MICLOUD BUSINESS VIRTUAL

FOR SERVICE PROVIDERS

DEPLOYMENT GUIDE
RELEASE 3.3

APRIL 2017

Mitel®

NOTICE

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

Trademarks

MiCloud Business Virtual for Service Providers
Deployment Guide
Release 3.3
April 2017

Chapter 1: MiCloud Business Virtual deployment process

MiCloud Business Virtual deployment process 9
Documentation and training sources 12
Prerequisites 12
MiCloud Business Virtual deployment process and roles 13
MiCloud Business Virtual deployment process 14

Chapter 2: Virtual infrastructure deployment

Virtual infrastructure deployment 19
Prerequisites 19
Virtual infrastructure deployment task flow 19
Deploy server hardware (IaaS) 20
Deploy VMware® vCenter™, vSphere®, and vCloud Director® (IaaS) 21
Install a DNS server on the management VLAN (PaaS) 22
Assign management plane (PaaS) 23

Chapter 3: Oria deployment

Oria deployment 27
Prerequisites 27
Oria and management VLAN deployment task flow 27
Install Oria OVA (PaaS) 28
Configure external access to Oria portal (PaaS) 29
Configure Oria (SaaS) 30
Define Oria User Bundles 31

Chapter 4: (Optional) Mitel Performance Analytics deployment

Optional: Mitel Performance Analytics deployment 35
Prerequisites 35
Mitel Performance Analytics deployment task flow 35
Install Mitel Performance Analytics (PaaS) 36
Configure external access to Mitel Performance Analytics portal (PaaS) 37
Configure Mitel Performance Analytics (SaaS) 38

Chapter 5: UCC platforms deployment

UCC Platforms deployment 41
Prerequisites 41

UCC Platforms deployment task flow . . . 41
Assign customer VLAN and VRF (PaaS) . . . 42
Configure 1:1 NAT with MiCloud Management Gateway (PaaS) . . . 43
Install and configure 1:1 NAT with VMware vCloud Networking and Security (PaaS) . . . 45
Configure Mitel Performance Analytics Probes (SaaS) . . . 47
Deploy MiVoice Business and MiCollab OVAs (PaaS) . . . 48
Optional: (SMB only) Use Oria Platform Manager to create Blueprints . . . 50
Deploy UCC OVAs (PaaS) . . . 52
Optional: Install MiContact Center Business and MiVoice Call Recording . . . 55
Optional: Deploy business analytics . . . 57
Deploy optional OVAs . . . 58
Optional: Deploy on-site survivable gateways . . . 59
Optional: Deploy Vidyo® functionality for MiCollab Client users . . . 60

Chapter 6: UCC platform configuration

UCC Platform system configuration. . . . 63
Prerequisites . . . 63
UCC Platform system configuration task flow . . . 63
Configure AMC licensing (SaaS) . . . 64
Synchronize to Applications Management Center (AMC) . . . 65
Install a DNS server for Customer management plane (SaaS) . . . 66
Add management DNS, customer DNS, and public DNS entries (SaaS) . . . 67
MLB only: Configure MiCollab (SaaS) . . . 68
Configure and cluster external MBGs (SaaS) . . . 69
MLB only: Configure and cluster MiVoice Business instances (SaaS) . . . 71
SMB only: Configure MiVoice Business Express . . . 72
SMB only: Optional - Configure MiVoice Business resilient controller . . . 73
Configure on-site survivable gateway interfaces (as needed) (SaaS) . . . 74
Optional: Deploy Open Integration Gateway Virtual Instances (SaaS) . . . 75
Optional: Deploy a customer backup server (SaaS) . . . 76

Chapter 7: (Optional) CRM integrations deployment

Deploy Customer Relationship Management (CRM) integrations . . . 79
Prerequisites . . . 79
CRM deployment task flow . . . 79
Deploy MiVoice Integration for Google, MiVoice Integration for Salesforce . . . 80

Deploy MiCloud CRM Integrations 82

Chapter 8: UCC platform services configuration

UCC Platform services configuration with Oria (SaaS) 87

Prerequisites 87

Customer services creation task flow 87

Register UCC platforms with Oria (SaaS) 88

Create Oria customer for UCC Platforms (SaaS) 90

Assign Bundles to customer (SaaS) 91

Chapter 9: UCC platforms end-user provisioning

UCC Platforms end-user provisioning with Oria 95

Prerequisites 95

End-user provisioning task flow 95

Bulk import end-users (SaaS) 96

Administer end-users (Reseller) 99

Configure telephony features (reseller or customer) 100

Tune the deployment in MiVoice Business, MiCollab, and MiVoice Border Gateway (SaaS or Reseller) 101

Deploy phones and clients (Reseller) 102

Optional: Prepare MiCollab Client for mobile users 103

Optional: Provision MiVoice Integration users 105

Synchronize users with MiContact Center Business 107

Chapter 10: Deployment completion

Deployment completion 111

Prerequisites 111

Deployment completion task flow 111

Obtain customer sign off 112

Transition deployment to operations 113

Chapter 11: UCC platform de-assignment

UCC Platforms de-assignment 117

Prerequisites 117

Platform de-assignment task flow 117

Delete a customer's Oria profile 118

Clear a customer configuration 119

Delete the customer OIG Virtual instances 120
Engage Mitel for license clean up 121

Chapter 12: MiCloud Business upgrade

Upgrading MiCloud Business Virtual 125
Prerequisites 125
Upgrade MiCloud Business Virtual 3.0/3.1 to MiCloud 3.3 126
1. Upgrade MiCloud Management Gateway (MMG) to Rls 5.0.6.0 126
2. Upgrade Oria to Rls 5.3 SP1 127
3. Upgrade Open Integration Gateway (OIG) to Rls 4.0 128
4. Upgrade MarWatch Server to Mitel Performance Analytics 2.1 131
5. Upgrade MiCollab to Rls 7.3 PR1 132
6. Upgrade external MiVoice Border Gateways (MBG) to Rls 9.4 PR3 133
7. Upgrade MiVoice Business controllers to Rls 8.0 PR3 135
8. Upgrade MiContact Center Business to Rls 8.1 SP1 135
9. Upgrade MiVoice Border Gateway Secure Recording Connector to Rls 9.4 PR3 136
10. Upgrade MiVoice Call Recording to 9.1 137
Upgrading MiCloud Business Virtual (SMB) 138
Prerequisites 138
Upgrade MiCloud Business Virtual (SMB) from Rls 3.0/3.1 to Rls 3.3 139
1. Upgrade MiCloud Management Gateway (MMG) to Rls 5.0.6.0 139
2. Upgrade Oria to Rls 5.3 SP1 140
3. Upgrade Open Integration Gateway (OIG) to Rls 4.0 141
4. Upgrade MarWatch Server to Mitel Performance Analytics (MPA) 2.1 144
5. Upgrade the MiVoice Business controllers (Remote Survivable Gateways) to Rls 8.0 PR3 145
6. Upgrade MiVoice Business Express to Rls 7.3 PR1 145
7. Upgrade MiContact Center Business to Rls 8.1 SP1 147
8. Upgrade MiVoice Border Gateway Secure Recording Connector to Rls 9.4 PR3 148
9. Upgrade MiVoice Call Recording to Rls 9.1 149

APPENDIX A: GLOSSARY OF ACRONYMS

Glossary of acronyms 153

APPENDIX B: MITEL PERFORMANCE ANALYTICS PROCEDURES

Mitel Performance Analytics deployment 159
Download Mitel Performance Analytics OVA 159

Deploy Mitel Performance Analytics OVA 159
Install Windows root certificate file for Probe 160
Install Linux root certificate file for Probe 160

Chapter 1

MICLOUD BUSINESS VIRTUAL DEPLOYMENT PROCESS

MiCloud Business Virtual deployment process

MiCloud Business Virtual deployments are based on a VMware virtual infrastructure. This guide describes how to deploy the Medium-Large Business and Small-Medium Business architectures described in the *MiCloud Solutions Blueprint*.

The MiCloud Business Virtual deployment process is used to install and configure the MiCloud Business MLB UC solution architecture and the Small Medium Business (SMB) architecture. The SMB architecture is the same as the MLB architecture, except that it uses the MiVoice Business Express. MiVoice Business Express is a virtual appliance that includes MiVoice Business, MiCollab, MiVoice Border Gateway and other applications, all in one OVA for easy deployment.

The deployment process described in this guide results in the creation of a topology that is verified as operational and ready for the addition of more customers as required. Licensing, infrastructure set-up, and end-user configuration are completed during this deployment process.

Table 1 shows the Mitel product lineup that comprises MiCloud Business 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.

The following figures show the MLB and SMB architectures.

Figure 1: MiCloud Business Virtual - MLB architecture

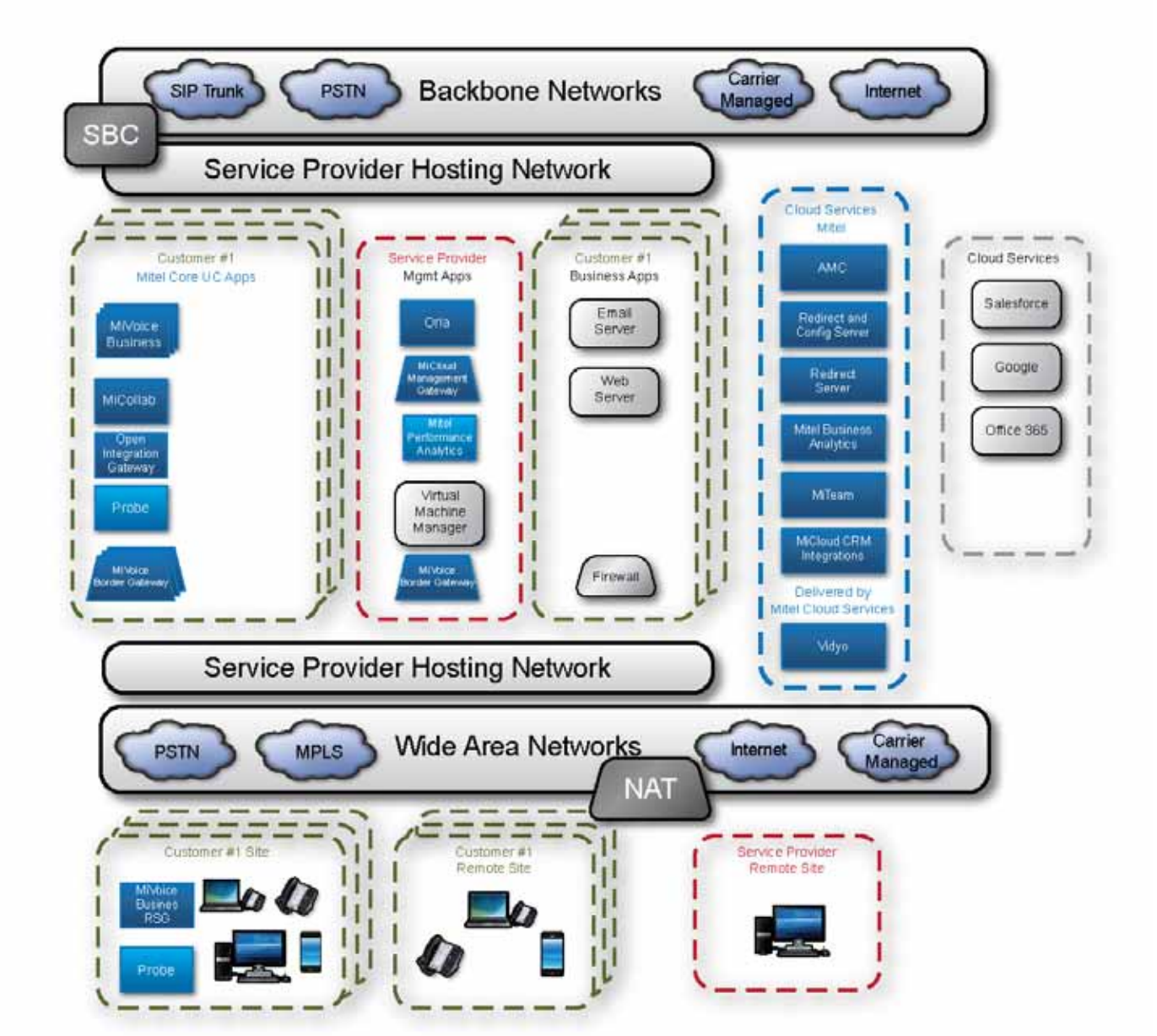
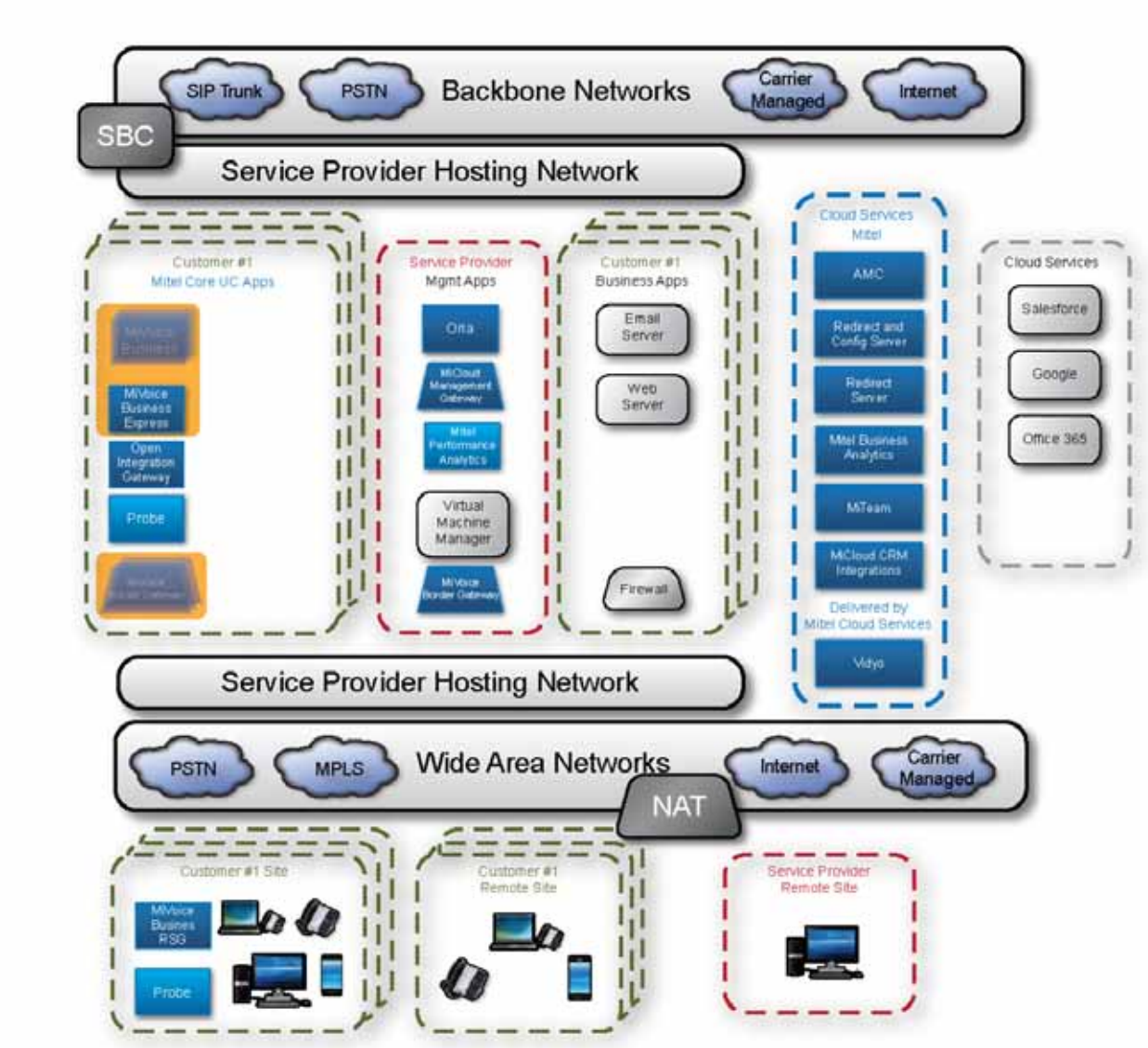


Figure 2: MiCloud Business Virtual - Small Medium Business (SMB) architecture



In this guide, the following terminology is used:

Table 2: Terminology used in this guide

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	Each customer of the service provider has its own network that is isolated from the service provider and from other customers of the service provider.
Reseller	The reseller has the ability to access the full system. The system administrator may perform a good part of this function.

System Administrator / 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 3, "Deployment roles," on page 13.
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 phone and UC 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
  - Engineering Guidelines for all of the Mitel platforms and applications are available on Mitel OnLine
- *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 documentation - available on Mitel OnLine
- MiCloud Business Analytics documentation
- Vidyo documentation - http://www.vidyo.com/services-support/technical-support/product-documentation/

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/.

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:
  - See 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

MiCloud Business Virtual deployment process and roles

The MiCloud Virtual deployment process (“MiCloud Business Virtual deployment process flow chart” on page 15) summarizes the actions for deploying the reference architectures. Each flowchart item corresponds to a task flow that breaks the deployment process down into a set of tasks.

The installation and configuration tasks are meant to be performed by various players; these players are described in Table 3.

Table 3: 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.
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 addressing plan for SaaS provider and customer IP.
- Determine the UCC service bundles to align with the end-user services offered by the SaaS provider
- Determine the number and type of UCC platforms required for a particular customer.

It is assumed this information will be available to the technical staff performing the deployment. The major steps in the deployment process are shown in Table 4. These deployment steps are described in this guide.

Table 4: Deployment steps

STEP	ROLE	SUB-STEPS
1. Deploy the virtual infrastructure	IaaS	
2. Deploy provider management tools	PaaS, SaaS	• Set up management plane networking (PaaS) • Deploy Oria and establish network access (PaaS • Optionally deploy and configure Mitel Performance Analytics server and establish network access (PaaS) • Deploy Probes (SaaS) • Configure Oria and define user bundles for reuse across customers (SaaS)

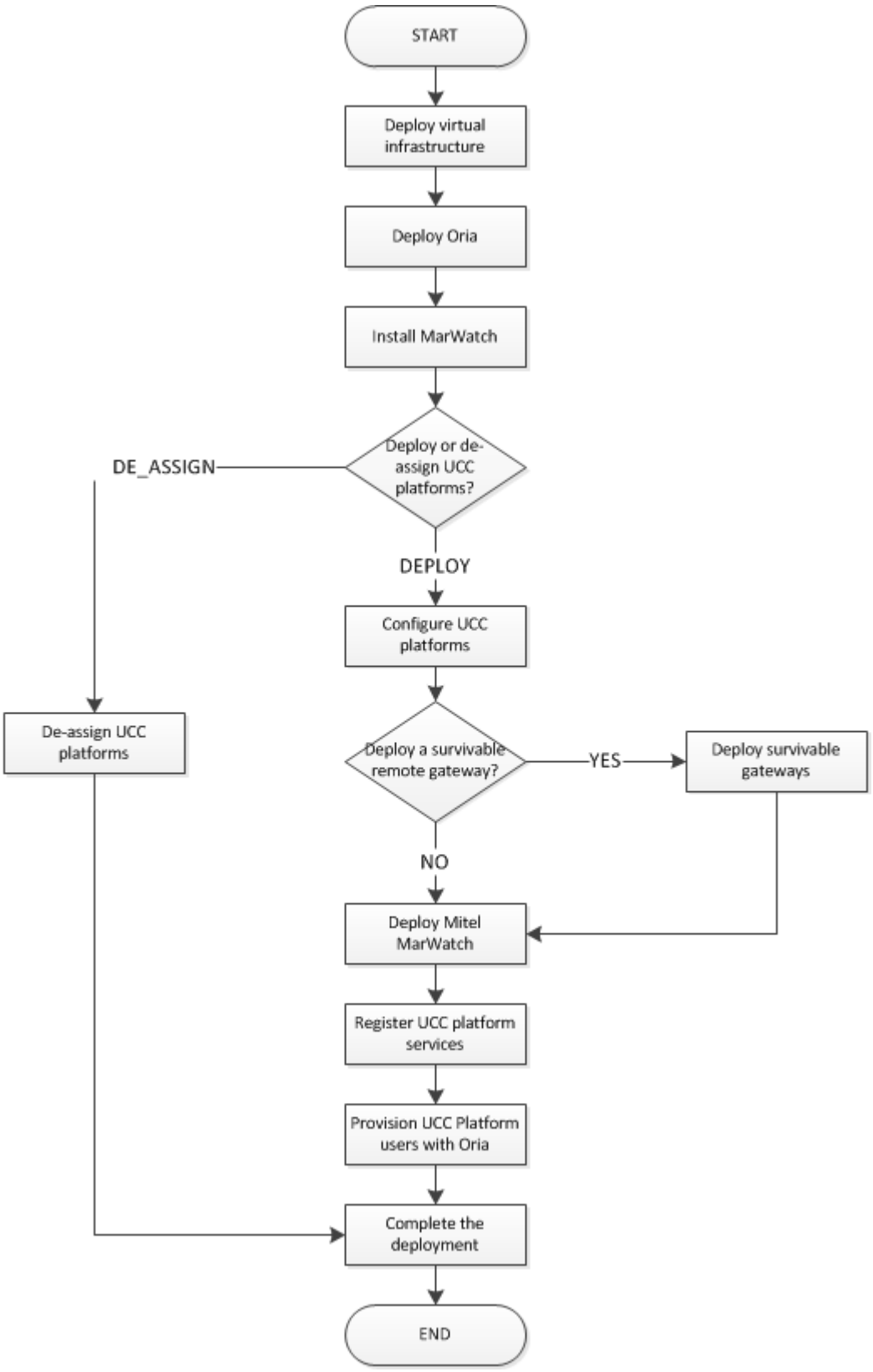
Table 4: Deployment steps

STEP	ROLE	SUB-STEPS
3. Deploy the UCC platforms.	PaaS	• Set up customer networking (PaaS) • Deploy UCC platforms (PaaS) • Configure AMC licensing (SaaS) • Configure UCC platforms (SaaS)
4. Provision the customer services and end-users with Oria	SaaS and/or Reseller	

MiCloud Business Virtual deployment process

The following flowchart summarizes the process for deploying the MiCloud Virtual topologies. 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 3: MiCloud Business Virtual deployment process flow chart



Chapter 2

VIRTUAL INFRASTRUCTURE DEPLOYMENT

Virtual infrastructure deployment

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

Prerequisites

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

Virtual infrastructure deployment task flow

The steps are as follows:

- “Deploy server hardware (IaaS)” on page 20
- “Deploy VMware® vCenter™, vSphere®, and vCloud Director® (IaaS)” on page 21
- “Install a DNS server on the management VLAN (PaaS)” on page 22
- “Assign management plane (PaaS)” on page 23

Also see the *Virtual Appliance Deployment Solutions Guide* for detailed information about deploying Mitel virtual appliances, including setting up storage, networking, and redundancy,

Deploy server hardware (IaaS)

Deploy server hardware to be used for installing the Mitel OVA files for Mitel virtual applications. The server hardware must be installed and configured in the network using the instructions in the manufacturer's documentation.

Servers are deployed and networked on the infrastructure network. The infrastructure LAN is independent of the management LAN.

Prerequisites

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

Resources

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

Deploy VMware® vCenter™, vSphere®, and vCloud Director® (IaaS)

To deploy the VMware infrastructure:

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

Prerequisites

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

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

Resources

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

Install a DNS server on the management VLAN (PaaS)

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

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

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
Third-party DNS server documentation	Configuration instructions

Assign management plane (PaaS)

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

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

The two choices for address translation are:

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

Optional: Install MiCloud Management Gateway (MMG)

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

You will configure it later, in “Configure 1:1 NAT with MiCloud Management Gateway (PaaS)” on page 43.

Considerations:

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

Note: MiVoice Business does not recognize FQDNs, so communication with Oria must be set up using IP addresses.

Use the Oria maintenance command to make the change to IP addresses.

$$UPDATE MCD CUSTOMER HOST NAME$$ <Management Host Name IP Address>, <New Customer Host Name>

See the *Oria Installation and Maintenance Guide* for instructions.

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

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

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

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

Prerequisites

-

Resources

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

Chapter 3

ORIA DEPLOYMENT

Oria deployment

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

Prerequisites

- VMware infrastructure is in place.
- Customers are connected to the hosted infrastructure using MPLS, with a common VRF router, and isolation using VLANs.
- No end-user IP phones are registered prior to provisioning users in Oria, or if there are phones registered, they are removed before provisioning. See also “Bulk import end-users (SaaS)” on page 96.

Oria and management VLAN deployment task flow

This chapter describes the following steps:

- “Install Oria OVA (PaaS)” on page 28
- “Configure external access to Oria portal (PaaS)” on page 29
- “Configure Oria (SaaS)” on page 30
- “Define Oria User Bundles” on page 31

Install Oria OVA (PaaS)

Oria provides a way to manage network elements, customers, and end-users.

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

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

Prerequisites

- If using MiCloud Management Gateway, external fire walls may be required for devices that require public Internet access, such as the public portal for the Oria platform. If using VMware vCloud Networking and Security (vCNS), this is covered in “Install and configure 1:1 NAT with VMware vCloud Networking and Security (PaaS)” on page 45.

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	Follow the instructions in the following sections: • “Oria OVA deployment” This creates the virtual machine. • “Oria-MiVoice Border Gateway (MBG) Synchronization”
Virtual Appliance Deployment Solutions Guide	Covers 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/
Oria Engineering Guidelines	See the “VLAN Support” section.
MiCloud Management Gateway Online Help	Available through MSL help.

Configure external access to Oria portal (PaaS)

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.

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

Prerequisites

- DNS must be set up with the public FQDN for Oria.

Resources

RESOURCE	CONTENT DETAILS
Third-party web proxy documentation	
MiVoice Border Gateway Engineering Guidelines	See “Remote Proxy Services”.

Configure Oria (SaaS)

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

Tip: Understand the scope of all the tasks 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 Mitel platforms
- Create test Bundles
- Assign Bundles to test Customers

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

For every MiVoice Border Gateway cluster that Oria will manage, define MBG cluster Zones in Oria. Oria will then display those cluster zones when creating sites in Platform Groups.

The concept of Cluster Zones applies to your MiVoice Border Gateway Clusters. In an earlier step, you created a MiVoice Border Gateway Cluster for MiNet devices, and a MiVoice Border Gateway Cluster for SIP Trunks. In an upcoming step, you will create another MiVoice Border Gateway Cluster for SIP devices. These MiVoice Border Gateway Cluster Zones must be entered into the Oria mbgZones.xml file. See the Oria 5.0 documentation for a description of how this is done.

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	For installation and configuration, see: • “Installation overview” • “Initial system configuration”
Oria Engineering Guidelines	For best performance, use the engineering guides to ensure that the configuration respects allowed capacities and limitations.

Define Oria User Bundles

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

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

1. Log into MSL and launch Oria.
2. Log in to Oria as an administrator.
3. Create **Administrator Bundles** and **User Bundles**.
   - **Administrator Bundles** define the features available to customer administrators.
   - **User Bundles** define the feature sets that will be offered to customers.
4. If you will be deploying MiCollab Clients for mobile users, you need to create a special User Bundle that includes a phone with **Phone Type** set to **Next Gen Mobile SIP Softphone**.
   - Scroll to the **Softphone Settings** section. In the **MBG SIP Port** field, change Port 5061 to 0 (zero).
5. If you will be deploying WebRTC MiCollab Web Clients for some users, you need to use a User Bundle that includes a phone with **Phone Type** set to **PC SIP softphone**.
6. Create **Feature Profiles**.
7. Create **Bundles**. The possible Bundle types are Admin Bundle, Basic IPT, Standard IPT, Entry, Standard, and Premium.

   To create a Bundle for contact center agents:

   a. Create a Bundle with:
      - **License Type** = **Contact Center Agent**
      - **Prime Phone Type** = **ACD with Softphone**.

   b. 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**.
8. When creating Premium Bundles, if you want to enable MiCollab MiTeam for users:

   a. Scroll down to **MiCollab Client Service**.

   b. Select **MiTeam**.

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

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

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

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

See also “UCC Platform services configuration with Oria (SaaS)” on page 87.

Prerequisites

- At least one Feature Profile has already been created.

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	See “Create bundles”.
Oria Online Help	In Oria, select the **Bundles** tab and click **Show Help** to display help topics for creating bundles.
MiTeam for MiCollab and MiCloud Business Virtual Reference Guide	
MiCollab Client Administrator Guide	See “MiTeam Integration”.

Chapter 4

(OPTIONAL) MITEL PERFORMANCE ANALYTICS DEPLOYMENT

Optional: Mitel Performance Analytics deployment

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

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

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

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

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

Prerequisites

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

Mitel Performance Analytics deployment task flow

These are the steps that must be performed to configure Mitel Performance Analytics monitoring of the topology.

- “Install Mitel Performance Analytics (PaaS)” on page 36
- “Configure external access to Mitel Performance Analytics portal (PaaS)” on page 37
- “Configure Mitel Performance Analytics (SaaS)” on page 38

Install Mitel Performance Analytics (PaaS)

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

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

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Mitel Performance Analytics installation and configuration instructions	See “Mitel Performance Analytics deployment” on page 159.
Mitel Performance Analytics System Guide	See “Probe Installation and Configuration”. Also see the documentation on Mitel OnLine.

Configure external access to Mitel Performance Analytics portal (PaaS)

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

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

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

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

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

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

Prerequisites

•

Resources

RESOURCE	CONTENT DETAILS
MiVoice Border Gateway Installation and Maintenance Guide	To configure MBG to support external traffic into the service provider's network: • "Server-Gateway Configuration on Network Edge"

Configure Mitel Performance Analytics (SaaS)

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

Mitel Performance Analytics server:

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

Probe:

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

Prerequisites

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

Resources

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

Chapter 5

UCC PLATFORMS DEPLOYMENT

UCC Platforms deployment

Deploy UCC platforms for end-customers.

Prerequisites

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

UCC Platforms deployment task flow

This chapter describes the following steps:

- "Assign customer VLAN and VRF (PaaS)" on page 42
- Configure 1:1 NAT with forwarding for management access using either MiCloud Management Gateway or vCNS. Use **one** of the following procedures:
  - "Configure 1:1 NAT with MiCloud Management Gateway (PaaS)" on page 43
  - "Install and configure 1:1 NAT with VMware vCloud Networking and Security (PaaS)" on page 45
- "Configure Mitel Performance Analytics Probes (SaaS)" on page 47
- "Deploy MiVoice Business and MiCollab OVAs (PaaS)" on page 48
- "Optional: (SMB only) Use Oria Platform Manager to create Blueprints" on page 50
- "Deploy UCC OVAs (PaaS)" on page 52
- "Optional: Install MiContact Center Business and MiVoice Call Recording" on page 55
- "Optional: Deploy business analytics" on page 57
- "Deploy optional OVAs" on page 58
- "Optional: Deploy on-site survivable gateways" on page 59
- "Optional: Deploy Vidyo® functionality for MiCollab Client users" on page 60

Note: For details and decision-making criteria to use to choose either MiCloud Management Gateway or vCNS, see the *MiCloud Blueprint Guide*.

Assign customer VLAN and VRF (PaaS)

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

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

Prerequisites

- The management plane is deployed and operational.

Resources

RESOURCE	CONTENT DETAILS
Engineering Guidelines for Industry Standard Servers (ISS) and MiVoice Business Virtual	See “MiVoice Business Virtual Engineering Guidelines System Overview”.
Installation and Administration Guide for Industry Standard Servers (ISS) and MiVoice Business Virtual	See “MiVoice Business Virtual Software Installation.”
Virtual Appliance Deployment Solutions Guide	See “Networking”.
Router or switch supplier documentation for VRF configuration	Instructions for installation and configuration

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

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

Use 1:1 network address translation (NAT) to isolate the service provider from the customers, and customers from each other. This is essentially a router function—IP to IP—with 1:1 direct IP Address (NAT) translation. A connection (and management IP address) is required for each of the Mitel virtual applications requiring management. Each MiCloud Management Gateway supports up to 100 customers.

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

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

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

Configuring MiCloud Management Gateway:

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

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
MSL Online Help	See the MiCloud Management Gateway configuration instructions.

Install and configure 1:1 NAT with VMware vCloud Networking and Security (PaaS)

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

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

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

This deployment includes:

- VMware vCloud deployment NAT from a Customer network
- VMware vCloud deployment NAT from a Reseller network
- Direct vCenter deployment with port group backed networks

Important considerations and things to watch for:

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

Note: MiVoice Business does not recognize FQDNs, so communication with Oria must be set up using IP addresses.

Use the Oria maintenance command to make the change to IP addresses.

$$UPDATE MCD CUSTOMER HOST NAME$$ <Management Host Name IP Address>, <New Customer Host Name>

See the *Oria Installation and Maintenance Guide* for instructions.

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Oria Engineering Guidelines	See “VLAN Support”.
VMware documentation	https://www.vmware.com/support/pubs/

Configure Mitel Performance Analytics Probes (SaaS)

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

Deploy Probes:

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Mitel Performance Analytics System Guide	See “Probe Installation and Configuration”.

Deploy MiVoice Business and MiCollab OVAs (PaaS)

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

Deploy the required OVAs:

1. If SMB: Deploy MiVoice Business Express.

   There are two ways to deploy MiVoice Business Express:

   - Standard VMware install and deploy. See the *MiVoice Business Express Deployment Guide* and the *Virtual Appliance Deployment Solutions Guide* for detailed instructions.
   - Oria Platform Manager: You can automatically deploy MiVoice Business Express from pre-defined blueprints. See "Optional: (SMB only) Use Oria Platform Manager to create Blueprints" on page 50 and the Oria Online Help for details.

Note: Note that if you resilient deployments of MiVoice Business Express are not supported in Platform Manager at this time. If you are adding MiVoice Business instances for resiliency in the SMB deployment, you must deploy MiVoice Business in the standard way.

2. If MLB: Deploy MiCollab.
   - Deploy the MiCollab instances. Make sure they are configured for Integrated Mode. See the MiCollab installation documentation for details.
3. If MLB: Deploy MiVoice Business.
   - Deploy MiVoice Business instances in a cluster. Add each one as a Network Element in the same network, and follow the instructions in the System Administration Tool on-line help to cluster the instances.
   - Perform an SDS Sync. This will synchronize the MiVoice Business instances with each other and with the MiCollab instances.
   - Install a third-party certificate, and export it for import into all of the applications.
4. Optional: Deploy Mitel Performance Analytics Probes. See "(Optional) Mitel Performance Analytics deployment" on page 33.

Note: If you are not planning to install MiContact Center Business, but the customer 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

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

- DNS Server and domain name are available.

Resources

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
MiVoice Business Express Deployment Guide	
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/

Optional: (SMB only) Use Oria Platform Manager to create Blueprints

Note: You can use Platform Manager to automate set up of MiVoice Business Express, but any resilient MiVoice Business or MiVoice Border Gateways must be added manually later.

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. Create a new VMware vCenter Infrastructure.
   b. Register the Oria file server(s).
   c. Register the AMC account.
   d. Create Blueprints (ARID, resource, and platform) to describe platforms to deploy.
   e. Upload an MSL golden database and the MiVoice Business Express OVA.

Note: The Platform Manager server contains reference database files, in the directory /opt/dist_oria-bim-setup/reference.

   f. Create inventory pool(s) of platform Blueprints describing systems that you want to provide to your Customers.
   g. 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 an MSL golden database.

Resources

RESOURCE	CONTENT DETAILS
Oria Service Provider Portal Help	Navigate to: **Set Up Customers** > **Register Platform Groups** > **Configure Blueprints**.

Deploy UCC OVAs (PaaS)

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

Configure Remote Proxy access for configuration and management.

Deploy the required OVAs:

1. Deploy the external MiVoice Border Gateways.

Note: When deploying the MiVoice Border Gateways, both internal and external, keep in mind that the master MBGs overwrite the slave MBGs.

Slave MBGs are used in the same way as for Teleworkers and SIP trunks.

Note: When certificates are required, the same certificates are required on both the external and internal MBGs. If this is not done, MiCollab Client Teleworker users cannot log in.

   a. If you are deploying MiCollab soft phone resiliency, configure the MiVoice Border Gateways into a cluster and a backup cluster. DNS SRV records are used to define the MiVoice Border Gateways, their host names, their priorities and weightings, and Time To Live (TTL) for each. The Registrar/Proxy file in the MiCollab Client for Mobile soft phone lists the host names of multiple MBGs. Each soft phone can register with any of the MBGs in the list subject to the priority and weighting settings. See the *MiCollab Client for Mobile Resiliency Guide* for details and instructions.

Note: During fail-over to the secondary MiVoice Border Gateway, in-progress calls are lost, and new calls are completed through the secondary MiVoice Border Gateway.

   b. From the Mitel Standard Linux Web Server panel, purchase and install a third-party certificate for use with MiContact Center Business. This can be the same certificate as you are using for MiCollab, but it must include an intermediate certificate. See the Mitel Standard Linux Online Help. “Manage Third-Party Certificates from an Alternate Certificate Authority”.

   c. Export the new certificate using the Mitel Standard Linux utility. You will later install this certificate to the MiContact Center Server when completing the instructions in “Optional: Install MiContact Center Business and MiVoice Call Recording” on page 55.

Note: If the CSR code was not generated on the MiContact Center server, you may need to combine the CRT and KEY Files into a PFX using OpenSSL. Then apply the PFX certificate to the MiContact Center server.
Otherwise use the standard method for importing a certificate to a Windows server.

2. If you are deploying WebRTC for users, complete the following steps on the external MiVoice Border Gateway. This can be the same MiVoice Border Gateway being used for MiCollab Client for Mobile users.

   a. In Mitel Standard Linux, click **Applications** > **MiVoice Border Gateway** in the left column.

b. In the panel that appears, click **Service Configuration** > **WebRTC**.

c. Select **Enabled** to enable WebRTC.

d. Enter the following settings:

- **Hosting mode**: **Host WebRTC on separate server**
- **Mode**: **Subscriber**
- **Anonymous WebRTC ICP**: Select the MiVoice Business controller that is hosting the WebRTC clients.
- **WebRTC protocol security mode**: **Public Only**

e. If you are deploying a firewall on the external network in front of the MiVoice Border Gateway, perform the steps in “Configure the firewall for the WebRTC gateway” on page 53.

3. If you are deploying MiContact Center Business with external users, you must enable an MiVoice Border Gateway web proxy.

a. On the MSL server, select **Applications** > **Remote proxy services**.

b. Click **Add new LAN server proxy**.

c. On the Configure **Web Proxy & Remote Management Service** page:

- Select **Enabled** to enable the web proxy.
- In **WAN-side FQDN**, enter the FQDN of the MiContact Center server.
- Select **MiContact Center**.

4. If you are deploying MiVoice Call Recording web proxy, repeat step 3., selecting **MiVoice Call Recording** in place of **MiContact Center**, and entering the MiVoice Call Recording server FQDN.

Configure the firewall for the WebRTC gateway

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

Prerequisites

- vSphere is installed and configured, using VMware best practices and the Mitel resource requirements.
- vCenter is installed and configured, using VMware best practices.

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

Resources

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

Optional: Install MiContact Center Business and MiVoice Call Recording

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

Deploy the OVAs in the following order:

1. If you will be offering call recording, deploy one or more additional MiVoice Border Gateways, configured in Secure Recording Connector (SRC) mode.

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

2. Deploy the MiVoice Call Recording OVAs.
   - Connect MiVoice Call Recording to MiVoice Business (MiTAI connection).
   - Connect MiVoice Call Recording to MiVoice Border Gateway (Secure Recording Connector). MiVoice Call Recording requires an SQL database, either Standard or Express, depending on the capacity you need.

Note: Contact Mitel Professional Services for help sizing and configuring storage for call recording archives.

3. Deploy MiContact Center Business.

Note: MiContact Center Business will be deployed and configured in one of several different ways, depending on the whether the contact center is small and informal, or the prime business, See the *Contact Center Blueprint* for details.

Use of Mitel Professional Services is strongly recommended.

   - Configure MiContact Center Business to point to MiVoice Call Recording, if applicable.
   - Install the certificate you exported from the MiVoice Border Gateway in “Deploy UCC OVAs (PaaS)” on page 52, in the MiVoice Border Gateways installation instructions.

Note: If the CSR code was not generated on the MiContact Center server, you may need to combine the CRT and KEY Files into a PFX using OpenSSL. Then apply the PFX certificate to the MiContact Center server.
Otherwise use the standard method for importing a certificate to a Windows server.

4. If you will be provisioning remote agents and/or supervisors, the MBG Connector must be enabled. On the existing MiNet user MiVoice Border Gateways (or if creating new MiVoice Border Gateways):
   a. Navigate to the **Service Configuration** tab > **Applications Integration**, select **MiContact Center connector enabled**.
   b. In **MiContact Center Service hostname or IP address**, enter the FQDN of the MiContact Center server.
5. If you are also providing integration with Salesforce, see “Deploy optional OVAs” on page 58.

Optional

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
VMware documentation	https://www.vmware.com/support/pubs/
MiContact Center Installation and Administration Guide	Use the instructions in the following sections: • “Enterprise Server installation” for how to download and install (MiContact Center (MiCC) Setup wizard) • “MiContact Center product registration” for how to register and set up MiContact Center on the Enterprise Server and client computers • “Remote Server Installation” for how to install and configure MiContact Center at remote sites • “Call Recording” for how to deploy MiVoice Call Recording
MiVoice Call Recording Installation and Configuration Guide	See “Software Installation”.
MiVoice Call Recording Administration Guide	See “Getting Started”.
MiVoice Business Integration Guide (9.1)	Describes how to connect SIP Trunks via MiVoice Border Gateway Secure Recording Connector.

Optional: Deploy business analytics

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

MiVoice Business Reporter

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

MiCloud Business Analytics

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

Prerequisites

- MiCloud Business Analytics requires an SMDR server.

Resources

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

Deploy optional OVAs

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).

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
Mitel product-specific documentation, including Installation Guides and Engineering Guides	Mitel 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/
Mitel OIG Installation and Maintenance Guide	To install OIG, see “Installing the Mitel OIG”. If you will be using OIG with MiContact Center Business and Salesforce, see “The Network Elements Tab”.
Mitel OIG Engineering Guidelines	For requirements and capacity.
MiVoice Integration for Google Administration Guide *MiVoice Integration for Google Quick Reference Guide*	For instructions for installing and configuring MiVoice Integration for Google.
MiVoice Integration for Salesforce Administration Guide	For installing and configuring MiVoice Integration for Salesforce with OIG and MiContact Center Business.

Optional: Deploy on-site survivable gateways

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

Install the secondary gateway before installing the primary. In the MiVoice Business System Administration Tool, run an SDS Sync to synchronize the primary and secondary gateways.

The Gateways will be configured in a later step.

Prerequisites

- Management and customer VLANs are deployed and operational.

Resources

RESOURCE	CONTENT DETAILS
3300 ICP Technician's Handbook	Planning and performing the installation
3300 ICP System Administration Tool Help	See the following: • "Start Here Guide" for hardware installation and licensing. • "Installation and Programming"

Optional: Deploy Vidyo® functionality for MiCollab Client users

Vidyo® is a cloud-based video collaboration service. The Vidyo service enhances MiCollab Client by adding a Vidyo icon to the MiCollab Client user interface.

See the *MiCollab Vidyo Administrator Quick Reference Guide* for detailed instructions.

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Vidyo documentation	https://selfservice.vidyo.com/eService/OnlineDocumentation.aspx
MiCollab Vidyo Administrator Quick Reference Guide	Follow all of the instructions in this guide.

Chapter 6

UCC PLATFORM CONFIGURATION

UCC Platform system configuration

Configure the UCC platforms.

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

Prerequisites

- UCC platform OVAs have been deployed

UCC Platform system configuration task flow

Use the steps in this chapter to complete this deployment task.

MLB/SMB STEP

- “Configure AMC licensing (SaaS)” on page 64
- “Synchronize to Applications Management Center (AMC)” on page 65
- “Install a DNS server for Customer management plane (SaaS)” on page 66
- “Add management DNS, customer DNS, and public DNS entries (SaaS)” on page 67

MLB STEPS

“MLB only: Configure MiCollab (SaaS)” on page 68

“Configure and cluster external MBGs (SaaS)” on page 69

“MLB only: Configure and cluster MiVoice Business instances (SaaS)” on page 71

SMB STEPS

- “Configure and cluster external MBGs (SaaS)” on page 69
- “SMB only: Configure MiVoice Business Express” on page 72
- “SMB only: Optional - Configure MiVoice Business resilient controller” on page 73

MLB/SMB STEP

- “Configure on-site survivable gateway interfaces (as needed) (SaaS)” on page 74
- “Optional: Deploy Open Integration Gateway Virtual Instances (SaaS)” on page 75
- “Optional: Deploy a customer backup server (SaaS)” on page 76

Configure AMC licensing (SaaS)

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

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

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

Note: Do not add Oria to the ULM.

Prerequisites

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

Resources

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

Synchronize to Applications Management Center (AMC)

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

On the Mitel Standard Linux (MSL) status panel:

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

Prerequisites

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

Resources

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

Install a DNS server for Customer management plane (SaaS)

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

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

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

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

Prerequisites

-

Resources

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

Add management DNS, customer DNS, and public DNS entries (SaaS)

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

- In the customer DNS, add FQDNs that map to the management addresses of the platforms in the hosted customer network.
- In external and/or public DNSs, add FQDNs and public addresses for the gateways; reaches to MiVoice Border Gateway WAN interface, but public IP address may be the MiVoice Border Gateway WAN interface or external firewall interface depending on networking.

Prerequisites

-

Resources

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

Note: Proceed to the next step:

- MLB: “MLB only: Configure MiCollab (SaaS)” on page 68
- SMB: “Configure and cluster external MBGs (SaaS)” on page 69

MLB only: Configure MiCollab (SaaS)

License and install the MiCollab OVA.

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
MiCollab Installation and Maintenance Guide	See the following: • “UCC Licensing” • “Installing Virtual MiCollab in a VMware environment”

Note: Proceed to the next step:

- MLB: “Configure and cluster external MBGs (SaaS)” on page 69
- SMB: “SMB only: Configure MiVoice Business Express” on page 72

Configure and cluster external MBGs (SaaS)

Note: When deploying:

- MLB: Perform this step after “MLB only: Configure MiCollab (SaaS)” on page 68.
- SMB: Skip Configure MiCollab, and perform this step immediately after “Add management DNS, customer DNS, and public DNS entries (SaaS)” on page 67.

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

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

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

Note: Update Emergency Location information for customer with SIP Trunk provider; Also ensure updates are passed through to the local PSAP.

Example: One MBG cluster

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

Example: Teleworker cluster and SIP cluster

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

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

Prerequisites

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

Resources

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

MLB only: Configure and cluster MiVoice Business instances (SaaS)

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

Install and cluster MiVoice Business instances.

Cluster the MiVoice Business instances with MiCollab to enable Flow Through Provisioning and do an SDS Sync operation.

Prerequisites

- MiVoice Border Gateways are already installed.

Resources

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

SMB only: Configure MiVoice Business Express

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

The general steps to follow:

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

Note: Skip the step, “Configure Integrated Directory Services”. This step is not used when provisioning is done with Oria.

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	See “Deploying Mitel virtual appliances in VMware”.
MiVoice Business Express Deployment Guide	See “Configure system”.
MiVoice Border Gateway Installation and Maintenance Guide	See “Installing MiVoice Border Gateway software”.

SMB only: Optional - Configure MiVoice Business resilient controller

This is an optional step.

1. Deploy an additional MiVoice Business controller. This is usually a 3300 ICP, deployed locally. This allows continued operation in the event of WAN loss, but does require additional external trunks to be provided for external connections. (See also “Configure on-site survivable gateway interfaces (as needed) (SaaS)” on page 74.)
2. Configure it to match the MiVoice Business controller in MiVoice Business Express to make sure that it can be used to take over if MiVoice Business Express fails, or connection to it is lost.
3. In the MiVoice Business System Administration Tool:
   a. Configure the two MiVoice Business controllers to share using SDS, and perform a Sync operation.
   b. Configure the devices to use the two MiVoice Business controllers as Primary and Secondary.

Prerequisites

•

Resources

RESOURCE	CONTENT DETAILS
MiVoice Business Resiliency Guidelines	See the following: • “Implementing Resiliency” • Programming the Cluster and ARS”
MiVoice Business System Administration Tool Help	See the following help topics: • “Configuring a Cluster”
Using System Data Synchronization Solutions Guide	Description and instructions for System Data Synchronization (SDS) among MiVoice Business and MiCollab network elements.

Configure on-site survivable gateway interfaces (as needed) (SaaS)

Configure the following interfaces.

Automatic Route Selection (ARS) for the survivable gateway

Note: ARS can also be used for local trunks.

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

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

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

Emergency routes for survivable mode

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

Prerequisites

- The resilient MiVoice Business controllers must be deployed.

Resources

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

Optional: Deploy Open Integration Gateway Virtual Instances (SaaS)

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

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

Because OIG cannot be managed through Oria, OIG must be managed separately.

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

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

- MiVoice Integration for Salesforce
- MiVoice Integration for Google

Program a password for each application selected. User provisioning for these applications is done in “Optional: Provision MiVoice Integration users” on page 105.

In each MiVoice Business instance:

1. Add the OIG to the MiVoice Business **Network Elements** form as a member of the SDS Cluster.
2. Click **Start Sharing** and do a full SDS Synchronization.

   This allows end-users a simpler configuration because only the end-user DN is required.
3. The OIG then automatically finds the Call Server IP address.
4. Optional: Connect to MiContact Center Business for use with Salesforce. See the *MiContact Center and Business Reporter System Engineering Guide*.

Prerequisites

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

Resources

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

Optional: Deploy a customer backup server (SaaS)

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

Prerequisites

- A server is available for use in performing backups.

Resources

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

Chapter 7

(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 80

  OR

- “Deploy MiCloud CRM Integrations” on page 82

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*

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Virtual Appliance Deployment Solutions Guide	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/
Mitel OIG Installation and Maintenance Guide	To install OIG, see “Installing the Mitel OIG”. If you will be using OIG with MiContact Center Business and Salesforce, see “The Network Elements Tab”.
Mitel OIG Engineering Guidelines	For requirements and capacity.
MiVoice Integration for Google Administration Guide *MiVoice Integration for Google Quick Reference Guide*	For instructions for installing and configuring MiVoice Integration for Google.
MiVoice Integration for Salesforce Administration Guide	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 Admin 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	
MiCloud CRM Integrations User Guide	

Chapter 8

UCC PLATFORM SERVICES CONFIGURATION

UCC Platform services configuration with Oria (SaaS)

Configure customer services including:

- Feature Bundles
- Custom branding
- Emergency services access

This work was introduced in “Define Oria User Bundles” on page 31. Refer also to the *Oria Installation and Administration Guide*.

Prerequisites

- Person deploying has been trained on Oria.
- Customer branding components, such as logo, colors, custom banner, and browser-tab favicon have been created, and are available.
- Feature Bundles have been created in Oria. See “Configure external access to Oria portal (PaaS)” on page 29.

Customer services creation task flow

This list shows the tasks to be completed in this chapter:

- “Register UCC platforms with Oria (SaaS)” on page 88
- “Create Oria customer for UCC Platforms (SaaS)” on page 90
- “Assign Bundles to customer (SaaS)” on page 91

Register UCC platforms with Oria (SaaS)

Associate a platform group to an customer to connect the Oria profile of the customer with the platform group that includes the components providing the same customer's services.

Use the **Register Platform** wizard to register MiCollab and any external MBGs.

1. Register the Mitel products in Oria.
   - MiVoice Border Gateway or Gateways
   - MiCollab
2. If you will be provisioning mobile users, you must include the following steps in the MiCollab registration:
   a. Select **Use Embedded MiVoice Border Gateway**.
   b. In **Public Facing FQDN of External MBG**, enter the FQDN for the Teleworker MiVoice Border Gateway.
3. Optional: To provision MiCollab MiTeam users (Premium Bundles only), include the following steps in the MiCollab registration:
   a. In **Platforms > Edit Platform > MiCollab Client Tenant** tab, select **MiTeam Services**.
   b. Click **Save**.
4. Optional: To enable the emergency call warning on SIP clients:
   a. In **Platforms > Edit Platform > MiCollab Client Tenant** tab, select **Enable emergency call warning**.
   b. Click **Save**.

   The warnings 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."

Note: MiVoice Business instances and the embedded MiVoice Border Gateway are reached through MiCollab; they are not directly registered with Oria.

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

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	See “Register Platform Groups in Oria”.
MiTeam for MiCollab and MiCloud Business Virtual Reference Guide	

Create Oria customer for UCC Platforms (SaaS)

Use the Oria **Create Customer** wizard.

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

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

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

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

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

- Create an customer's user administration account - Create a customer's user administration account. This account is used to build an administrator profile in Oria for each customer for end-user administration. The customer uses the administration account to manage its own end-users. The service provider will also use this account for end-user changes when necessary.
- If the customer will have users who will use MiCollab Client on Mac computers, on the **Service Bundles** screen, select **Enable deployment for a MAC Client when at least one bundle contains a PC SIP Softphone and MiCollab's version is 7.1 or higher.**

Prerequisites

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

Resources

RESOURCES	CONTENT DETAILS
Oria Installation and Administration Guide	See “To assign a Platform Group to a customer”.

Assign Bundles to customer (SaaS)

Assign Admin and User Bundles to a customer or create custom bundles. This specifies, in the customer's Oria profile, all the features that they will have available.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	See "Create and Change Bundles".

Chapter 9

UCC PLATFORMS END-USER PROVISIONING

UCC Platforms end-user provisioning with Oria

Provision and configure end-users for the customer.

Prerequisites

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

End-user provisioning task flow

The following tasks are described in this chapter:

- “Bulk import end-users (SaaS)” on page 96
- “Administer end-users (Reseller)” on page 99
- “Configure telephony features (reseller or customer)” on page 100
- “Tune the deployment in MiVoice Business, MiCollab, and MiVoice Border Gateway (SaaS or Reseller)” on page 101
- “Deploy phones and clients (Reseller)” on page 102
- “Optional: Prepare MiCollab Client for mobile users” on page 103
- “Optional: Provision MiVoice Integration users” on page 105
- “Synchronize users with MiContact Center Business” on page 107

Bulk import end-users (SaaS)

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

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

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

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

Note: The following types cannot be provisioned from Oria:

- paths
- agent groups

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

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

Import users using 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.

Adjust the ACD soft phone users/devices

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Maintenance Guide	See “Create Welcome Email”.
Oria Service Provider Portal Help	Provisioning users by importing an Active Directory LDIF file

Administer end-users (Reseller)

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:

- 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

- Administrator access is provisioned for the customer in Oria.

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	For ring groups, hunt groups and pickup groups, auto attendant, etc.: • "Configure the Default MiVoice Business Platform database" For music on hold and ACD features: • "Create and Change Bundles"

Configure telephony features (reseller or customer)

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.

In the Oria Administration Portal, program the ACD groups for each customer.

In the MiVoice Business System Administration Tool, do the detailed programming of the ACD functions. ACD agents are programmed as Hot Desk agents.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	See "Create and Change Bundles".
MiVoice Business System Administration Tool Online Help	See the following help topics: • "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: • **ACD Agent Skill Groups** • **ACD Paths**

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.

Note: 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.

Note: Call Mitel Professional Services for any tuning in Oria.

Prerequisites

•

Resources

RESOURCE	CONTENT DETAILS

Deploy phones and clients (Reseller)

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

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

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

Each agent must install MBG Connector on their station.

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

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

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

Prerequisites

•

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	See “Overview”.
MiContact Center Installation and Administration Guide	See “Setting up phones for remote agents and employees”.

Optional: Prepare MiCollab Client for mobile users

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

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

Note: Third-party SSL certificates are **REQUIRED** on MiCollab and MiVoice Border Gateway for Service Providers deploying the MiCollab Client. Individual certificates are **REQUIRED** for every customer connected to the Service Provider.

1. Purchase and install third-party SSL certificates on MiCollab and MiVoice Border Gateway for the Service Provider and for every customer connected.
   - See MSL Online Help: “Manage Web Server Certificate”.
2. If you are configuring soft phone resiliency, on the **Manage MiCollab Client Deployment** screen, follow the instructions in the *MiCollab Client for Mobile Resiliency Guide*, “Configuration” section, with the following exception:
   - IGNORE the section, “Specify FQDN of MBG Cluster”.

Note: This step has to be done on every MiCollab Client Server that will support resiliency for mobile client users

Note: The *MiCollab Client for Mobile Resiliency Guide* assumes that DNS SRV is already set up with primary and secondary hosts.

3. If users will be configured to use MiTeam, ensure that the MiCollab Audio, Web and Video Conference service is running.
4. In the MiCollab Client **Configuration Tab**, customize the Deployment e-mail. This step customizes the message each user receives; this e-mail includes a link for downloading and installing the MiCollab Client soft phone on the user’s mobile devices.

   For details, see MiCollab Client Deployment Help topic, “Mobile Client Deployment Email”.
5. Apply branding (your company logo and custom colors), if required. In the **Configuration Tab**, under **Branding Settings**, select **Activate Custom Branding**. Enter the **Branding ID** and **Branding Secret**. Branding can be added to the Next Gen clients.

   Contact your sales representative for information about creating your branding ID and password.
6. In Oria, add the MiCollab Client users.
   - See the *Oria Installation and Administration Guide*.

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS
Mitel Standard Linux (MSL) Online Help	See the help topic: “Manage Web Server Certificate”.
MiCollab Client Deployment Help	See the following help topics: • “About MiCollab Client Deployment • “Deploy Client with MiVoice Business or MiVoice Business Express” • “Run Diagnostics” • “Mobile Client Deployment Email”
MiCollab Client for Mobile Resiliency Guide	Follow the instructions in “Configuration”, with the following EXCEPTION: • IGNORE the section, “Specify FQDN of MBG Cluster”.
Oria Installation and Administration Guide	See the following topics: • “DNS Resiliency ON MiCollab Client Server for Mobile Softphones (Register MBG)” • “Add a Next Gen Mobile Softphone” • “Create Brands”
MiTeam for MiCollab and MiCloud Business Virtual Reference Guide	

Optional: Provision MiVoice Integration users

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

Provision users for MiVoice Integration for Salesforce

Enable Salesforce users for MiVoice Integration for Salesforce.

Administrator actions (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 Extension 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 user must follow the steps in the *MiVoice Integration for Google Quick Reference Guide* to add and configure MiVoice Integration for Google.

Prerequisites

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

Resources

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

Synchronize users with MiContact Center Business

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

To synchronize contacts with MiVoice Business network:

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

Prerequisites

- Users have been provisioned in 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
MiContact Center User Guide	See “Performing Synchronization”.

Chapter 10

DEPLOYMENT COMPLETION

Deployment completion

Confirm that the following operation is complete:

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

Prerequisites

- All nodes and configurations are in place.

Deployment completion task flow

Perform the following tasks to complete the deployment:

- “Obtain customer sign off” on page 112
- “Transition deployment to operations” on page 113

Obtain customer sign off

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

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

Prerequisites

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

Resources

RESOURCE	CONTENT DETAILS

Transition deployment to operations

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

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS

Chapter 11

UCC PLATFORM DE-ASSIGNMENT

UCC Platforms de-assignment

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

In Oria, when you delete a customer, the following is done:

- delete platform
- reclaim resources

For detailed information, see the *Oria Installation and Administration Guide*.

Prerequisites

-

Platform de-assignment task flow

The tasks for deleting customers are:

- “Delete a customer’s Oria profile” on page 118
- “Clear a customer configuration” on page 119
- “Delete the customer OIG Virtual instances” on page 120
- “Engage Mitel for license clean up” on page 121

Delete a customer’s Oria profile

Delete a customer’s Oria profile to remove the connections between the license server, the platform group, and Oria for the customer.

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
Oria Installation and Administration Guide	

Clear a customer configuration

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

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

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

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS
MiVoice Business System Administration Tool Online Help	See the help topic: “Network Elements”.
Oria Installation and Administration Guide	See “Create and Change Bundles”, particularly the sections describing the features of Administrator Bundles.

Delete the customer OIG Virtual instances

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

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

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

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

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

Prerequisites

-

Resources

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

Engage Mitel for license clean up

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

Prerequisites

-

Resources

RESOURCE	CONTENT DETAILS

Chapter 12

MICLOUD BUSINESS UPGRADE

Upgrading MiCloud Business Virtual

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

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

Prerequisites

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

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

Upgrade options described in this chapter are:

- “Upgrade MiCloud Business Virtual 3.0/3.1 to MiCloud 3.3” on page 126
- “Upgrade MiCloud Business Virtual (SMB) from Rls 3.0/3.1 to Rls 3.3” on page 139

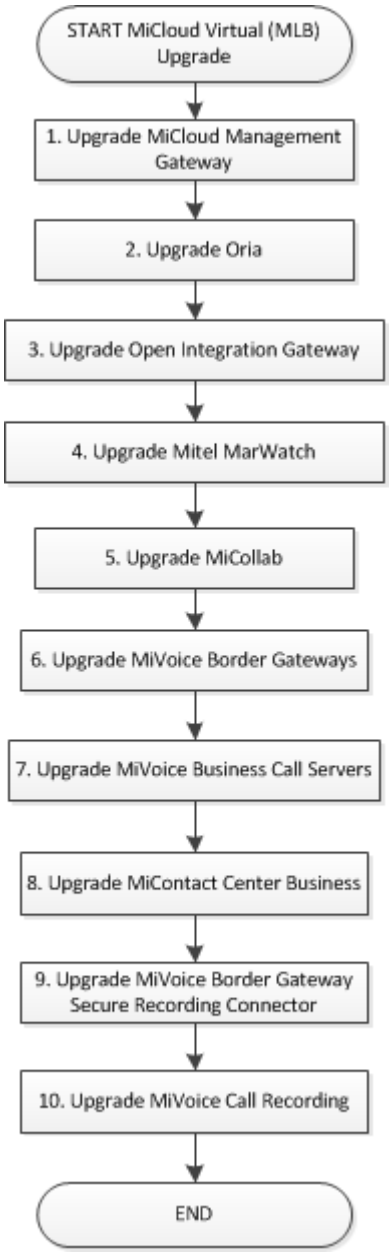
Note: To upgrade MiCloud Business Virtual from Release 2.0 to Release 3.3, you must perform the upgrade in two stages:

- Upgrade from MiCloud 2.0 to MiCloud 3.1: Follow the instructions in *MiCloud Release 3.1 Deployment Guide*.
- Upgrade from MiCloud Business 3.1 to MiCloud 3,2: Follow the instructions in this guide.

Upgrade MiCloud Business Virtual 3.0/3.1 to MiCloud 3.3

The upgrade to MiCloud Business 3.3 follows the flow shown in the graphic below.

Figure 4: Upgrading MiCloud Virtual from MiCloud 3.0/3.1 to 3.3



1. Upgrade MiCloud Management Gateway (MMG) to Rls 5.0.6.0

There are two ways to upgrade MMG

- Install new MMG OVA.

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

Primary resources:

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

Pre-upgrade tasks:

Table 5: Upgrade MiCloud Management 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[1]
replace VMware vCloud Networking and Security (vCNS)	5.0.x	5.0.x	0.5	0.5	Al	No manage-ment services available[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. Management services here refers to NAT managements hosts for the platforms.

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

2. Upgrade Oria to Rls 5.3 SP1

Primary resource: *Oria Installation and Administration Guide*

Pre-upgrade tasks: Full MSL back-up

No administrative changes are allowed during the Oria upgrade. If this is not acceptable, then 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 6: Upgrade Oria

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[1]	USER[1]	ADMIN[1]
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 **Restore from Running Server** option is not supported by Oria.

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.

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

- Reboot the OIG server as instructed to install the new MSL OS.
- In the OIG blades panel, install OIG 4.0.29+.

Table 7: Upgrade Open Integration Gateway

CURRENT RELEASE	UPGRADE TO	PRE-UPGRADE EFFORT	TIME TO UPGRADE (HRS)	ROLL-BACK TIME (HRS)	SERVICES AVAILABLE DURING UPGRADE USER[1]	SERVICES AVAILABLE DURING UPGRADE ADMIN[2]	SERVICES AVAILABLE AFTER UPGRADE USER[1]	SERVICES AVAILABLE AFTER UPGRADE 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 129
  - “Upgrade MiVoice Integration for Google” on page 130
- 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 8: 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*

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 9: 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

4. Upgrade MarWatch Server to Mitel Performance Analytics 2.1

Primary resource:

- *MarWatch Upgrade Guide*

Pre-upgrade tasks:

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

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 MarWatch server.

Table 10: 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	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.

5. Upgrade MiCollab to Rls 7.3 PR1

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

Primary resource:

- *MiCollab Installation and Maintenance Guide*

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

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

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

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

Pre-upgrade tasks:

- Request third-party certificate.

Table 11: Upgrade MiCollab

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]
7.1/7.2 SP1	7.3 PR1		Without SAA[4]: 1.0 With SAA: 2.0	1.0	Voice only[3]	None	All	All except database changes and user provisioning

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.
4. SAA = Speech Auto Attendant

Post-upgrade tasks:

1. Apply the third-party SSL Web Server Certificate to MiCollab and to the external MiVoice Border Gateways.
2. User desktop clients will be prompted to upgrade at their next log-in.
3. Mobile clients will not receive an upgrade prompt. You must change the user bundle for the new Mobile client, and explicitly re-send the Deployment e-mail to the mobile users.

   Users will install the new Mobile client from the Deployment e-mail. The old Mobile client will remain on their device until they delete it. It can be deleted in the same way as any other application on the device.

6. Upgrade external MiVoice Border Gateways (MBG) to Rls 9.4 PR3

This procedure upgrades all MiVoice Border Gateways except for the one included in MiCollab.

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

Upgrade MiVoice Border Gateway with Teleworker desk sets

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

Pre-upgrade tasks:

1. Full back-up

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

For large sites deploying separate Teleworker and SIP trunk MiVoice Border Gateway clusters; the clusters may be upgraded independently. Perform the upgrade procedure on each external MiVoice Border Gateway.

Table 12: 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[3,4]	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.
4. MiNet phones: devices may be load balanced in clusters that are not yet. Service may be affected due to lack of licenses and/or capacity limits.

Post-upgrade tasks:

1. Install a third-party SSL Web Server certificate, if one is not already present.
2. Using the option in the web server panel on MSL, export the certificate. Save it for installation on the MiContact Center Business server, For more detailed instructions, see “Deploy UCC OVAs (PaaS)” on page 52.

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

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

Note: The separate SDS synchronization step is not necessary when upgrading MiCloud 3.0/3.1 to 3.3. Synchronization is automatic after upgrade.

7. Upgrade MiVoice Business controllers to Rls 8.0 PR3

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

Pre-upgrade tasks:

- Full back-up of each MiVoice Business

Note: Upgrade secondary controllers before upgrading primary controllers.

Table 13: Upgrade MiVoice Business platform

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 (0.5 hours) Run MiCollab script (0.5 hours)	1.0 / MiVoice Business controller Depends on the number of users	1.0	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:

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

8. Upgrade MiContact Center Business to Rls 8.1 SP2

Primary resources:

- *MiContact Center Installation and Administration Guide*

Pre-upgrade tasks: Full back-up

There are three back-up methods. See Table 14 for details.

Table 14: MiContact Center Business back-up methods

BACK-UP METHOD	TIME TO PERFORM BACK-UP	DESCRIPTION/NOTES
VMware snapshot	5 mins	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.
VMware OVA back-up	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.
MiContact Center Business Client database backup	10 mins	From the MiContact Center Business Client, create an XML file of the Contact Center database. This is the most common method used in the Mitel test lab.

Table 15: Upgrade MiContact Center Business

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]
8.0	8.1 SP2	Back up	2.0	from minutes up to 2 hours	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.

9. Upgrade MiVoice Border Gateway Secure Recording Connector to Rls 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 16: Upgrade MiVoice Border Gateway Secure Recording Connectors

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	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: None

10. 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 17: Upgrade MiVoice Call Recording

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]
9.0 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

Upgrading MiCloud Business Virtual (SMB)

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

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

To upgrade from a release prior to MiVoice Business 3.1, see Table 18 for how to perform the complete upgrade.

Table 18: To Upgrade MiCloud Business Virtual (SMB) from Rls 2.0

IF DEPLOYMENT IS RESILIENT (CONTAINS MIVOICE BUSINESS REMOTE SURVIVABLE GATEWAYS)	
Upgrade from Rls 2.0 to Rls 3.1:	Follow the procedure in the *MiCloud Business Virtual Release 3.1 Deployment Guide*.
Upgrade from Rls 3.1 to Rls 3.3	Follow the upgrade instructions in this chapter.
IF DEPLOYMENT IS NOT RESILIENT (THERE ARE NO MIVOICE BUSINESS REMOTE SURVIVABLE GATEWAYS)	
Upgrade from Rls 2.0 to Release 3.3	Use the upgrade order in this guide to upgrade all of the products all the way from their Rls 2.0 versions to their Rls 3.3 versions.

Prerequisites

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

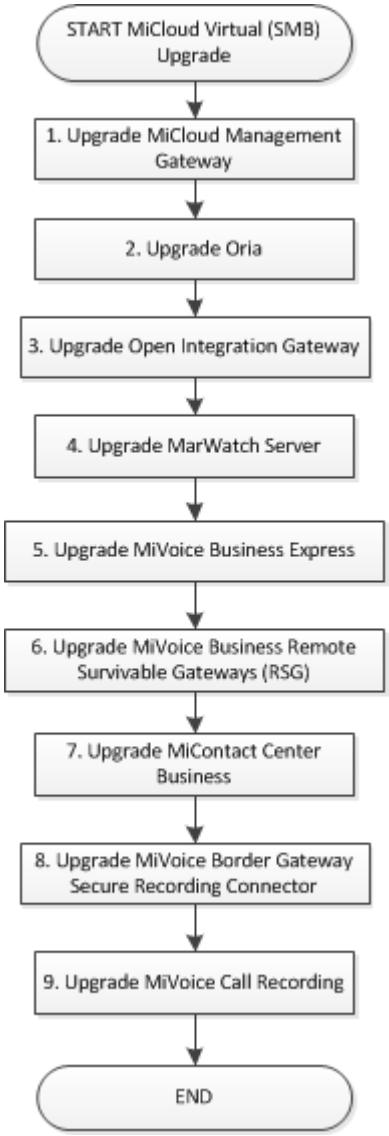
Note: Only one certificate is needed for both MiCollab and the MiVoice Border Gateway (MBG) if the embedded MBG in MiVoice Business Express is used as the Network edge MBG for Mobile Client connections.

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

Upgrade MiCloud Business Virtual (SMB) from Rls 3.0/3.1 to Rls 3.3

Follow these steps to upgrade MiCloud Business Virtual (SMB) 3.0/3.1 to 3.3.

Figure 5: Upgrading MiCloud SMB from MiCloud 3.0/3.1 to 3.3



1. Upgrade MiCloud Management Gateway (MMG) to Rls 5.0.6.0

Primary resources:

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

Pre-upgrade tasks: None

Table 19: Upgrade MiCloud Management 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[1]	USER[1]	ADMIN[1]
5.0	5.0.6.0		0.5	0.5	Al	No manage-ment services	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: Configure MiCloud Management Gateway interface. See MMG Online Help.

2. Upgrade Oria to Rls 5.3 SP1

Primary resource: *Oria Installation and Administration Guide*

Pre-upgrade tasks: Full back-up

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

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.

Table 20: Upgrade Oria

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[1]	USER[1]	ADMIN[1]
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

3. Upgrade Open Integration Gateway (OIG) to Rls 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 21: Upgrade Open Integration Gateway

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]
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 142
  - “Upgrade MiVoice Integration for Google” on page 143
- 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 22: Upgrade MiVoice Integration for Salesforce

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]
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 23: 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

4. Upgrade MarWatch Server to Mitel Performance Analytics (MPA) 2.1

Primary resource: *Mitel Performance Analytics 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 24: 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: None

5. Upgrade the MiVoice Business controllers (Remote Survivable Gateways) to Rls 8.0 PR3

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

Primary resource: *Mitel 3300 IP Communications Platform (ICP) Technician's Handbook* or *MiVoice Business Installation* and *MiVoice Business System Administration Tool Help*

Pre-upgrade tasks:

- Full back-up of each MiVoice Business

Note: Upgrade secondary controllers before upgrading primary controllers.

Table 25: Upgrade MiVoice Business (RSG)

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]
7.2 SP1	8.0 PR3	Back-up (0.5 hours) Run MiCollab script (0.5 hours)	1.0 / MiVoice Business controller Depends on the number of users	1.0	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:

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

6. Upgrade MiVoice Business Express to Rls 7.3 PR1

Primary resource: *MiVoice Business Express Deployment Guide*

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

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

Pre-upgrade tasks: A virtual machine (VM) back-up must be available.

LAN based desk sets will upgrade automatically. MiCollab desktop clients will prompt for upgrade when user logs in.

Table 26: Upgrade MiVoice Business Express

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 VM	1.0	0.5	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. Voice only through Remote Server Gateways; no Unified Communication features and no soft phones are available during upgrade. Teleworker phones and SIP phones are out of service.

Post-upgrade tasks:

1. Request third-party Web Server certificate if one has not previously been used. Apply the certificate to MiCollab.
2. Mobile clients will not receive an upgrade prompt. You must change the user bundle for the new Mobile client, and explicitly re-send the Deployment e-mail to the mobile users.

   Users will install the new Mobile client from the Deployment e-mail. The old Mobile client will remain on their device until they delete it. It can be deleted in the same way as any other application on the device.
3. On the MiVoice Border Gateway, use the following procedure to reset the MiNet devic-es.This triggers the Teleworker sets to upgrade their firmware. Hot Desk users may need to log in again.
   - Select **Service Configuration** > **Minet devices**.
   - Click **Bulk Edit**.
   - Click **Reset**.

7. Upgrade MiContact Center Business to Rls 8.1 SP2

Primary resources:

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

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

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

Pre-upgrade tasks: Full back-up

There are three back-up methods. See Table 27 for details.

Table 27: MiContact Center Business back-up methods

BACK-UP METHOD	TIME TO PERFORM BACK-UP (MINUTES)	DESCRIPTION/NOTES
VMware snapshot	5	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.
VMware OVA back-up	60	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.
MiContact Center Business Client database backup	10	From the MiContact Center Business Client, create an XML file of the Contact Center database. This is the most common method used in the Mitel test lab.

Table 28: Upgrade MiContact Center Business

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]
8.0	8.1 SP2	Back up	2.0	from minutes up to 2 hours	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: Upgrade desk top clients.

8. Upgrade MiVoice Border Gateway Secure Recording Connector to Rls 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 29: Upgrade MiVoice Border Gateway Secure Recording Connectors

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	9.4 PR3	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: None

9. Upgrade MiVoice Call Recording to Rls 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 30: Upgrade MiVoice Call Recording

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]
9.0 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

ACRONYM	TERM
GARID	Group Applications Record ID Group ARID Examples: Both ULM and DLM are types of GARID.
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
MiCloud Business Analytics	Real-time call analytics application, with services delivered via the cloud.
MLB	Medium-Large Business - One of the MiCloud architectures. Now c.alled the Virtual architecture
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).
SB	Small Business - One of the MiCloud architectures. Now referred to as the Multi-instance architecture.
SMB	Small-Medium Business - One of the MiCloud architectures. Now referred to as one of the Virtual 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.
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

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 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 the 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 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.