configure Open Integration Gateway Virtual proxy services” on page 96 are complete.

Resources

RESOURCE

CONTENT DETAILS

*Open Integration Gateway
Installation and
Maintenance Guide*

Configure the MiVoice Border Gateway to support external traffic into the service provider's network to the OIG.

- “Server-Gateway Configuration on Network Edge”

Update SIP provider with emergency location information

Update the SIP provider with emergency location information to comply with any local legislation for emergency location services, and to allow end-user location details to be passed to responders for emergency situations.

Use the CESID information to provide the PSAP with appropriate location information for each phone/user.

Prerequisites

- A SIP Trunk provider is available that can handle emergency routing to an appropriate PSAP.

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Chapter 13

END-USER CONFIGURATION

End-user configuration

Set up the initial end-users.

Do not attach the new phones to the network until the user programming in Oria is complete

Prerequisites

- No end-user IP phones are registered prior to provisioning users in Oria, or if there are phones registered, they are removed from MiVoice Border Gateway, MiVoice Business, and MiCollab before provisioning.

End-user configuration task flow

This is the sequence of tasks that must be performed to create a new Customer's user accounts and complete the customer premise deployment.

- "Create a Customer's user administration account" on page 142
- "Bulk import end-users" on page 143
- "Administer end-users" on page 145
- "Configure groups" on page 146
- "Configure call flows and paths, and auto attendants" on page 147
- "Configure ACD functions" on page 148
- "Optional: Provision users for MiVoice Integrations" on page 149
- "Tune the deployment manually" on page 151
- "Optional: Deploy ACD phones and clients" on page 152
- "Optional: Deploy Vidyo® functionality" on page 154

Create a Customer's user administration account

On Oria, create an administration account that the service provider and Customer can use for adding, editing, and removing individual end-user accounts.

This account will provide the Customer Administrator with their own management access into the Oria portal. See the Customer Administrator Knowledge Portal.

Prerequisites

- A pre-configured bundle for administrator roles simplifies creating the administrator accounts for each customer.
- The Customer must be defined in Oria. This includes assigning a MiVoice Business Platform Group.
- User Bundles must already be created and allocated to the Customer. The Bulk Import operation refers to the User Bundle name definition when importing.

Resources

RESOURCE

CONTENT DETAILS

Oria Online Help	In Oria, select a customer in the Customers > View Customers tab and log in as the customer administrator. Select the Users tab and click Show Help to display help topics for creating and managing end-users.
Customer Administrator Knowledge Portal	

Bulk import end-users

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 Oria can program the MiVoice Border Gateway.

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

Import users using Oria

Prepare an Oria import spreadsheet:

1. Use the Oria import spreadsheet template to create a file containing the users to import. There are two ways to prepare an Oria import spreadsheet:
 - Download the Oria 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.
 - 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 for them as part of their setup. For detailed instructions, see the Oria Service Provider 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 Oria, upload the LDIF file map the LDIF attributes to Oria import spreadsheet fields.
 - d. Assign the bundles to the users.
 - e. Download the new Oria import spreadsheet and edit to remove any errors and add any phones that may be missing.
 - f. Save the file.

In the Oria Service Provider Portal:

1. In the main portal of Oria, 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 device1*234.



Note: To change existing users to ACD users, you must change the Bundle for the users. For instructions, see the Oria Service Provider Help: **Set Up Portal > Create Bundles**.

- 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.

If the end-users are already configured in MiVoice Business, they can be imported directly into Oria using bulk import methods.

Adjust MiCollab Client for mobile users

- 1. If you need to support Conference/Transfer/Hand-off for any SIP Devices, (including these Mobile SIP Soft phones), you must add a device, **Feature Key**.

In the MiVoice Business System Administration Tool, Navigate to **Keys** tab > **User and Services Configuration** panel. In the new Feature Key device, set:

- **Type = Multicall**
- Feature Key device **DN** = SIP device **DN**



Note: The new UC soft phone users display “Invalid Dynamic Status” until the nightly **Sync to PBX** occurs at the MiCollab Client server.

Prerequisites

- User Bundles must already be created and allocated to the Customer. The Bulk Import operation refers to the User Bundle name definition when importing.

Resources

RESOURCE

CONTENT DETAILS

Oria Online Help	In Oria, select a customer from the Customers > Bulk Import tab and log in as the customer administrator. Click Show Help to display help topics for bulk imports for any of the listed customers.
Oria Service Provider Portal Help	Provisioning users by importing an Active Directory LDIF file
MiCollab Client Deployment Help	See “Features Tab”.
MiVoice Business System Administration Tool Help	See: <ul style="list-style-type: none"> • “User and Services Configuration” • “Changing a User Profile”

Administer end-users

Add, edit, or remove individual end-users using the Customer's user administration account. User administration can be done by a Customer, a service provider, or reseller, depending on the negotiated service contract. One example of programming by the Customer Administrator is to configure telephone Key Templates.

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

If the Bundles include UC end-points (SIP devices or SIP soft phones), add at least one more key line: create a Key Template that adds a key with a Line Type of Multicall, and which holds a Directory Number matching the number of the device, and Ring Type of Ring.

Synchronization of MiCollab Client with MiVoice Business instances is required, and can be done in one of two ways:

- Automatic: 24-hour cycle to synchronize MiCollab Client and MiVoice Business.
- Manual. In Oria, perform a manual Sync. Navigate to **Advanced > Synchronize Platforms**.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

Oria Online Help	<p>In Oria, select a customer in the Customers > View Customers tab and log in as the customer administrator.</p> <p>Select the Users tab and click Show Help to display help topics for creating and managing end-users.</p>
------------------	---

Configure groups

Set up the Customer's call groups.

The groups that can be configured in Oria include:

- Call groups (ring, hunt, and pickup groups) and page groups

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

Oria Installation and Administration Guide

See the chapter: "Customer Creation".

Oria Online Help

Click **Show Help** for context-sensitive help.

Configure call flows and paths, and auto attendants

Configure call flows and auto attendants. Set up the interactions and menus between callers and MiVoice Business using the MiVoice Business forms via the System Administration Tool.

If Oria is not being used, these features are configured directly in MiVoice Business. See the Voice Mail, Auto Attendant, and ACD topics in the MiVoice Business System Administration Tool Help.



Note: If MiContact Center Business is not being deployed, both ACD and auto attendants use the Message Greetings functionality of Embedded Voice mail, and must be configured directly in the MiVoice Business call manager.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
<i>Oria Installation and Administration Guide</i>	See "Create and Change Bundles".
Oria Online Help	Click Show Help for context-sensitive help topics.
MiVoice Business System Administration Tool Help	See: <ul style="list-style-type: none"> • "Setting the Auto Attendant Transfer Type" • "Automatic Call Distribution" • "Voice Mail (Embedded)"

Configure ACD functions

Configure automatic call distribution functions to ensure that incoming calls are appropriately distributed and assigned for the Customer's business hours, location, and staffing.

In MiVoice Business, complete the ACD configuration. Use the forms in the MiVoice Business System Administration Tool.

When Oriá is not being used, you must do the full ACD configuration in MiVoice Business. See the ACD topics in the System Administration Tool Help.

Prerequisites

- Additional á la carte licensing is required to provision ACD operations.

Resources

RESOURCE	CONTENT DETAILS
<i>Oriá Installation and Administration Guide</i>	See "Create and Change Bundles".
MiVoice Business System Administration Tool Help	See "Automatic Call Distribution".

Optional: Provision users for MiVoice Integrations

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 (this is done in Salesforce by a Salesforce Administrator):



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

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 Extensions must be installed by each end-user.

Administrator actions:

1. Install MiVoice Integration for Google 1.1. 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; the *MiVoice Integration for Google Quick Reference Guide* contains the instructions.

User actions:

1. Each users 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 is installed. The MiVoice Integrations are purchased and licensed.

Resources

RESOURCE

CONTENT DETAILS

<i>MiVoice Integration for Salesforce Administration Guide</i>	Complete description of installation and configuration of MiVoice integration for Salesforce.
<i>MiVoice Integration for Salesforce Guide</i>	User reference for MiVoice Integration for Salesforce users and agents.
<i>MiVoice Integration for Google Administration Guide</i>	Complete description of installation and configuration of MiVoice integration for Google.
<i>MiVoice Integration for Google Quick Reference Guide</i>	User reference for MiVoice Integration for Google users.
<i>Open Integration Gateway Installation and Maintenance Guide</i>	See “Configure Mitel OIG software”.

Tune the deployment manually

The service provider tunes the deployment manually to modify the configuration to meet any unique requirements for the Customer. This may include Class of Service settings and Feature Access Codes, for example.



CAUTION: Do not override any Oria managed configurations. Overriding settings made by Oria can cause synchronization errors between the databases.

Configuration changes that apply to all customers should be managed through feature bundles and the database template, to avoid manual tuning for every new customer.

Set up MiVoice Border Gateway web proxies, if required.

1. If you are deploying MiContact Center Business web proxy, you must enable the 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 Business server.
 - Select **MiContact Center**.
2. If you are deploying MiVoice Call Recording web proxy, repeat step 1. with the following changes:
 - a. Select **MiVoice Call Recording** (in place of **MiContact Center**).
 - b. In **WAN-side FQDN**, enter the MiVoice Call Recording server FQDN.

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Optional: Deploy ACD phones and clients

Deploy phones and clients to install, connect, and activate the Customer’s devices, including desk phones and soft phones. This is done manually, one phone at a time.

The term “soft phone” is used to describe the following:

- MiCollab Client desktop client/soft phone (also called PC soft phone)
- Mobile client plus soft phone. See “Configure MiCollab for mobile users” on page 85.

Deploy ACD phones and users

1. 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 Oria can program the MiVoice Border Gateway.

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

2. In Oria, provision the phones.
 - a. Select a customer from the **Customers > View Customers** tab and log in as the customer administrator.
 - b. Add ACD desk phone users.
3. If this was a previously connected phone, reconnect the phone.

Prerequisites

- Power-over-Ethernet (PoE) devices require a network that provides both power and IP connectivity before trying to deploy the phone.
- A support plan needs to be in place for end-users that face challenges with deploying or using their new phones and clients.
- If Teleworkers have been provisioned through RCS, there is no work required. If not, users must manually configure their IP phone for Teleworker mode.

Resources

RESOURCE	CONTENT DETAILS
Oria Online Help	In Oria, select a customer from the Customers > View Customers tab and log in as the customer administrator. Select the Users tab and click Show Help to display help topics for creating and managing end-users.
MiVoice Business System Administration Tool Online Help	See the following help topics: <ul style="list-style-type: none"> • “Adding Users and Services” • “ACD Agent Hotdesking - Programming” • “User and Services Configuration form”
MiCollab Users and Services Help	See “View User Directory”.

RESOURCE

CONTENT DETAILS

<i>IP DECT Base Station and Installation and Operation Guide</i>	This document describes the processes for deploying IP DECT systems.
Installation guides for end-user devices	The installation documentation for all Mitel end-user devices is found here: http://edocs.mitel.com/Installation%20Guides/index.html .
Phone set documentation	See the Mitel User Documentation page for the phone set documentation.

Optional: Deploy Vidyo® functionality

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.

Contact Mitel Cloud Services for Vidyo licensing and installation.

Prerequisites

- Vidyo licenses have been purchased, and Vidyo authentication credentials are known.

Instruct end-users in connecting to Vidyo services

Vidyo® is a cloud-based video chat service. Each end-user must download and install the Vidyo client.

To connect to the Vidyo service:

1. Install Vidyo desktop client, **VidyoDesktop**.
2. Log in to the Vidyo client with your Vidyo credentials.

Resources

RESOURCE

CONTENT DETAILS

MiCollab Vidyo User Quick Reference Guide <https://selfservice.vidyo.com/eService/OnlineDocumentation.aspx>
MiCollab Vidyo Administrator Quick Reference Guide

Chapter 14

MICONTACT CENTER BUSINESS

DEPLOYMENT

Install and provision MiContact Center Business

Install, provision, and configure MiContact Center Business.

Prerequisites

- End-users have been added in Oria.
- The network infrastructure is set up and a server is available for MiContact Center Business.
- MiContact Center Business licenses have been purchased.

MiContact Center Business configuration task flow

The following tasks are described in this chapter:

- “Install MiContact Center Business and configure with MiVoice Business” on page 158
- “Administer agents in Oria” on page 159
- “Adjust configuration on MiVoice Business” on page 160
- “Synchronize users with MiContact Center Business” on page 161
- “Tune the deployment in MiVoice Business, MiCollab, and MiVoice Border Gateway (SaaS or Reseller)” on page 163
- “Deploy phones and clients (Reseller)” on page 164

Install MiContact Center Business and configure with MiVoice Business

Install MiContact Center Business into the network. See the *MiContact Center Installation Administration Guide* for instructions. Connect it to MiVoice Business (see MiContact Center Knowledge Base <http://micc.mitel.com/kb>. “Golden Rules for configuring PBX options”).

On the MiVoice Business, adjust the parameters for overflow timers, RAD, and Interflow settings and configure embedded MOH programming. See the MiVoice Business System Administrator Tool Help for details.

If the IVR ports are not pre-configured in the MiVoice Business “Golden database”, you must set them up when you are setting up the MiContact Center Business. The IVR connects to MiVoice Business using trusted 5020 ports. These ports are not licensed. There are two supported options for configuring the 5020 ports:

- The recommended process is to create a Golden database containing an over-provisioned range of IVR ports. The MiContact Center Business administrator can provision within that range and can be assured that the port exists on the MiVoice Business.
- Provision the IVR ports on the MiVoice Business. Synchronize to MiContact Center Business. Following the Sync, the administrator can select which ports to use for IVR and which ports to exclude.



Note: Other applications also use trusted 5020 ports, for example MiCollab Unified Messaging.

Service providers must have an external process to ensure the alignment of ports to applications.

If you will be provisioning remote supervisors:

The MBG Connector must be enabled. On the existing MiNet user MiVoice Border Gateways (or if creating new MiVoice Border Gateways):

1. Navigate to the **Service Configuration** tab > **Applications Integration**, select **MiContact Center connector enabled**.
2. In **MiContact Center Service hostname or IP address**, enter the FQDN of the MiContact Center Business server.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

MiContact Center Installation Guide

See “Installation Overview”.

MiContact Center Knowledge Base, <http://micc.mitel.com/kb>

Search for “Golden Rules for configuring PBX options”, and download the attached Excel spreadsheet.

Administer agents in Oria

In Oria, 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 custom Oria Customer Portal to add, provision, and delete the following. If Oria is not being used, these must be provisioned in the MiVoice Business System Administration Tool.

- 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

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Adjust configuration on MiVoice Business

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 groups are programmed in the Oria Administration Portal for each customer, while detailed programming of the ACD functions are performed on the MiVoice Business controller using the System Administration Tool forms.

ACD agents are programmed as Hot Desk agents in the MiVoice Business System Administration Tool.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

MiVoice Business System Administration Tool Online Help	See the following help topics: <ul style="list-style-type: none">• "ACD Overview"• "ACD Planning"• "ACD Terminology"• "ACD Programming"• "ACD Agent Hot Desking - Programming"
MiVoice Business System Administration Tool Forms	Programming is done on the following forms: <ul style="list-style-type: none">• ACD Agent Skill Groups• ACD Paths

Synchronize users with MiContact Center Business

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

By default, MiContact Center Business synchronizes the full MiContact Center Business server with all MiVoice Business Instances. To configure MiContact Center Business, perform a manual Sync, and set it to synchronize one MiContact Center tenant and one MiVoice Business instance at a time.

To synchronize contacts with MiVoice Business network:

For detailed instructions and other information, see the *MiContact Center Installation and Administration Guide*.

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**. (The default setting is **Read/Write**, so you must change this.)



Note: There are several options for dealing with new users that exist in MiVoice Business but not in MiContact Center Business. Set the options to create new MiContact agents with voice extensions. These are the default settings.

- For multi-tenant MiContact Center Business, sites with large numbers of remote agents and sites with relatively few agents within a large general business user group, it is recommended to ignore non-required extensions to minimize the database size.
- For sites with MPLS connectivity and relatively few non-required extensions, it is recommended to use disabled extensions to simplify operations.

See the *MiContact Center Installation and Administration Guide* ("Specifying synchronization settings") for instructions.

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 cannot be synchronized automatically.

14. Repeat these steps for every tenant in the MiContact Center Business Multi-Tenant.
15. For post-Sync configuration steps, see the *MiContact Center Installation and Administration Guide*.



Note: The nightly (2:00 am) maintenance Sync of MiContact Center Business and MiVoice Business always synchronizes all tenants; you cannot Sync tenants individually. Manual Sync can be performed on individual tenants. To control which tenants and which MiVoice Business are synchronized, use manual synchronization as described above.

Prerequisites

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

Resources

RESOURCE

CONTENT DETAILS

<i>MiContact Center Installation and Administration Guide</i>	See <ul style="list-style-type: none">• “Specifying synchronization settings”• “Performing Synchronization”
---	--

Tune the deployment in MiVoice Business, MiCollab, and MiVoice Border Gateway (SaaS or Reseller)

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 Oria.

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.



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

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Deploy phones and clients (Reseller)

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

The customer needs to deploy DNS and DHCP servers, and have these programmed to the right 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 MiVoice Border Gateway 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 Oria can program the MiVoice Border Gateway.

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

For MiContact Center Business supervisors that will be working remotely:

Each supervisor 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

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Chapter 15

CUSTOMER DELETION

Customer deletion

Used when a customer is leaving the Service Provider.

Delete customers to remove all artifacts in the network related to providing hosted services for a former Customer. Accounts are removed, virtual network components are deleted, and licenses are reclaimed for future use.

Prerequisites

-

Customer deletion task flow

This list shows the sequence of tasks that must be performed to delete a Customer:

- “Delete a Customer profile” on page 168
- “Delete the customer Platform Group” on page 169
- “Delete the customer Open Integration Gateway instances” on page 170
- “Clear the Customer configuration” on page 171
- “Optional: Engage Mitel Professional Services for licensing clean up” on page 172

Delete a Customer profile

Delete a customer's profile in Oria to remove the connections between the license server, the Platform Group, and Oria for the customer.

Remove the customer and Platform Group association from Oria and return the resources used. Deleting the customer also deletes all of the end-users configured for the customer.

Removing the customer does not delete the Entry UCC and Standard IPT feature bundles that were used. They are referred back to the DLM.

Oria does not destroy the MiVoice Business instances; only the user and device programming is removed. The Service Provider can later manually delete MiVoice Business instances through the MiVoice Business Multi Instance Server-Manager.

Licenses are still allocated under the ULM in the AMC, and are all still available to any new Customer MiVoice Business instances that you associate and synchronize with the same corresponding DLM/ARIDs. You must clear hardware IDs in the DLM/ARIDs in the AMC.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

*Oria Installation and
Administration Guide*

Delete the customer Platform Group

Delete the customer's Platform Group to remove the virtual association of the topology components, making them available for other Customers.

This also deletes all MiVoice Business instances and the enterprise from the MiCollab Client Service, and all customer DIDs are removed from the MiVoice Border Gateway SIP Trunks.

Removing the test Platform Group does not remove the bundles that are used by other customers.



Note: A Platform Group cannot be deleted if it contains Sites that are still being used. When an entry in a Site is in use, this means there is a Customer with Users/Devices defined, and DIDs and/or MiVoice Border Gateways programmed.

Prerequisites

-

Resources

RESOURCE

CONTENT DETAILS

*Oria Installation and
Administration Guide*

Delete the customer Open Integration Gateway instances

Delete the customer OIGs 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, 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. To delete a blade, click the **Remove** link beside it. Note that:

- Deleting the OIG 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 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 the MiVoice Integration for Salesforce plug-in.

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Clear the Customer configuration

Clear the Customer configuration to remove all the remaining customer settings that are not automatically torn down by Oria.

The following items must be removed manually:

- Private DNS server entries
- Public DNS server entries
- Customer details with SIP trunk service provider
- Web proxy settings in MiVoice Border Gateway and MiVoice Border Gateway Virtual
- MAC addresses in RCS server
- MiVoice Business instances on MiVoice Business Multi Instance. ULM licenses may be reusable, too. Remember to clear the hardware IDs in the ARIDs of the deleted MiVoice Business instances in the AMC.
- Remove MiContact Center Business.
- Remove Probes.
- If you have deployed Vidyo services, call Vidyo to remove the Customer so that you can reclaim the licenses.

After completion of all of these manual steps:

- Verify that the Customer enterprise and all end-users have been removed from the MiCollab server (MiCollab Client).
- Verify that end-user devices have been deleted from the MiVoice Business and MiVoice Border Gateway servers.

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Optional: Engage Mitel Professional Services for licensing clean up

Engage Mitel Professional Services for licensing clean up to properly reclaim any licenses, allowing reuse by the service provider. Depending on the complexity of the system, this may also be done by Service Provider staff, managing the existing licenses in the ULM.

Prerequisites

-

Resources

[RESOURCE](#)

[CONTENT DETAILS](#)

Chapter 16

MICLOUD BUSINESS UPGRADE

Upgrading MiCloud Business Multi-Instance

Use the instructions in this chapter to upgrade your MiCloud Business 3.0 or MiCloud Business 3.1 installation to MiCloud Business 3.3. This 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.



Note: The upgrade sequence in this chapter is optimized to minimize user down-time. If user down-time windows are permitted, then the order of upgrades is more flexible.



Note: This chapter assumes an upgrade from MiCloud 3.1 to MiCloud 3.3. The same sequence can be used to upgrade from MiCloud 3.0 to 3.3.

To upgrade from MiCloud Business 2.0, you can follow this same sequence if windows of down-time can be scheduled. If you must minimize down-time:

- Upgrade from MiCloud Business 2.0 to MiCloud 3.1, following the instructions in *MiCloud Business RIs 3.1 Deployment Guide*.
- Upgrade from MiCloud Business 3.0 or 3.1 using the instructions in this chapter.

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

Sections in this chapter:

- “Prerequisites” on page 175
- “Upgrade MiCloud 3.0/3.1 to MiCloud 3.3” on page 177

Prerequisites

Prepare a full backup of every system and every database in the MiCloud system.



Note: For multi-tenant applications, maintenance and upgrades affect all tenants. Backup and restore is system-wide; per-tenant backup and restore is not supported.

There are three back-up methods for virtual applications in VMware. See Table 4 for details.

Table 4: Back-up methods

BACK-UP METHOD	TIME TO PERFORM BACK-UP	DESCRIPTION/NOTES
VMware snapshot	5 mins	<p>This is a VMware feature that creates a snapshot of all states on the VM. A VMware snapshot takes a lot of memory and the system performance may suffer while the snapshot exists in the system. A VMware snapshot is convenient and easy to use when restoring the system.</p> <p>Note: Use and keep VMware snapshots for short durations only.</p>

Table 4: Back-up methods

BACK-UP METHOD	TIME TO PERFORM BACK-UP	DESCRIPTION/NOTES
VMware OVA back-up (Export Template)	60 mins	Make a local copy of the VMware virtual machine in a OVA file. To roll-back the upgrade, restore the OVA file to the virtual machine.
Application database backup	10 mins	Follow the instructions in the specific product documentation. This is the most common method used in the Mitel test lab.

Additional information to smooth the upgrades:

- MiCollab for Mobile is a simplified user application for mobile devices introduced in MiCloud 3.0. You must add a Web Server certificate to the MiCollab and MiVoice Border Gateway servers. Purchase a third-party SSL certificate and install it on the MiVoice Border Gateways on the network edge and the MiCollab Multi-tenant on the LAN. See the **Add Web Server Certificate** topic in MSL help for details.
- The AMC licensing server can be used to check for and download the latest software loads available directly to the connected components (except for MiContact Center Business, MiVoice Business Reporter, and MiVoice Call Recording).



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

Upgrade MiCloud 3.0/3.1 to MiCloud 3.3

In the upgrade from MiCloud 3.1 to MiCloud 3.3, not all of the underlying products need to be upgraded.



Note: The upgrade sequence in this chapter is optimized to minimize user down-time. If user down-time windows are permitted, then the order of upgrades is more flexible.



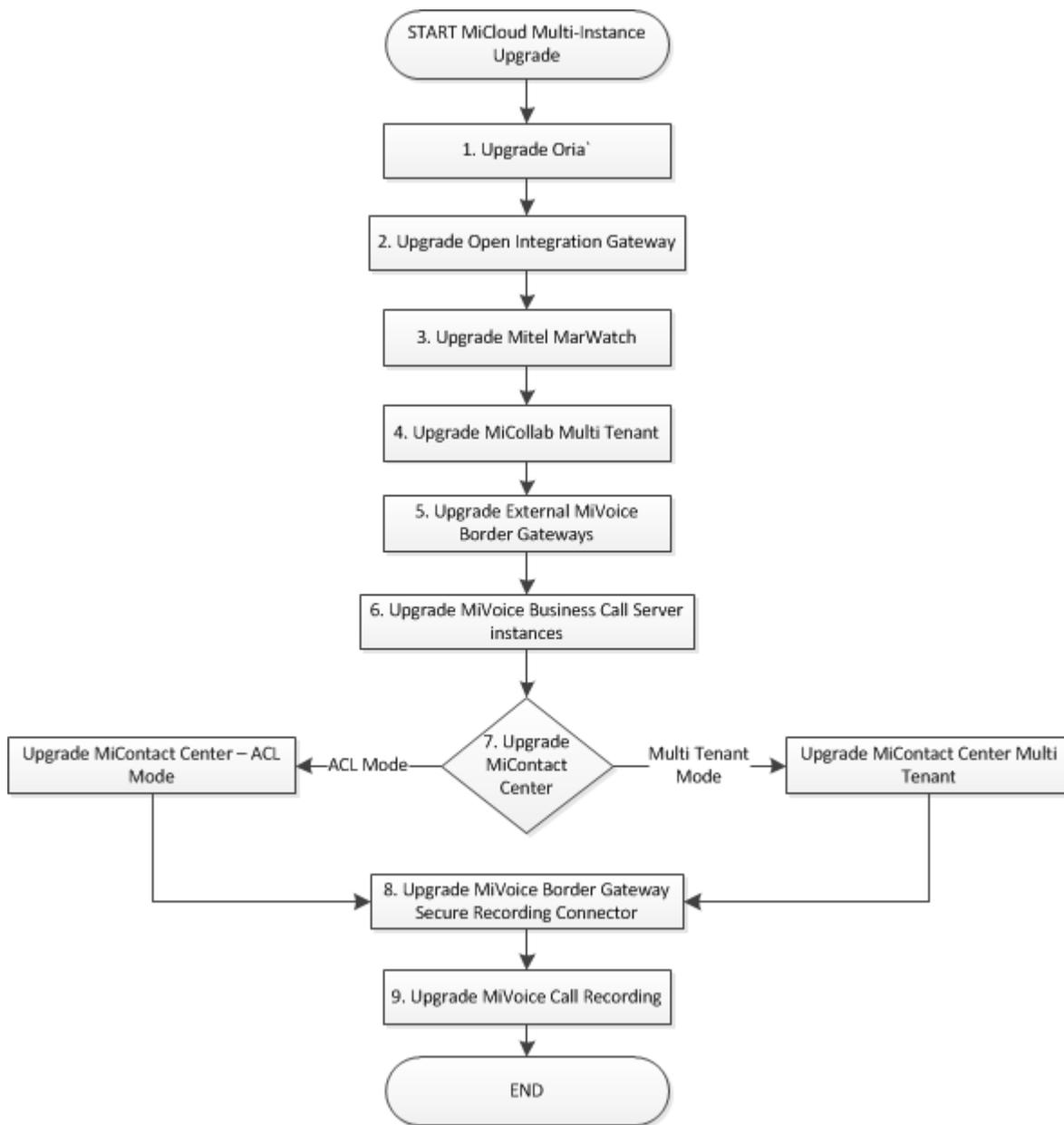
Note: This chapter assumes an upgrade from MiCloud 3.1 to MiCloud 3.3. The same sequence can be used to upgrade from MiCloud 3.0 to 3.3.

To upgrade from MiCloud Business 2.0, you can follow this same sequence if windows of down-time can be scheduled. If you must minimize down-time:

- Upgrade from MiCloud Business 2.0 to MiCloud 3.1, following the instructions in *MiCloud Business RIs 3.1 Deployment Guide*.
- Upgrade from MiCloud Business 3.0 or 3.1 using the instructions in this chapter.

See the flowchart in [Figure 3](#) for an overview of the upgrade.

Figure 3: Upgrading MiCloud Business Multi-Instance from Release 3.0/3.1 to 3.3



1. Upgrade Oria to RIs 5.3 SP1

Primary resource: *Oria Installation and Administration Guide.*

Pre-upgrade tasks: Full back-up

1. Back up the MSL.
2. Shut down Oria.
3. Back up Oria.

Oria Release 5.1 introduced Oria Platform Manager, which requires two additional servers. Both can be virtual machines.

- Oria Platform Manager
- Oria File Server



Note: Oria Platform Manager and Oria File Server can reside on the same server, if desired, depending on the projected size of the databases on the Oria File Server.

Oria Platform Manager and Oria File Server CANNOT be co-located with Oria on the same server.

Refer to the MiCloud and Oria Release Notes and the Oria documentation.

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

Table 5: Upgrade Oria

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE (HRS)	ROLL-BACK TIME (HRS)	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
					USER ¹	ADMIN ²	USER ¹	ADMIN ²
5.0/5.1	5.3 SP1	Back-up	0.5	0.5	All	None	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.

Post-upgrade tasks: None



Note: The Oria 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 Oria Services to start.

2. Upgrade Open Integration Gateway (OIG) to RIs 4.0

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



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. If MiVoice Integration for Salesforce is installed, uninstall the 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+.
 - Reboot the OIG server as instructed to install the new MSL OS.
 - In the OIG blades panel, install OIG 4.0.28+.

Table 6: Upgrade Open Integration Gateway

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE	ROLL-BACK TIME	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
			(HRS)	(HRS)	USER ¹	ADMIN ²	USER ¹	ADMIN ²
3.0	4.0		0.5	0.5	All ³ except for MiVoice Integrations	All ⁵	All ⁴ except for MiVoice Integrations	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.
3. MiVoice Integration for Salesforce: the hosted or premise-based application must be updated with a new MiVoice Integration for Salesforce package.
4. MiVoice Integration for Google will be available to users after they are also updated to the latest version.
5. All functions of MiCloud continue operating during the OIG upgrade, except for OIG and MiVoice Integrations functions.



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.
 - “Upgrade MiVoice Integration for Salesforce” on page 181
 - “Upgrade MiVoice Integration for Google” on page 182
- 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*.

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

Table 7: Upgrade MiVoice Integration for Salesforce

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE (HRS)	ROLL-BACK TIME (HRS)	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
					USER ¹	ADMIN ²	USER ¹	ADMIN ²
2.0	2.1.6	N/A	Admin: 1.0 User: 0.5	0.5	None	All	All	All

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.

Post-upgrade tasks:

- None

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

Table 8: Upgrade MiVoice Integration for Google

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE	ROLL-BACK TIME	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
			(HRS)	(HRS)	USER ¹	ADMIN ²	USER ¹	ADMIN ²
1.1	1.1.20	N/A	Admin: 0.5 User: 0.5	0.5	None	All	All	All

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.

Post-upgrade tasks:

- None

3. Upgrade MarWatch server to Mitel Performance Analytics (MPA) 5.2

Primary resource: *MarWatch (MPA) Upgrade Guide*

Pre-upgrade tasks: None

MarWatch reporting is affected by the in-progress upgrade, but Oria and similar administrative services remain available.



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

Table 9: Upgrade MarWatch server

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE	ROLL-BACK TIME	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
			(HRS)	(HRS)	USER ¹	ADMIN ²	USER ¹	ADMIN ²
5.1	MPA 2.1.	Back-up	1.0	1.0	All	All	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.

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

4. Upgrade MiCollab Multi-tenant to RIs 7.3 PR1

Primary resource: *MiCollab Installation and Maintenance Guide*



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

Pre-upgrade tasks: Full back-up

Table 10: Upgrade MiCollab Multi Tenant

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE	ROLL-BACK TIME	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
			(HRS)	(HRS)	USER ¹	ADMIN ²	USER ¹	ADMIN ²
7.1/7.2.1	7.3 PR1	Back-up	1.0	1.0	Voice only ³	None	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.
3. No Unified Communication features are available during upgrade.



Note: Flow Through Provisioning is not supported for the Multi Tenant deployment of MiCollab, so there are no upgrade requirements related to this MiCollab upgrade.

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. Teleworker sets are upgraded at the completion of both MiVoice Border Gateway and MiCollab. This happens automatically when a user unplugs the phone and plugs it back in.
4. 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 remains on their device until they delete it. It can be deleted in the same way as any other application on the device.

5. Upgrade the external MiVoice Border Gateways to RIs 9.4 PR3



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

For each external MiVoice Border Gateway (non-MiCollab MBGs):

1. Upgrade the Master MiVoice Border Gateway.
2. On the MiVoice Border Gateway, navigate to **MBG Settings > Service parameters > SSL Ciphers** and select **8.x Compatibility**. See the Release Notes for details.



Note: Although the UI will not show that the MBG Cluster link is connected, the link is up and can support IP Phone recovery.

3. After all of the MiVoice Border Gateways have been upgraded, disable the RC4 script on each MBG where it has been implemented, as applicable. See the Release Notes for details.

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

Pre-upgrade tasks: Full back-up

Note that the Clusters are upgraded independent of each other. The SIP trunk cluster is independent of the Teleworker cluster.

Table 11: Upgrade MiVoice Border Gateway

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE	ROLL-BACK TIME	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
			(HRS)	(HRS)	USER ¹	ADMIN ²	USER ¹	ADMIN ²
9.2/9.3 PR1	9.4 PR3	Back-up	0.5 each + 0.5 each re-balance time	0.5 each	All ³	All Except for user provisioning	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.
3. Non-resilient SIP devices will be out of service while their primary MiVoice Border Gateway is upgrading.

Post-upgrade tasks:

1. Install a third-party 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 MiVoice Border Gateway clusters for end-user MiNet devices” on page 47.

6. Upgrade the MiVoice Business instances to RIs 8.0 PR3

Primary resource: *MiVoice Business Multi Instance Installation and Administration Guide*

Pre-upgrade tasks: Full back-up



Note: Upgrade secondary controllers before upgrading primary controllers.

Table 12: Upgrade MiVoice Business instances

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE	ROLL-BACK TIME	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
			(HRS)	(HRS)	USER ¹	ADMIN ²	USER ¹	ADMIN ²
7.2 SP1	8.0 PR3	Back-up Fail-over to another MiVoice Business instance	1.0 per tenant Duration is also affected by number of users	1.0 per tenant	All	All ³	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.
3. While the Secondary MiVoice Business is being upgraded (do this before the Primary), the Primary MiVoice Business is still available for Management access. Later, when the Primary is being upgraded, it is good practice not to make any changes on the Secondary MiVoice Business, which will be available at that point.

Post-upgrade tasks:

1. Install a third-party certificate on each MiVoice Business. Export the certificate for install on each application in the system.
2. 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.
 - a. Select **Service Configuration > Minet devices**.
 - b. Click **Bulk Edit**.
 - c. Click **Reset**.
3. The GARID is not restored after upgrade to MiVoice Business 7.2, so you must manually synchronize the Application group DLM License (GARID) from all MiVoice Business controllers after upgrade. (Upgrading from MiVoice Business 7.2 and above will restore the DLM correctly).

7. Upgrade MiContact Center Business to RIs 8.1 SP2

Primary resources:

- *MiContact Center Installation and Administration Guide*
- *MiContact Center Site-Based Security (Multi-tenant) 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 Business Multi Tenant, follow the instructions in the guides.
- If you are currently managing multiple tenants using Access Control Lists (ACL):
 - For customers using MiContact Center Call Costing module, MiContact Center will continue to be used in single tenant mode using ACL for tenant segregation.
 - After upgrade, re-create the tenants in the new MiContact Center Multi Tenant deployment. Contact Mitel Support for details. There is no upgrade path from the ACL deployment to MiContact Center Multi-tenant.

Pre-upgrade tasks: Full back-up

Table 13: Upgrade MiContact Center Business

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE (HRS)	ROLL-BACK TIME (HRS)	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
					USER ¹	ADMIN ²	USER ¹	ADMIN ²
8.0	8.1 SP2	Back up			All UC, but no contact center features	All UC, except for MiContact Center Business admin	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.

Post-upgrade tasks:

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

8. Upgrade MiVoice Border Gateway Secure Recording Connector to RIs 9.4 PR3

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

Table 14: Upgrade MiVoice Border Gateway Secure Recording Connectors

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE (HRS)	ROLL-BACK TIME (HRS)	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
					USER ¹	ADMIN ²	USER ¹	ADMIN ²
9.2/9.3	9.4 PR2	Back-up	0.5 each	0.5 each	All	All	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.

Post-upgrade tasks: Users must upgrade desktop clients.

9. Upgrade MiVoice Call Recording to 9.1 SP1

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

Table 15: Upgrade MiVoice Call Recording

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE (HRS)	ROLL-BACK TIME (HRS)	SERVICES AVAILABLE DURING UPGRADE		SERVICES AVAILABLE AFTER UPGRADE	
					USER ¹	ADMIN ²	USER ¹	ADMIN ²
9.0 SP3	9.1 SP1	Back-up			All except for call recording	All except for MiVoice Call Recording admin	All	All

Notes:

1. User: End-user services; making a voice call, for example.
2. Admin: Management services; provisioning new users, for example.

Post-upgrade tasks: None

Appendix A

GLOSSARY OF ACRONYMS

Glossary of acronyms

ACRONYM	TERM
ACD	Automatic Call Distribution - Enables calls to be evenly distributed among contact center agents, for a cost-effective use of pooled resources and improved customer service. It ensures the equal distribution of incoming calls to the most appropriate group of agents based on the type of information or service required by the caller.
AMC	Applications Management Center - Mitel's licensing center
ARD	Alternative Recording Device
ARID	Application Record ID
ARS	Automatic Route Selection
controller	A MiVoice Business platform, whether it is hosted on a 3300 ICP, an industry standard server, or a VMware virtual machine. Also called a controller, or a node or network element.
CoR	Class of Restriction
CoS	Class of Service
CPH	Calls per Hour - Call volume statistic
CPN	Called Party Number
CRE	Call Recording Equipment
CTI	Computer Telephony Integration
DHCP	Dynamic Host Configuration Protocol is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
DID/DDI	Direct Inward Dial
DLM	Designated License Manager
DNS	Domain Name Server
DNS SRV	The DNS SRV record points to a server for Session Initiation Protocol (SIP) protocol services.
DPM	VMware Distributed Power Management
DRS	VMware Distributed Resource Scheduler
E911	Enhanced 911 - In the United States, E911 (Enhanced 911) is support for wireless phone users who dial 911, the standard number for requesting help in an emergency. Since wireless users are often mobile, some sort of enhancement is needed to 911 service that allows the location of the user to be known to the call receiver.
EMEM	MiVoice Business Embedded Messaging
ESXi (ESX)	VMware ESXi (formerly ESX) is an enterprise-class, type-1 Hypervisor developed by VMware for deploying and serving virtual computers.
FQDN	Fully Qualified Domain Name

MiCloud Business Multi-Instance Deployment

ACRONYM	TERM
GARID	Group Applications Record ID Group ARID Examples: Both ULM and DLM are types of GARID.
Golden database	MiVoice Business Multi-instance supports the use of a “golden database”, an initially created database that can subsequently be distributed across all instances of the MiVoice Business software.
ICP	Mitel IP Communications Platform
ICMP	Internet Control Message Protocol - One of the main protocols of the Internet Protocol Suite; used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
IP	Internet Protocol
IPT	IP Telephony
IaaS	Infrastructure as a Service - Refers to on-line services that abstract the user from the detail of infrastructure like physical computing resources, location, data partitioning, scaling, security, and backup.
ISS	Industry Standard Server - In addition to running on the MX, CX, and LX controllers, MiVoice Business is also supported on industry standard servers, and on VMware virtual machines (MiVoice Business Virtual).
IVR IVR Routing	Interactive Voice Response - A technology that enables callers to interact with a contact center's phone system by pressing keys or using speech recognition while following IVR dialog instructions.
LAN	Local Area Network
MAC	Media Access Control address (MAC address) - Also called physical address. A unique identifier assigned to network interfaces for communications on the physical network segment.
MAN	Metropolitan Area Network
MBG	MiVoice Border Gateway
MIB	SNMP Management Information Base
MLB	Medium-Large Business - One of the MiCloud architectures.
MMG	MiCloud Management Gateway - A Mitel product (delivered as an OVA) used to set up connectivity between the SaaS provider and multiple customer networks.
MPLS	Multi protocol Label Switching - A mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.
MSL	Mitel Standard Linux - Mitel custom implementation of CentOS Linux.
NAT	Network Address Translation - A method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
OIG vOIG	Open Integration Gateway - an open, standards-based web services platform that enables application development and integration with Mitel products. Open Integration Gateway Virtual - For deployment in virtualized environments.

ACRONYM	TERM
OTT	Over-the-Top - Describes a scenario in which a telecommunications service provider delivers one or more of its services across all IP networks, predominantly the public Internet although sometimes telco-run cloud services delivered via a corporation's existing IP-VPN from another provider.
OVA	Open Virtualization Archive - A tar archive file with the OVF directory inside.
OVF	Open Virtualization Format - An open standard for packaging and distributing virtual appliances or, more generally, software to be run in virtual machines.
PaaS	Platform as a Service - Refers to a category of cloud computing services that provides a platform, allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.
PRG	Personal Ring Group - An association of two or more devices for a single user.
PSAP	Public Safety Answer Point
PSM	(Contact Center) PhoneSet Manager
PSTN	Public Switched Telecommunications Network Public Switched Telephone Network
RAD	Recorded Announcement Device
RTE	Real Time Events
SaaS	Software as a Service - Refers to a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software".
Salesforce/SFDC	A cloud-based Customer management system (CRM).
SMB	Small-Medium Business - One of the MiCloud architectures.
SRC	Secure Recording Connector - One of the applications of MiVoice Border Gateway. Enables third-party call recording solutions to securely record IP end-point and Teleworker extensions.
TCP	Transmission Control Protocol - One of the main protocols in TCP/IP networks. While the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also that packets will be delivered in the same order in which they were sent.
Tollring	Company that delivers real-time call analytics via the cloud. www.tollring.com
UC	Unified Communications
UCC	Unified Communications and Collaboration
UDP	User Datagram Protocol - A simple connectionless transmission model. It has no hand-shaking, and thus exposes the user's program to any unreliability of the underlying network protocol. There is no guarantee of delivery, ordering, or duplicate protection. Provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.
ULM	Mitel UCC Group License Manager
vCNS	VMware vCloud Networking and Security
VLAN	Virtual Local Area Network

MiCloud Business Multi-Instance Deployment

ACRONYM	TERM
Voice Platform	Oria terminology for MiVoice Business
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding - Allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.
WAN	Wide Area Network

Appendix B

MITEL PERFORMANCE ANALYTICS

PROCEDURES

Mitel Performance Analytics deployment

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 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: (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"
```

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 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 MSL Blade install.

