MITEL

Unified Communications & Collaboration Virtual Appliance

Deployment Guide
Release 5.0 SP1

MITEL®
Simply Communicating®

NOTICE

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

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

Trademarks

Mitel and Mitel Applications Suite are trademarks of Mitel Networks Corporation.

Windows and Microsoft are trademarks of Microsoft Corporation.

Dell is a trademark of Dell Inc.

PowerEdge is a trademark of Dell Inc.

VMware, VMware vMotion, VMware vCloud, VMware vSphere, VMware vCenter, ESX, and ESXi are trademarks of VMware Incorporated.

Google and the Google logo are registered trademarks of Google Inc.

Chrome is a trademark of Google Inc.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

UCC Virtual Appliance Deployment Guide
Release 5.0 SP1
December 2013

®,™ Trademark of Mitel Networks Corporation
© Copyright 2013, Mitel Networks Corporation
All rights reserved

Chapter 1: Introduction

Chapter 2: Description

Chapter 3: Plan Customer Site

Chapter 4: Deploy UCC Virtual Appliance

Chapter 5: Configure System

Chapter 6: Maintain

Chapter 7: Troubleshoot

Appendix A : System Defaults

Appendix B : VMware Support for vUCC

Chapter 1

Introduction

Purpose of This Guide

This guide provides instructions on how to deploy the Mitel® Unified Communications and Collaboration Virtual Appliance (vUCC) software on VMware vSphere. It covers the following topics:

- Plan Customer Site
- Deploy UCC Virtual Appliance
- Configure System
- Maintenance, and
- Troubleshooting.

Intended Audience

This guide is intended primarily for

- service providers who host vUCC in a data center and provide it as a software solution to customers
- data center providers who host the VMware infrastructure on which the vUCC resides
- dealers who deploy, configure, provision, and maintain the vUCC solution
- customers who choose to deploy the VMware infrastructure and then allow a dealer to deploy, configure, provision, and maintain the vUCC solution.

Service providers, dealers, and customers who use this document must have successfully completed the required Mitel vUCC Deployment Training.

In addition, service providers must have the ability to

- configure and manage a data center infrastructure
- deploy and support VMware products.

Note: This document does not describe management tools that Service providers might use or offer to resellers to manage their infrastructure.

Roles and Tasks

The tasks that you perform during a vUCC deployment depend on your role (solution provider, data center provider, dealer, or customer) and the deployment model (Software as a Service, Infrastructure as a Service, or customer premise equipment). Use the following table as a general guideline to help you identify your responsibilities.

Table 1: vUCC Roles and Tasks

Task/Deployment	Software as a Service (Saas)	Infrastructure as a Service (Iaas)	Customer Premise Equipment (CPE)
Set up vCenter vSphere environment (page 39)	Service provider	Data center provider	VMware dealer or customer
Plan site (page 27)	Service provider	Dealer	Dealer
Deploy virtual appliance (page 47)	Service provider	Dealer or Service provider	Customer
Run configuration wizard (page 76)	Service provider	Dealer or Service provider	Dealer
Initial user provisioning (page 90)	Service provider	Dealer	Dealer
Perform advanced configuration (page 90)	Service provider	Dealer	Dealer
Perform backups (page 115)	Service provider	Dealer	Dealer or customer administrator
Configure optional standalone vMBGs (page 101)	Service provider	Dealer	Dealer
Install phones and train users	Service provider	Dealer	Dealer
Perform user administration (adds, edits, and deletes) from the MAS Users and Services application	Service provider or customer administrator	Dealer or customer administrator	Dealer or customer admin st rat or
Perform maintenance (page 111)	Service provider	Dealer	Dealer

About the Documentation Set

Mitel vUCC

- *vUCC Deployment Guide* (this guide) provides installation instructions for the MAS software and for the supported applications.
- *MAS and vUCC Engineering Guidelines* provides deployment models, limitations and constraints, and performance capacities for the vUCC solution.
- *Virtual Appliance Deployment Solutions Guide* provides guidelines for deploying Mitel Virtual Appliances and applications in a VMware virtual infrastructure.
- *Mitel Collaboration Advanced Configuration and Maintenance Manual* provides configuration and maintenance procedures for the MCA application.

Mitel MCD Communications Platform

- *MCD System Administration Tool Online Help* provides instructions on how to configure and program the Mitel Communications Director communications platform.

Mitel Applications Suite

Administrator

- *Server Manager help* provides configuration, administration, and maintenance procedures for the MAS server.
- *Users and Services help* provides instructions on how to manage user data (adds, edits, and deletes) and assign or remove user services, such as Mitel Border Gateway or Teleworker.
- *NuPoint Unified Messaging help* provides system administrators instructions on how to configure and maintain NuPoint Unified Messaging functionality through the web console interface.
- *Mitel Collaboration Advanced help* provides instructions on how to provision the MCA application.

End User

- *My Unified Communications Online Help* provides you with instructions on how to configure your portal settings and use the communication applications.
- *Mitel Collaboration Advanced Quick Reference Guide* provides procedures on how to set up and use the conferencing features.

NuPoint Unified Messaging

- *NuPoint Unified Messaging User Guide* describes how to use the voice mail system.
- *Nupoint Unified Messaging Mitel TUI Quick Reference Guide* provides a summary of basic user options and procedures for the Mitel TUI.

Mitel Border Gateway (Teleworker)

- *Engineering Guidelines:* provides Firewall configuration information.
- *Installation and Maintenance Guide with Web Proxy* describes the installation requirements and provides installation instructions for the MBG server.

Unified Communications Advanced (UCA)

- *Administrator Guide* provides instructions on how to configure UCA on Mitel Communications Platforms.
- *Administrator Portal Online Help* provides information and instructions for the UC Server administrator interface.

Mitel Standard Linux

- *Mitel Standard Linux Installation and Administration Guide* provides installation and administration information for the MSL operating system.

User Documentation

- Download end-user documentation for Mitel phones, softphone clients, and applications from the **End-User** screen on the Mitel Customer documentation site.

Phone Installation Guides

- Download phone installation guides from the Mitel Customer documentation site.

Accessing Documentation

Mitel Product Documentation

To access Mitel product documentation:

1. Log on to Mitel OnLine.
2. Click **Support** and then click **Product Documentation**.
3. Click **Applications** and then click **Mitel Applications Suite**.

Mitel Knowledge Base Articles

To access Mitel Knowledge Base articles:

1. Log on to Mitel OnLine.
2. Click **Technical** and then click **Knowledge Base**. The Knowledge Base search engine opens.
3. From the Product list, select your application name and click **Search**.

Product Bulletins

To access Mitel Product Bulletins:

1. Log on to Mitel OnLine.
2. Click **Sales** and then click **Bulletins**.
3. Click the link to access a list of product bulletins.

Glossary

Abbreviation	Term	Description
ACD	Automated Call Distribution	An telephone system application that manages incoming calls based on the called number. ACD is used to validate callers, make outgoing responses or calls, forward calls, allow callers to record messages, gather usage statistics, and balance phone line usage.
ACD Traditional Agent	Automated Call Distribution Traditional Agent	A traditional ACD agent is identified by an Agent ID that is programmed in the ACD Agent IDs form. When a traditional ACD agent logs into an ACD set, only the Class of Service (COS) and Class of Restriction (COR) that are associated with the agent's directory number are applied to the ACD set.
ARID	Application Record ID	A unique number in the MSL operating system of the UCC virtual appliance that identifies vUCC to the Application Manager Center. The system's ARID specifies a set of licenses on the AMC. The ARID allows MSL to obtain the license bundle from the Application Management Center and apply it to the vUCC system.
Authorized Partner		Dealers, resellers, and solutions providers who are authorized by Mitel to sell and service Mitel products and solutions.
CAPEX	Capital Expenditure	Funds used by a company to acquire or upgrade assets such as property, equipment, or software licenses (as in the case of the vUCC product). vUCC CAPEX licensing is used with SaaS deployment models where user licenses are purchased as a capital expense and not on a subscription basis.
Cloning	Cloning a VMware template means to create a copy of it.	
CPE	Customer Premise Equipment	Mitel vUCC certified dealers install and configure the UCC virtual appliance in the VMware environment on the customer's premise.
DID	Direct Inward Dial	Also known as Direct Dialing Inwards (DDI). Allows an external caller to dial an internal extension without having to go through an attendant or operator.
DRS	Dynamic Resource Scheduler	A VMware feature allowing dynamic load sharing across hosts within a vSphere cluster.

Abbreviation	Term	Description
EHDU	External Hot Desk User	External Hot Desking extends hot desking capabilities to an external device, which makes it appear as an extension on the system. When the external hot desk user (EHDU) is logged in to the MCD, a caller only needs to dial the extension number assigned to the user and the system automatically rings the user's cell phone, home phone or other device of choice—including an extension on another private network or PBX.
ESXi	Hypervisor for VMware.	A virtualization layer that runs directly on the server hardware. Provides processor, memory, storage, and networking resources on multiple virtual appliances.
Hot Desk ACD Agent	Hot Desk Automated Call Distribution Agent	A hot desk ACD agent can log into any hot desk enabled set and the system will apply the agent's personal phone profile to that set. After the agent logs into the set, the agent has access to his or her own personal speed calls, features, and phone settings. If you use hot desk ACD agents in a call center, you do not have to provide agents with their own separate phones for their personal use.
Hot Desking	Allows a number of users to share one or more phones. Hot desking is ideal for telecommuters, sales agents, and other employees who spend only part of their time in the office. With hot desking, a company does not have to provide a dedicated phone for each of these employees. Instead, the company can make a pool of shared phones available on a first-come, first-served basis. A hot desk user can to log in to any available hot desk-enabled phone on the system. After a user logs into a hot desk phone, the system applies the user's profile to the phone and it functions as the user's desk phone.	
Hypervisor	A platform that allows multiple operating systems to run on a host computer at the same time.	
IaaS	Infrastructure as a Service	Infrastructure providers rent out the resources (for example: vCPU, GHz, RAM, HDD, ports and so forth) on their VMware vSphere Shared Infrastructure that are required to host the vUCC solution.
IDS	Integrated Directory Services	Allows you to integrate the user database of a corporate directory service with the vUCC user database to minimize data entry and administration. The user data on the corporate directory server is synchronized with the vUCC database using Lightweight Directory Access Protocol (LDAP). If single point provisioning is enabled, then the system distributes the user data to the vMCD.
Initial Configuration Wizard		A configuration wizard that guides you through the initial configuration of the vUCC system.
MAS	Mitel Applications Suite	Software solution that manages Mitel applications.

Abbreviation	Term	Description
MBG	Mitel Border Gateway	Formerly know as the Multi-Protocol Border Gateway. MBG is a platform for the secure deployment of multiple services in a variety of network configurations. MBG provides the following services: • **Teleworking**: remote MiNET and SIP access ("Teleworker") for IP phones on Mitel Communications Director (MCD) platforms; Nat traversal for tenant offices for the Multi-instance Communications Director (MiCD) application. • **Secure call recording**: call recording solution that allows third-party recording equipment to record Mitel encrypted voice streams. • **SIP trunking**: SIP trunking from an internal MCD platform to external third-party SIP providers • **Web proxy**: a reverse proxy that provides access to hosts on a corporate LAN for clients on the Internet
MCA	Mitel Collaboration Advanced	Software solution that provides conferencing and collaboration services using a Web-based browser.
MCD	Mitel Communications Director	Mitel Communications Director (MCD) is the voice over IP call-processing software that runs as a virtual appliance within the VMware environment.
MKB	Mitel Knowledge Base	A collection of Mitel technical bulletins that provide support information on wide a variety of installation, configuration, maintenance and troubleshooting topics. The Mitel Knowledge Base is accessible through Mitel Online. You need a Mitel Online account and password in order to access the database.
MICW	Mitel Integrated Configuration Wizard	A software tool that performs initial system setup of the MCD system and MAS applications. Do not confuse this tool with the Initial Configuration Wizard that is used with the vUCC.
MPLS	Multi protocol Label Switching	MPLS directs telecommunications data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in routing tables. It integrates Layer 2 information about network links into Layer 3 (IP) information within a particular an Internet Service Provider network to simplify IP data exchange.
MOL	Mitel Online	Mitel’s web site for customers, resellers, dealers, technicians and support personnel. You must register with Mitel to obtain an Mitel Online account and password in order to access this site.The site provides information, sales tools, technical support, customer documentation, training, and so forth for Mitel products.
MSL	Mitel Standard Linux	The operating system that supports MAS software; along with Mitel SDK components, it comprises a base for all MAS applications.
My UC Portal	My Unified Communications Portal	A MAS end-user web portal that allows users to • control their general settings: password, TUI personal identification number, and preferred language • access their application settings, such as voicemail, call director, and Mitel Collaboration Advanced.

Abbreviation	Term	Description
NP-UM	NuPoint Unified Messaging	Mitel’s voice mail application
Oria	Oria System Management & Customer Self-Service Portal	A system management and customer self-service application that allows a service provider to manage and deploy hosted Mitel voice services for their customers. At the same time, Oria allows a service provider to offer each of their customers an administration and self-service portal to make site specific user adds, edits, and deletes. Oria offers three tiers or levels of control: • System Configuration & Administration • Site Administration & Self-Service • End User Self-Service
OVA	Open Virtual Format Archive	A packaging format for virtual appliances that allows them to be distributed. It is a single tar ball of the OVF directory and files.
OVF	Open Virtualization Format	A distribution format for virtual appliances that uses existing packaging tools to combine one or more virtual machines with a standards-based XML wrapper. OVF gives the virtualization platform a portable package containing all required installation and configuration parameters for virtual machines. This format allows any virtualization platform that implements the standard to correctly install and run virtual appliances.
RAD	Recording Announce Device	A device which automatically answers a call and delivers a pre-recorded message. RAD is often used to inform a caller that they are in a queue and their call will be dealt in due order.
SAA	Speech Auto Attendant	A speech-enabled application allows users to place calls to people quickly and efficiently by speaking their names. Typically, you say the name of the person you want to speak to and the system transfers your call to the requested party. In addition to placing calls by name, users can say a department name or telephone number. A tutorial introduces users to the system features, and voice-based help is available to answer questions.
SaaS	Software as a Service	Service Providers host the vUCC solution as a software application within a VMware vSphere Shared Server Infrastructure and offer it to customers as a service.
SAS	Suite Applications Services	This application provides single-point user services provisioning and centralized management of shared system resources for all the MAS applications. This application also provides the My Unified Communications web portal.
SIP	Session Internet Protocol	An ASCII-character-based signaling protocol designed for real-time transmission using Voice over IP (VoIP). SIP is a streamlined protocol, developed specifically for IP telephony. Using SIP, programmers can add new fragments of information to messages without compromising connections.
SP	Service Provider	A company that provides customers with communications, data storage, computer processing, or application services. SIP trunking or internet access are examples of typical communications services. Service Providers can be Mitel Authorized Partners who provide Mitel communications solutions to end customers as services.

Abbreviation	Term	Description
SRC	Secure Recording Connector	Formerly a standalone Mitel call recording product, SRC is now incorporated in the MBG software.
TTS	Text -to-Speech	Enables Advanced Unified Messaging users to listen to their email messages from their NP-UM voice mailbox. The text of the email message is converted to speech and played back over the phone. Emails that are heard through the Telephone User Interface (TUI) are marked as read (played) in the user's email inbox.TTS is only available with the Advanced Unified Messaging feature.
TW	Teleworker	Software that connects a remote office to the corporate voice network to provide full access to voice mail, conferencing and all the other features of the office phone system.
UC Advanced (UCA)	Unified Communicator Advanced	Software solution that provides clients (UCA deskphone users or UCA softphone users) with a single access point for communication and collaboration needs. It converges the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications
UCA Integration Wizard	Unified Communicator Advanced Integration Wizard	A software application (wizard) that integrates UCA user and phone data with the MAS USP data (see UCA Integrated Mode). Note that for vUCC, UCA is configured in integrated mode.
UCA Integrated Mode	Unified Communicator Advanced Integrated Mode	In this mode, the MAS system keeps the Users and Services database and UCA database synchronized so they function like a single database on the MAS server. It allows you to provision UCA services from the MAS Users and Services application and supports single point provisioning of the UCA services on the MCD platform(s). This is the recommended mode for sites that meet the integration requirements. Note that for vUCC, UCA is automatically set in integrated mode by the Initial Configuration Wizard.
UCA Co-located Mode	Unified Communicator Advanced Co-Located Mode	In this mode, the Users and Services data and UCA data are contained in separate, independent databases on the MAS server. This mode is supported for sites with either MCD or 5000 CP platforms. With this mode, you must provision UCA services separately from the UCA Server Application interface. Single point provisioning of UCA services is not supported. UCA Co-located Mode is not supported for vUCC.
UM	Unified Messaging	An application that provides NP-UM users with email notification of their voicemail messages.
USP	User and Services	MAS application for provisioning users and services on the vUCC system.
vApp	Virtual Appliance	VMware term that describes a solution that contains multiple virtual machines configured to work together for a cloud environment and packaged as an OVF.
vCenter	vSphere vCenter Server	VMware management server that provides a centralized platform for managing virtual infrastructure.

Abbreviation	Term	Description
vCloud Director		A cloud computing initiative from VMware that allows customers to migrate work on demand from their "internal cloud" of cooperating VMware hypervisors to a remote cloud of VMware hypervisors. The goal of the initiative is to provide the power of cloud computing with the flexibility allowed by virtualization.
VM	Virtual Machine	Virtual machines allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system. The software layer providing the virtualization is called a hypervisor. A hypervisor can run on bare hardware (Type 1 or native VM) or on top of an operating system (Type 2 or hosted VM).
vMBG	Virtual Mitel Border Gateway	MBG running as a virtual application (vApp) within the VMware vSphere environment.
vMCD	Virtual Mitel Communications Director	MCD running as a virtual application (vApp) within the VMware vSphere environment.
vMAS	Virtual Mitel Applications Suite	MAS running as a virtual application (vApp) within the VMware vSphere environment.
VOIP	Voice over IP	VoIP technology, also known as IP Telephony, is the technology used to deliver telephony over a data network instead of using the standard public switched telephone network. VoIP means that voice is converted from an analogue signal, encoded digitally, and then converted into packets. It then uses a data network to move those packets along the most efficient path to their destination, where they are reassembled and delivered and converted back into a voice transmission.
vSphere	VMware Cloud Operating System	Cloud computing is Internet-based computing. VMware’s Cloud Operating system provides software resources and information to computers and other devices on-demand over the Internet.
vSphere Standalone	VMware vSphere deployed as a standalone ESX/ESXi host.	
vSphere Managed	VMware vSphere deployed as a vCenter Server “managed” environment with ESX/ESXi hosts.	
vUCC	Unified Communication and Collaboration Virtual Appliance	Mitel communications solution for small to medium business that runs as virtual appliance on a VMware vSphere or vCloud Director infrastructure.

Chapter 2

Description

About the UCC Virtual Appliance

The Mitel® Unified Communications and Collaboration Virtual Appliance (vUCC) provides a complete communications solution for small to medium businesses. vUCC runs as virtual appliance on a VMware vSphere infrastructure.

Components

The vUCC consists of the following components:

- *Mitel Communications Director*: provides Voice over IP (VoIP) telephony support for Mitel IP phones, SIP trunking, and a wide range of phone features.
- *Mitel Applications Suite*: provides the Server Manager interface for system administration and the following applications:
  - *Users and Services*: for provisioning users and their services.
  - *NuPoint Unified Messaging*: provides voice messaging, unified messaging and speech auto attendant
  - *Unified Communications Advanced*: combines the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications
  - *Mitel Collaboration Advanced*: allows users to collaborate in real time, give presentations, and conduct interactive online meetings
- *Mitel Border Gateway*: provides teleworker service and secure recording connector for the remote Teleworker sets only.
- *Initial Configuration Wizard*: guides you through the initial configuration of the vUCC system.

Figure 1 is a block diagram of the main components:

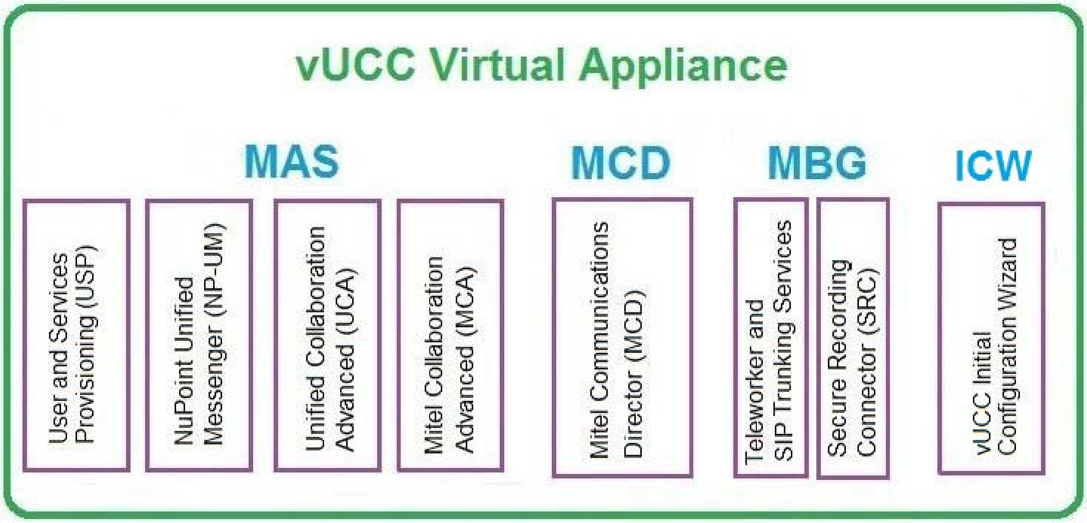

vUCC Virtual Appliance
MAS
MCD
MBG
ICW
User and Services Provisioning (USP)
NuPoint Unified Messenger (NP-UM)
Unified Collaboration Advanced (UCA)
Mitel Collaboration Advanced (MCA)
Mitel Communications Director (MCD)
Teleworker and SIP Trunking Services
Secure Recording Connector (SRC)
vUCC Initial Configuration Wizard

Figure 1: vUCC Components

Characteristics

vUCC has the following characteristics:

- Supports up to 250 users with a license mix of 25% Entry, 50% Standard, 25% Premium. A maximum of 150 Premium users are supported.
- All applications are installed from the vUCC OVA.
- Employs an initial configuration wizard and system default settings to simplify installation and minimize initial system configuration.
- Provides single point of user provisioning to the MCD and applications from MAS.
- Minimizes user provisioning through Bulk data import and the application of roles and templates
- Integrates with Active Directory (supports the addition and deletion of users from Active Directory)
- Supports a subset of VMware vSphere, vCenter, and vCloud Director management tools. See “VMware Support for vUCC” on page 159 for details.

Deployment Models

This solution is well-adapted to the following deployments:

- **Unified Communications as a Service (UCaaS)**: Service Providers host the vUCC solution as a software application within a VMware vSphere Shared Server Infrastructure and offer it to customers as a service.
- **Infrastructure as a Service (IaaS)**: Infrastructure providers rent out the resources (for example: vCPU, GHz, RAM, HDD, ports and so forth) required to host the vUCC solution on their VMware vSphere Shared Infrastructure.
- **Customer Premise Deployment**: Mitel certified dealers install and configure vUCC in the VMware environment on the customer’s premise.

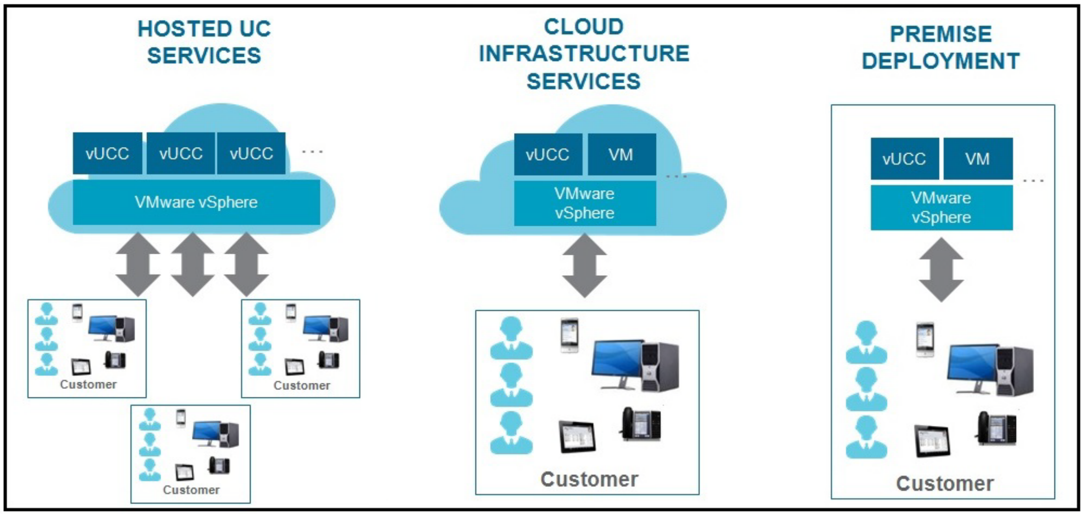


Figure 2: vUCC Deployment Models

Depending on the deployment model and site requirements, you deploy vUCC in server gateway mode

- by itself with the integrated MBG used for Teleworker and SIP trunking.
- with a standalone vMBG that provides SIP trunk proxy.
- with a third-party SBC/gateway for SIP trunk interconnect to the service provider.

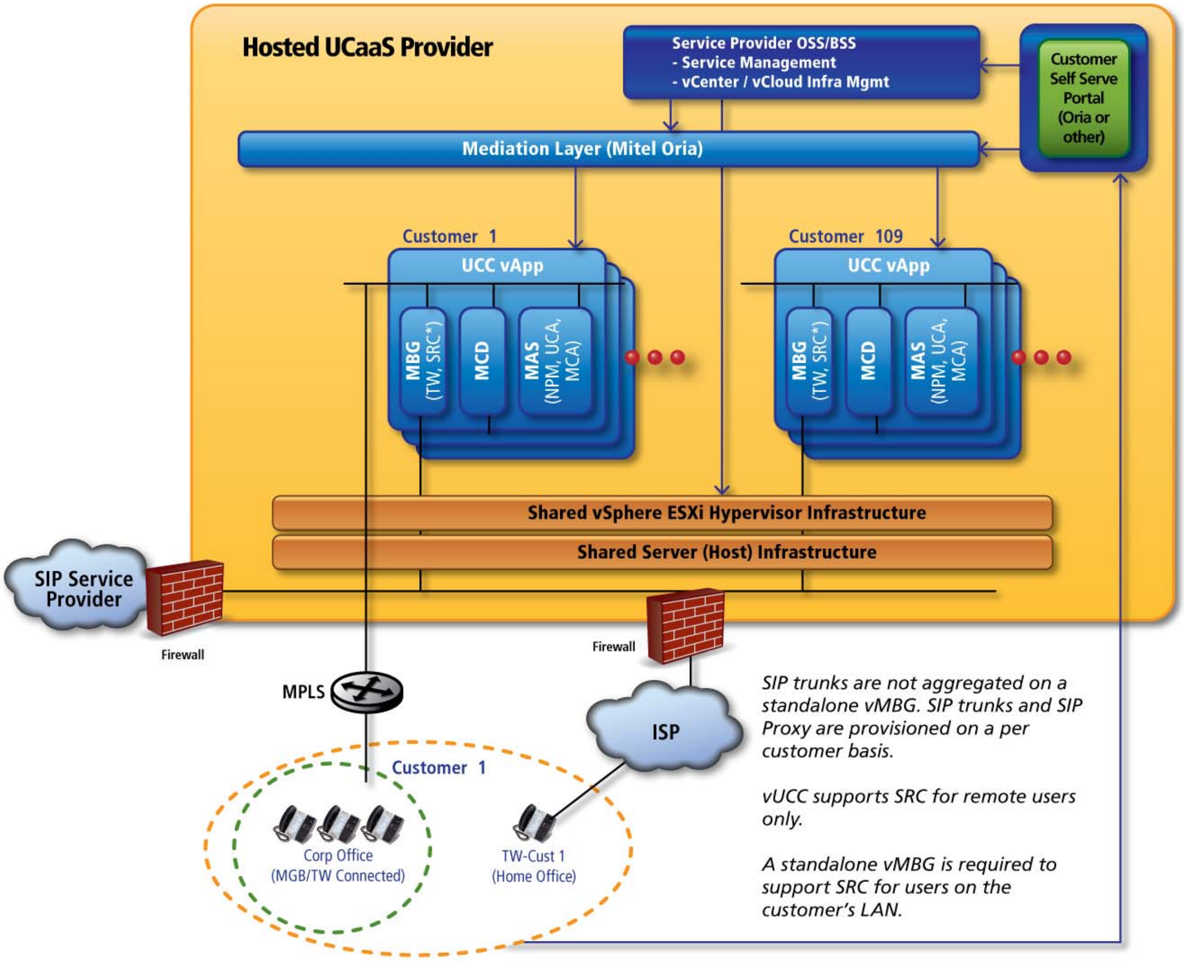
Note: To support Secure Recording Connector for phones on the LAN, you must deploy a separate vMBG on the LAN (preferably on the same LAN segment as vUCC). The SRC component within vUCC can only be used to record calls on remote Teleworker sets.

UCaaS Deployment

Figure 3 shows the vUCC and VMware components in a typical UCaaS deployment. In this deployment model:

- vUCC is deployed as a single virtual appliance that provides MAS, MCD, and MBG functionality. The MBG component of vUCC provides the firewall, router, MCA Web Proxy, and Secure Recording Connector of remote Teleworker sets. It also acts as the main hub for the remote Teleworker sets.
- The hosted UCaaS service provider deploys and maintains the vUCC solution. If the service provider deploys a management solution with a customer self-serve portal, then the end customer’s IT administrator can manage their users directly.
- For UCaaS deployments, the vUCC software bundle and user licenses can be licensed on a subscription basis from Mitel or purchased as a capital expense (CAPEX).
- Two distinct network connectivity models are supported from the end customer premise to the hosted UCaaS infrastructure:
  - **MPLS Connected End Customer(s)**: vUCC connected to a remote office using an MPLS router.
  - **Public Internet Connected End Customer(s)**: standalone vUCC servicing Telworker phones in one or multiple remote offices.
- UCaaS deployments typically use the on-board MBG to provide the SIP trunking proxy. However, a separate external standalone vMGB can be added to provide SIP trunking resources. Adding an external standalone vMBG has the following advantages:
  - consolidates trunking capacity for multiple customers; all trunks come to one location and the incoming calls are routed to the appropriate customer's vUCC.
  - increased simplicity for bandwidth management
  - cost savings when SIP services are purchased in bulk
  - the ability to configure trunk resiliency for disaster recovery.
- There are two routable networks in this deployment configuration:
  - On the LAN side, the MAS, MCD, and MBG components within the vUCC communicate with each other. The vUCC MBG communicates with the teleworker phones in the internet over an MPLS router.
  - On the WAN side, the standalone vMBG functions as a SIP trunk proxy.

Note: This deployment model is available from Mitel as part of the Mitel Authorized Partner Service Provider Addendum. It can be commercially licensed under Subscription or CAPEX pricing from Mitel.

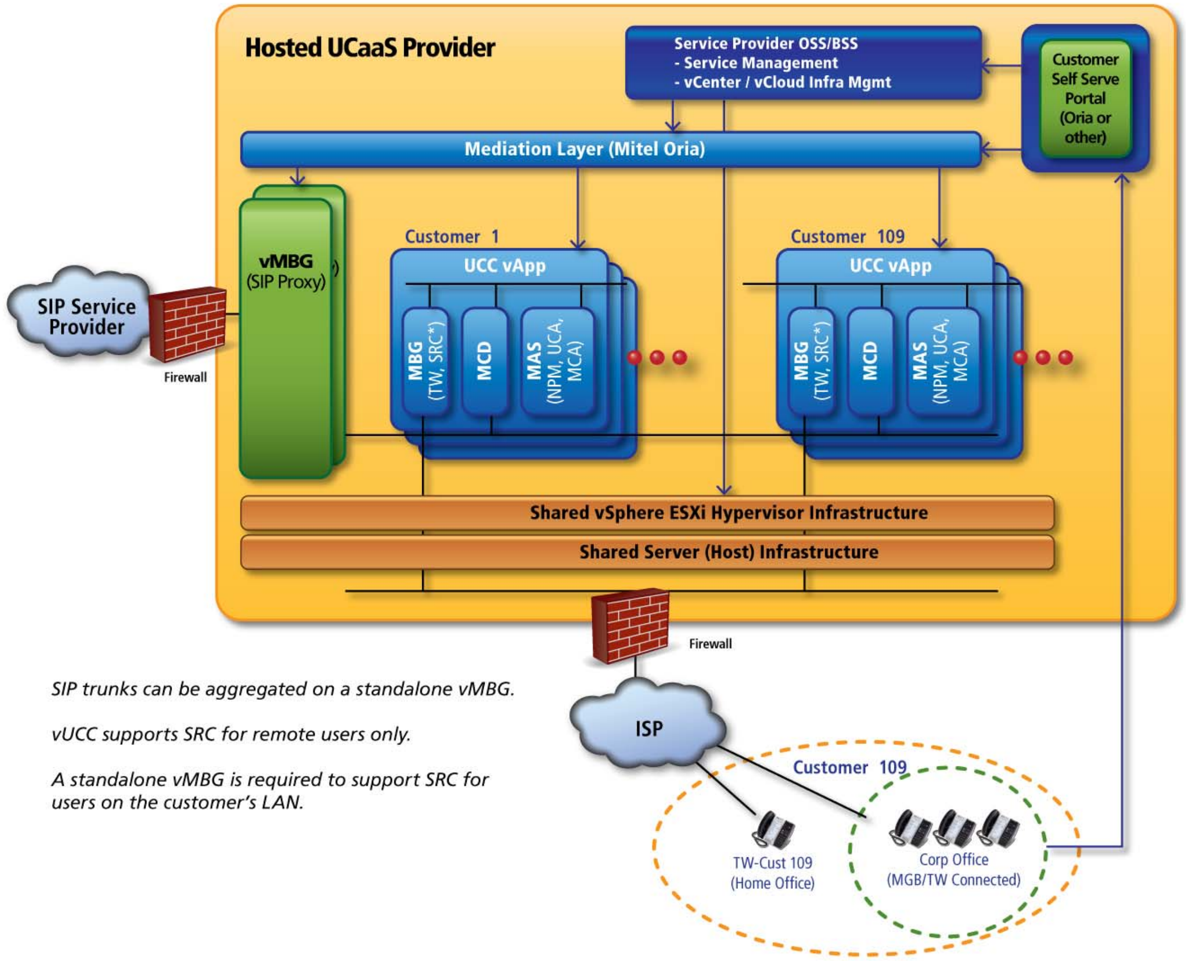


SIP trunks are not aggregated on a standalone vMBG. SIP trunks and SIP Proxy are provisioned on a per customer basis.

vUCC supports SRC for remote users only.

A standalone vMBG is required to support SRC for users on the customer's LAN.

Figure 3: UCaaS Infrastructure: MPLS Connected End Customer(s)



SIP trunks can be aggregated on a standalone vMBG.

vUCC supports SRC for remote users only.

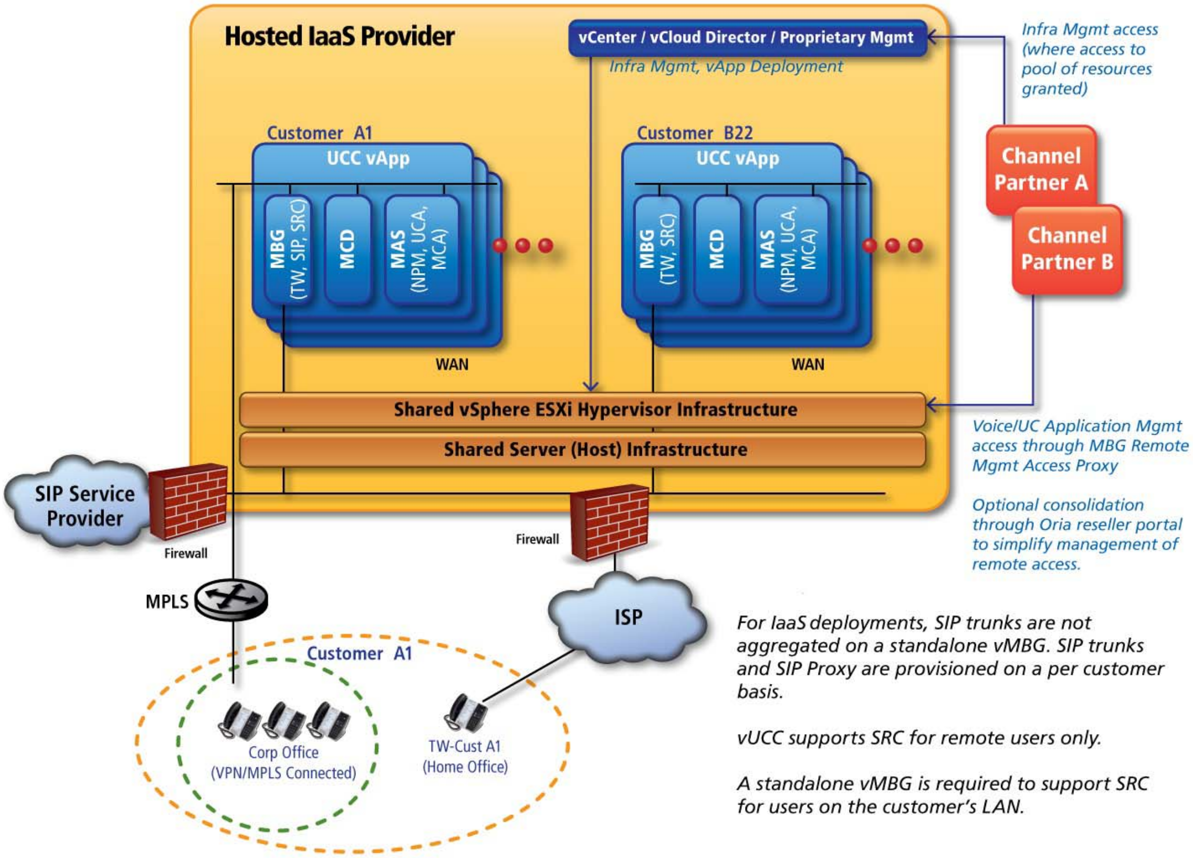
A standalone vMBG is required to support SRC for users on the customer's LAN.

Figure 4: UCaaS Infrastructure: Public Internet Connected End Customer(s)

IAAS Deployment

Figure 5 shows the vUCC and VMware components in a typical IaaS deployment. In this deployment model:

- vUCC is deployed as a single virtual appliance that provides MCD, MAS, and MBG functionality. The MBG component of each vUCC provides a SIP proxy to the SIP Service provider.
- The service provider maintains the infrastructure and a channel partner deploys and maintains the vUCC solution. The channel partner may, or may not, have access to the hosted infrastructure.
- Two distinct network connectivity models are supported from the end-customer premise to the hosted UCaaS infrastructure:
  - **MPLS Connected End Customer(s)**: vUCC connected to a remote office using an MPLS router.
  - **Public Internet Connected End Customer(s)**: standalone vUCC servicing Telworker phones in one or multiple remote offices.



Infra Mgmt access (where access to pool of resources granted)

Voice/UC Application Mgmt access through MBG Remote Mgmt Access Proxy

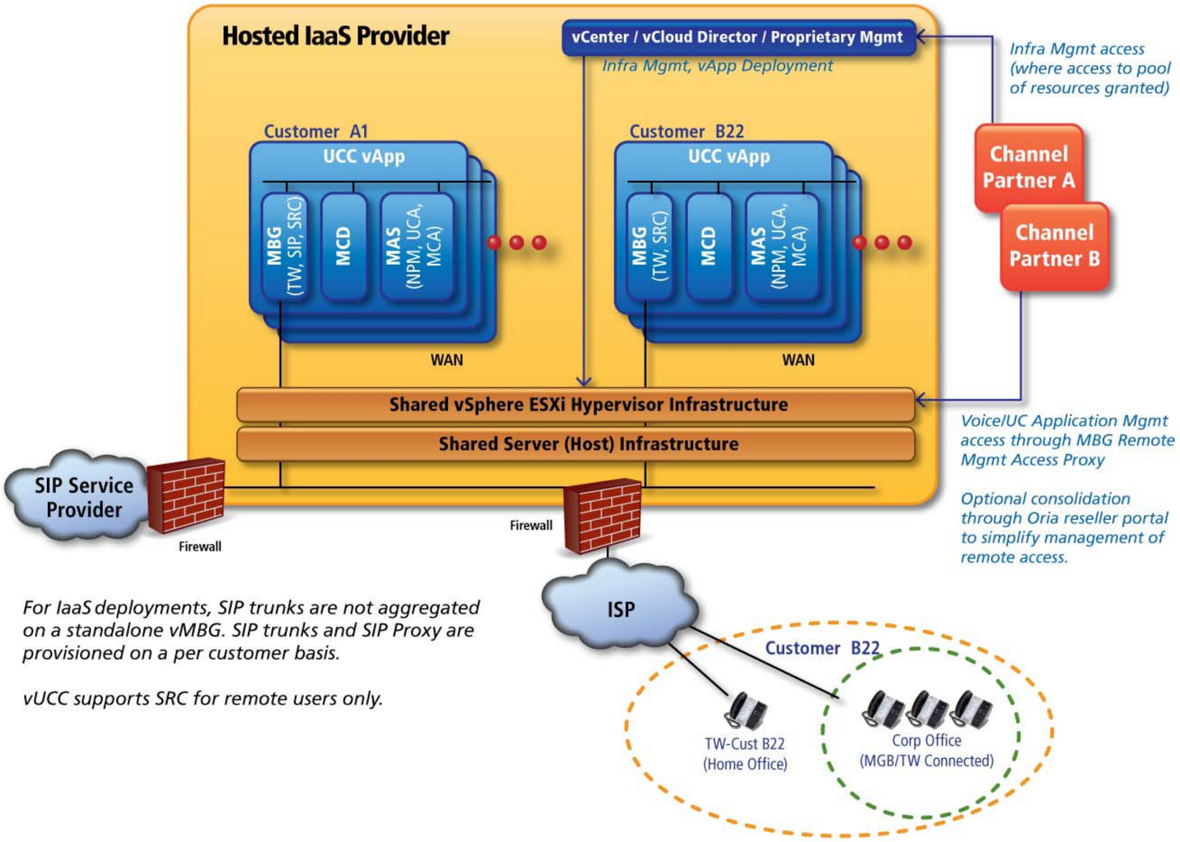
Optional consolidation through Oria reseller portal to simplify management of remote access.

For IaaS deployments, SIP trunks are not aggregated on a standalone vMBG. SIP trunks and SIP Proxy are provisioned on a per customer basis.

vUCC supports SRC for remote users only.

A standalone vMBG is required to support SRC for users on the customer's LAN.

Figure 5: Example IaaS MPLS Connected End Customers



Infra Mgmt access (where access to pool of resources granted)

Voice/UC Application Mgmt access through MBG Remote Mgmt Access Proxy

Optional consolidation through Oria reseller portal to simplify management of remote access.

For IaaS deployments, SIP trunks are not aggregated on a standalone vMBG. SIP trunks and SIP Proxy are provisioned on a per customer basis.

vUCC supports SRC for remote users only.

Figure 6: IaaS Infrastructure: Public Internet Connected End Customer(s)

CPE Deployment

Figure 7 shows the vUCC and VMware components in a typical Customer Premise Equipment (CPE) deployment. In this deployment model:

- vUCC is deployed as a single virtual appliance that provides MCD, MAS, and MBG functionality.
- The UCC vApp MBG application provides SIP trunking support. A separate, optional external standalone vMGB can be added for SIP trunking.
- CPE deployments typically use the on-board MBG in the vUCC to provide the SIP Proxy. However, a separate, optional external vMBG can also be used.
- Customers use the vUCC solution and can perform user self-provisioning through the vUCC administration tools (MAS server manager).

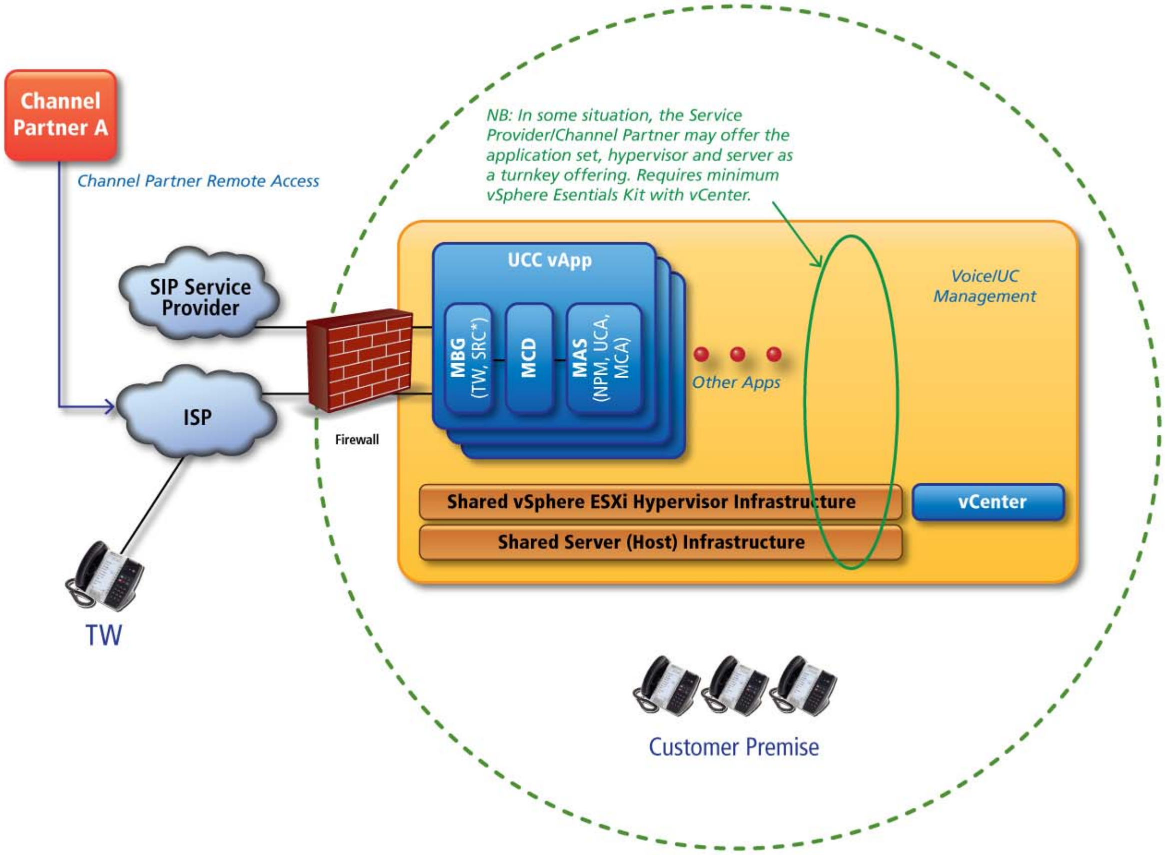

Channel Partner A
Channel Partner Remote Access
NB: In some situation, the Service Provider/Channel Partner may offer the application set, hypervisor and server as a turnkey offering. Requires minimum vSphere Esentials Kit with vCenter.
SIP Service Provider
ISP
Firewall
UCC vApp
MBG (TW, SRC*)
MCD
MAS (NPM, UCA, MCA)
Other Apps
Voice/UC Management
Shared vSphere ESXi Hypervisor Infrastructure
vCenter
Shared Server (Host) Infrastructure
TW
Customer Premise

Figure 7: Customer Premise Equipment Deployment

Supported Functionality

Overview

vUCC supports the following:

- Applications Suite Management
  - Central point of management for applications
  - User and services provisioning
  - Single point of user provisioning
  - Active Directory integration
- Mitel Communications Director voice over IP telephony platform, including
  - IP Phone features
  - SIP trunking
  - Automatic Call Distribution (ACD) and ACD Express
- NuPoint Unified Messenger voicemail application
  - Voicemail,
  - Standard UM and Advanced UM
  - Auto Attendant, Inbound and Outbound FAX, Record-A-Call, Call Director, Miscellaneous Options (NP Page, Forms, On Demand, Rapid Dial)
- Unified Communications Advanced
  - Desktop client with optional softphone
  - Web and mobile client support for audio, video, and instant messaging collaboration
  - Collaboration features
  - ACD agent
  - Console
- Mitel Collaboration Advanced
  - Audio, video, and web collaboration
  - Desktop/application collaboration
- Mitel Border Gateway, providing
  - Teleworker Service
  - Secure Recording Connector (for remote Teleworkers only)
  - SIP Trunking Proxy
- Initial Configuration Wizard

Note: Speech applications are not supported (MCD embedded voicemail, Speech Auto Attendant, Text to Speech, Speech to Text, Speech Navigation, or Network Voicemail).

Applications Suite Management

The MAS administration interface allows administrators to configure system settings for all the applications. Common data elements are shared among the applications, reducing both the need for duplicate entry and the possibility for error.

The administrator uses the Users and Services Provisioning application to add, edit, or delete user data and to modify users' application settings. This application significantly reduces administration costs.

The MAS My Unified Communications portal is a web-based interface that gives end users a single point of access to all their applications. The portal allows users to

- set personal settings, such as passwords and phone numbers
- configure and maintain their communication application settings.

Mitel Communications Director

Mitel Communications Director is a feature-rich communications system that provides IP-PBX capability plus a range of embedded applications, such as auto-attendant, hot desking, multimedia collaboration, and unified messaging. It provides seamless IP networking and SIP trunking.

Mitel Communications Director software has over 500 telephony features – features that are provided to users through easy-to-use phones and web-based user desktop interfaces. It also supports a wide-range of desktop devices, including entry-level IP phones, web-enabled IP devices, wireless handsets (WiFi or IP DECT), and full-duplex IP audio conference units.

NuPoint Unified Messenger

NuPoint Unified Messaging is a powerful, voice processing application that provides voice messaging and paging support. Users can access their voice mails remotely and can be notified by telephone or pager when a voice message is left for them. Users can also use NuPoint's Unified Messaging capabilities to listen to their voice mail messages through their Lotus Notes, Novell GroupWise, or Microsoft Outlook clients with Message Waiting Indicator (MWI) on playback via a URL. In addition, they can play their emails through the Telephony User Interface. Messages between these clients and the NuPoint TUI are synchronized for message playback. NuPoint Unified Messaging also offers desktop access to voice messages from an email client or web browser.

Features include:

- Multiple language support
- Integration to MCD communications platform.
- Automated attendant.
- Unified Messaging

Unified Communications Advanced

This application provides a single access point for business communication and collaboration needs. It converges the call control capabilities of the Mitel Communications Director platform with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications. It gives users control over their communications and allows real-time access to everyone in the organization, on or off the premises, with user and phone presence information.

Mitel Collaboration Advanced

The Mitel Collaboration Advanced (MCA) application allows users to schedule and create audio or web conferences. A web-based interface is used to schedule conferences, and to view conference calls. Configuration of MCA is performed in the MAS administrator portal. All interfaces are directly accessed through the secure HTTPS protocol. Authorization and authentication allows only valid users to access the services. Secure Sockets Layer (SSL) encryption for secured messages and server-side digital certificates are used to meet the highest security requirements.

Mitel Border Gateway

The Mitel Border Gateway (MBG) is a multi-service software solution that provides the following functionality:

- Teleworker service
- Web proxy blade that provides a secure method for UCA and MCA end-user web clients to connect with their LAN-based applications
- Secure remote SIP access for IP phones on the Mitel 3300 ICP and an outbound proxy for SIP trunking from internal 3300 ICPs to external third-party SIP providers
- Secure Recording Connector service to facilitate the recording of Mitel-encrypted voice streams by third-party call recording equipment.

Initial Configuration Wizard

The vUCC Initial Configuration Wizard guides you through the initial system set up. It allows you to configure the system with the basic settings required to get the system up and running. It guides you through the following configuration steps:

- Select configuration options (restore from backup or create from scratch)
- Review initial configuration parameter
- Configure administration email and servers
- Configure numbering plan
- Configure Incoming call configuration
- Configure SIP provider
- Configure SIP trunk proxy
- Configure optional services: Hot Desking, Mitel Collaboration, and Music on Hold
- Set the system password.

You only run this wizard once during the initial configuration of the system. After you deploy the vUCC OVA file in the VMware vSphere environment, you run this wizard in an internet browser and enter the site specific settings in the screens. The wizard then configures the system with your settings.

After you run the wizard, you must

- Configure advanced features through the application programming interfaces
- Provision users through the Users and Services application.

Note: Do not confuse the vUCC Initial Configuration Wizard with the Mitel Integrated Configuration (MiCW) that configures standalone MAS and MCD systems. They are separate tools

Chapter 3

Plan Customer Site

Planning Overview

To prepare for vUCC deployment, complete the following:

□ Collect service provider and customer details

□ Collect customer site requirements

□ Record licensing requirements

□ Review engineering guidelines

□ Collect site configuration data

□ Review installation and provisioning workflow

Collect Service Provider and Customer Details

Table 2: Collect Service Provider and Customer Details

Step	Details
1. List site information	
Company Name	
Address	
State/Province/Country	
ZIP/Postal Code	
Time zone	
2. List contact information	
Contact Name	
Telephone Number	
Cell Phone	
Email Address	
3. List Authorized Partner Information	
VAR/Partner Name	
Address	
City	
State/Province	
Country	
Time Zone	
4. Complete pre-installation VoIP Site Survey	

Table 2: Collect Service Provider and Customer Details

Step	Details
5. Complete data network assessment	
6. Obtain customer site floor plan	
Site plan should identify	Site locations Trunk Requirements Numbering Plans Building Layout Existing PBXs Existing cable runs Equipment rooms LAN information
7. Obtain information on site power distribution, backup power, and the physical distribution	
8. Obtain IP addresses for vUCC and IP Phones	
9. Obtain and review Layer 2 switch settings with customer.	

Collect Customer Site Requirements

Table 3: Identify Deployment Configuration Requirements

Step	Details	
1. Identify Deployment Model	Unified Communications as a Service (UCaaS)	□
	Infrastructure as a Service (IaaS)	□
	Customer Premise Equipment	□
2. Identify Connectivity Model	vUCC hosting remote office via MPLS router	□
	vUCC hosting remote office Teleworker sets (internet connected)	□
3. Identify Firewall Configuration Requirements (refer to Mitel Border Gateway Engineering Guidelines at http://edocs.mitel.com for details)	Checkpoint "Network Gateway" Firewall	□
	Port forwarding Firewall	□
	SIP-Aware Firewall	□
	UDP Flood Protection	□
	Remote Site Firewall	□
	Firewall Configuration for SIP Trunking	□
	Firewall for Remote SIP Devices	□

Table 3: Identify Deployment Configuration Requirements

Step	Details	
4. Optional vMBGs Required?	Do you require a SIP Trunk Proxy?	□
	Do you require Secure Recording Connector for phones on the LAN?	□

Table 4: Identify Telephony Requirements

Step	Details	Number Required
1. Record Number	IP Phone users	
	SIP Phone users	
	Hot Desk Users	
	External Hot Desk Users	
	Teleworkers	
	ACD Agents (Hot Desk)	
	SIP Trunks	
2. Identify DID/DDI Requirements?	Direct Inward Dial (DID)/Direct Dialing Inwards (DDI) required on SIP trunks?	□

Table 5: Identify Device Requirements

Device Type	Name	Number Required
Phones	5304 IP Phone	
	5312 IP Phone	
	5320 IP Phone	
	5324 IP Phone	
	5320e IP Phone	
	5330e IP Phone	
	M5324 IP Phone	
	5330e IP Phone	
	5340e IP Phone	
	5360 IP Phone	
Wireless DECT	56xx DECT Wireless Phones	

Table 5: Identify Device Requirements

Device Type	Name	Number Required
Conference Units	UC 360	
Softphones	UCA Softphones	
Generic SIP Phones (hard/softphone)	5304 SIP phone	
	5330e SIP Phone	
	5340e SIP Phone	
	5360 SIP Phone	
	UCA SIP Softphones	

Table 6: Identifying User Types

UCC User License	Functionality	Number Required
Entry	• Dynamic extension: MCD user license with External Hot Desk User (EHDU) license • Simple twinning • NuPoint voice mailbox with Call Director • Standard and Advanced Unified Messaging • UCA desktop and web client with Instant Messaging Presence only	
Standard	• Multi-device user group up to 8 devices • NuPoint voice mailbox with Call Director • Standard and Advanced Unified Messaging • MCA audio and collaboration access • MBG Teleworker, UCA MiNET and SIP softphone license • UC Advanced deskphone client • UCA Advanced web client • UCA advanced softphone client	
Premium	Standard functionality above + Advanced Mobile SIP for Softphone and Video client license	

Table 7: Identifying Database Management Requirements

Requirement	Details	
Integrated Directory Service Synchronization with Active Directory Database	□ Yes □ No If Yes, field attribute mapping: □ Default, or □ Custom?	Refer to Manage IDS Attribute Mappings in the USP application online help for details.
User Provisioning Method (See “Perform Advanced Configuration” on page 90 for information)	Sync AD database with vUCC	□
	Import user data from CSV file	□
USP Roles and Templates (See “Perform Advanced Configuration” on page 90 for information)	□ Use Default roles and templates? □ Create roles and templates?	
	Role Name:	**Associated Template Name**
	:	

Record Licensing Requirements

About Licensing

When you deploy vUCC, the virtual appliance WAN network must be connected to a network with internet connectivity. Internet connectivity is required to license the product and must be maintained to support the system licensing.

Unified Communications and Collaboration (UCC) licensing simplifies the selling and ordering process because it bundles the platform and application user licenses together. Instead of ordering a MAS license, MCD user license, and multiple individual applications licenses for each user, you just order a single UCC license per user. Although you can order licenses individually (“a la carte”) we recommend that you use UCC licensing because it offers the following benefits:

- Simplifies the licensing of a vUCC user by bundling the required MAS and MCD user licenses with a specific set of application user licenses.
- Offers a significant pricing discount over “a la carte” licenses.

- Provides tiered functionality with progressive discounts. The following UCC user licenses are available:
  - **UCC Entry license**: provides an MCD user license, voicemail and unified messaging.
  - **UCC Standard license**: adds the UCC desk and web client and full audio and web collaboration to the Entry license.
  - **UCC Premium license**: adds full mobile UCC functionality to the Standard license.
- Software assurance is more cost effective: The Mitel Software Assurance (SWAS) Program is a subscription-based service that provides customers with access to new software releases, software upgrades, and product support services for all users (ports) on a given application record. Under the SWAS program, software upgrades are provided at no additional cost without any of the new features or functionality that are available in the base upgrade package.

Licensing Rules

The following rules apply to UCC Licensing:

- There are two categories of UCC license bundles:
  - “Business” for use with MCD standalone systems, and
  - “Enterprise” for use with a network of MCD systems (not available or supported with vUCC).

  vUCC CPE and IaaS sites require "Business" licenses. vUCC UCaaS deployments require special licensing that is governed by the Service Provider addendum to the standard Authorized Partner Contract.
- You require a UCC License Manager (ULM) to create a UCC Group ARID on the AMC.
- You cannot split the UCC license bundle and deploy the application licenses across different users within a system.
- If you are configuring a **Public Internet Connected End Customer** deployment where the customers are internet connected, the following conditions apply:
  - All users are connected to the vUCC system through the internet (even desk phones are routed through an MBG).
  - Users hot desk between their home phone and their work phone.
  - Users are all assigned Premium UCC User Licenses and have been created with the default Premium UCC User Template.
  - Users have their desk phone and a soft phone in a MDUG. Both phones ring simultaneously for an incoming call.
  - In addition to the teleworker license provided in the Premium UCC User license, each user requires a second teleworker license.Two teleworker user licenses are required to allow both of the user’s phones to be registered with teleworker service (so that they both ring simultaneously on an incoming call).

Additionally, for UCaaS deployments:

- You can choose to license the vUCC software bundle and user licenses on a subscription basis from Mitel.

vUCC Licensing Detection and Violation Mode

vUCC appliances must maintain online connectivity to the AMC at all times. Loss of AMC connectivity for a short period of time is tolerated by the system. However, AMC connectivity must be re-established without delay in order to maintain access to all system functions and features. If AMC connectivity is lost for an extended period of time, an automatic alert is generated and sent to the Channel Partner AMC account administrator email address that is programmed in the AMC for the account. If AMC connectivity is not re-established, then the virtual appliance system goes into license violation mode and certain capabilities are no longer be accessible.

Mitel recognizes that in some deployment situations, it is not practical to implement online connectivity to the AMC from each virtual appliance deployed at a customer's site. For this reason, Mitel supports the ability to proxy online AMC connectivity from each virtual appliance through a single named proxy within the customer data center environment. This enables AMC online connections to be managed and controlled from one central point within the data center rather than from each individual product.

NuPoint VoiceMail Port Allocation

NuPoint ports are licensed on the vUCC system based on the number of UCC user licenses purchased. However the vUCC Integrated Configuration Wizard (IWC) configures fewer than the actual number of licensed NuPoint ports. The IWC does not configure all the ports in order to reserve some ports for Recording Announce Devices (RADs). You can manually configure these reserved ports up to the specified engineering limits.

Note: A basic user is created for each MCA port and these users are taken into consideration in the NuPoint voice port allocation algorithm.

Table 34 identifies the number of ports that are configured by the IWC based on the number of licensed users and ports.

Table 8: NuPoint VoiceMail Port Allocation

Licensed Users	Licensed Ports	Ports Configured by IWC	Ports Reserved for RADs
0	6	6	0
20	7	6	1
40	8	7	1
60	9	8	1
80	10	8	2
100	11	9	2
120	12	10	2
140	13	10	3

Table 8: NuPoint VoiceMail Port Allocation

Licensed Users	Licensed Ports	Ports Configured by IWC	Ports Reserved for RADs
160	14	11	3
180	15	11	4
200	16	12	4
220	17	12	5
240	18	13	5
250	19	14	5

Licensing Conditions for MCA

The following UCC Licensing conditions apply to the MCA application:

- Mitel Collaboration Advanced is licensed by port. Each port enables one simultaneous audio and web connection in the system. For example, a 10-party conference would require 10 ports.
- The system includes two ports plus an additional ports for every 10 Standard/Premium UCC User licenses. If the system has no Standard or Premium UCC User licenses, then no ports are included with the system. Typical configurations use one audio port for every 10 MCA users.
- The AMC uses a set of pre-defined rules to provision MCA audio and web collaboration ports based on the number of UCC Standard or Premium licenses that are assigned to the MAS base ARID. The AMC provisions three audio and web Collaboration ports for the first 10 UCC Standard or first 5 UCC Premium users. Every time another threshold of ten Standard or five Enterprise users is crossed, an additional MCA audio and web collaboration port is added at no extra charge:

  The following licenses are provisioned for every 10 Standard UCC Users:

  1 x MCD Connection User

  1 x MCA Web Port, 1 x MCA Audio Port, 1 x MCA HDCodec Port

  The following licenses are provisioned for every 5 Premium UCC Users:

  1 x MCD Connection User

  1 x MCA Web Port, 1 x MCA Audio Port, 1 x MCA HDCodec Port

  For example:

  - 10 UCC Standard licenses earns three MCA audio and web collaboration port at no additional charge

- A total of 11 UCC Standard licenses earns four MCA audio and web collaboration ports at no additional charge. Note, two MCA audio and web collaboration ports enable one-to-one collaboration.
- An MCA port is comprised of 1 audio port, 1 web port, and 1 H.264 video port.
- UCC Standard and Premium licenses include collaboration licenses. A UCC Entry license does not have a collaboration license so it does not include any MCA ports.

Note: System capacities are identified in the vUCC Engineering Guidelines. Licensing rules may grant you more port licenses than are allowed to be configured from an engineering standpoint. Obey the vUCC Engineering rules.

Licensing Tiers

There are three tiers of UCC license, Entry, Standard, and Premium.

Table 9: Licensing Tiers

Licenses included	UCC License (see Note 1)		
	Entry	**Standard**	**Premium**
Dynamic extension (includes MCD user license with EHDU license)	Yes (Simple twinning)	No	No
Multi-device user license (includes MCD user license)	No	Yes (Multi-device user group up to 8 devices)	Yes (Multi-device user group up to 8 devices)
NuPoint mailbox license with call director	Yes	Yes	Yes
Standard and Advanced UM license	Yes	Yes	Yes
MCA audio and collaboration access (also see “Licensing Conditions for MCA” on page 35)	No	Yes	Yes
MBG Teleworker license, UCA MiNET, and SIP softphone license	No	Yes	Yes
UCA desktop and web client with Instant Messaging Presence only	Yes	No	No
UC Advanced deskphone license	No	Yes	Yes
UC Advanced web license (see Note 1)	No	Yes	Yes
UC Advanced softphone license (see Note 1)	No	Yes	Yes
UC Advanced mobile SIP for Softphone and Video client license	No	No	Yes

Notes:

1. A UCC license (Entry, Standard, or Premium) is required to deploy an attendant position.
2. With an additional MCD user licence, you can configure a UCC Entry user with a Multi-device User Group.

3. The UCC Entry license provides UCA desktop and web client with only the Instant Messaging feature. The Standard license provides UCA desktop and web client with full UCA feature functionality.

Record UCC Licensing Requirements

You need to configure the vUCC with at least

- one Standard or Premium UCC User license,
- two MCD SIP Trunking Licenses, and
- if using internal SIP trunking, two MBG SIP Trunking Channel Licenses

Enter the licensing requirements for the site in the following table:

Licenses	Part Number	Number Required
Core vUCC Software for IaaS and Customer Premise Deployments		
UCC Virtual Appliance Base (without user licenses or SIP trunk licenses) Contains the following base system packages • Virtual MCD Business - with MCD Standard User licensing • Virtual MAS – with access to all advanced Unified Communications features and functions • Virtual MBG – Mitel’s Border Gateway for secure Voice and UC interaction with Service Providers and the Internet	54005919	
UCC Virtual Appliance Bundle Contains the following base system packages: • Virtual MCD Business - with MCD Standard User licensing • Virtual MAS – with access to all advanced Unified Communications features and functions • Virtual MBG – Mitel’s Border Gateway for secure Voice and UC interaction with Service Providers and the Internet Includes: • 16 x UCC Entry User License for Business • 4 x MCD SIP Trunk licenses • 4 x MBG SIP Trunk Proxy licenses	54005892	
Core vUCC Software for UCaaS and CAPEX Deployments		
UCC Virtual Appliance for Service Provider Subscription (SP SUB) Contains the following base system package: • 54005931 UCC Virtual Appliance Enterprise Base for SP SUB and includes the following licenses: • 275 x MCD SIP Trunk licenses • 5 x G.729 (8-pack) licenses	54005894	

Licenses	Part Number	Number Required
UCC Virtual Appliance for Service Provider CAPEX (CAPEX licensing is used with UCaaS deployment models where user licenses are purchased as a capital expense and not on a subscription basis) Contains the following base system package: • 54005920 UCC Virtual Appliance Enterprise Base for SP CAPEX and includes the following licenses: • 275 x MCD SIP trunk licenses • 5 x G.729 (8-pack) licenses • MBG SP client license (MBG SIP Proxy client license is not included.)	54005921	
User - Business		
UCC (V2) Entry User License for Business	54005983	
UCC (V2) Standard User License for Business	54005984	
UCC (V2) Standard User License for Business (50 User)	54005985	
UCC (V2) Premium User License for Business	54005986	
UCC (V2) Premium User License for Business (50 User)	54005987	
User - Enterprise		
UCC (V2) Entry User License for Enterprise	54005978	
UCC (V2) Standard User License for Enterprise	54005979	
UCC (V2) Standard User License for Enterprise (50 User)	54005980	
UCC (V2) Premium User License for Enterprise	54005981	
UCC (V2) Premium User License for Enterprise (50 User)	54005982	
User - SP CAPEX		
UCC (V2) Entry User License for SP CAPEX	54005960	
UCC (V2) Standard User License for SP CAPEX	54005956	
UCC (V2) Premium User License for SP CAPEX	54005957	
Uplift		
UCC (V2) Entry to UCC (V2) Standard for Business	54006012	
UCC (V2) Standard to UCC (V2) Premium for Business	54006013	
UCC (V2) Entry to UCC (V2) Standard for Enterprise	54006014	
UCC (V2) Standard to UCC (V2) Premium for Enterprise	54006015	
Service Provider Subscription User		
UCC Entry User Licenses for Service Provider Subscription (50)	54005922	
UCC Standard User Licences for Service Provider Subscription (50)	54005923	
UCC Premium User Licenses for Service Provider Subscription (50)	54005924	
Software Assurance Support (SWAS)		
Standard SWAS UCC(V2) Entry Business	54005998	

Licenses	Part Number	Number Required
Standard SWAS UCC(V2) Standard Business	54005999	
Standard SWAS UCC(V2) Premium Business	54006000	
Premium SWAS UCC(V2) Entry Business	54006001	
Premium SWAS UCC(V2) Standard Business	54006002	
Premium SWAS UCC(V2) Premium Business	54006003	
Standard SWAS:UCC Virtual Appliance Base	54005936	
Premium SWAS:UCC Virtual Appliance Base	54005937	
Standard SWAS:UCC Virtual Appliance Base for SP CAPEX	54005938	
Premium SWAS:UCC Virtual Appliance Base for SP CAPEX	54005939	

Note: Premium SWAS must be applied as an upgrade to Standard SWAS.

Note: vUCC also supports "a la carte" licensing.

Review Engineering Guidelines

Review the vUCC site requirements detailed in the MAS and vUCC Engineering Guidelines. Review the *Virtual Appliance Deployment Solutions Guide*. It provides engineering guidelines for deploying Mitel Virtual Appliances and applications in a VMware virtual infrastructure.

Collect Site Configuration Data

Before you begin deployment, collect and record the data specified in Table 10. You will need this information in order to successfully deploy the vUCC OVA and perform initial configuration using the wizard.

Table 10: Collect vUCC Properties of Application

Configuration Items	Field Description	Site Configuration Data
Localization		
Time zone	Identify the MSL operating system time zone setting. The default is America/New York. The Time zone setting also determines your system telecommunications regional settings.	
Region (country)	Identify the country in which the vUCC virtual appliance is being deployed.	
Keyboard Type	Identify the preferred keyboard type (default is **us**)	

Table 10: Collect vUCC Properties of Application

Configuration Items	Field Description	Site Configuration Data
Application		
Administrator Password	Record the initial administrator password for the MAS server manager interface.After you access the MAS server manager, you will be prompted to change this initial password. **Note**: You must enter a password before you deploy the vUCC; otherwise, the system will not boot up.	Initial MAS Server Manager Administrator Password: ______________________ Final MAS Server Manager Administrator Password: ______________________ **Note**: It is recommended that you use a strong password that contains all of the following: upper case letter, lower case letter, number, non-alphanumeric character, and be at least seven characters long. Do not use a commonly used words (for example: 'password').
Hostname	Set the hostname of the vUCC. The default hostname is "vUCC". **Note**: You do not require a name if you are just creating a blank template of the OVA file for cloning.	
Domain Name	Specify the domain name for the hostname above. The default domain name is "mycompany.local". **Note**: You do not require a name if you are just creating a blank template of the OVA file for cloning.	
UCC License Key (vUCC Business Base ARID)	Identify the UCC License Key (vUCC Business Base ARID) for this system. The ARID is used by the AMC to distribute the system licenses. See “Create ARIDs and Assign Licenses in AMC” on page 51 for instructions. **Note**: You do not require an ARID if you are just creating a blank template of the OVA file for cloning.	
DNS Server IP	Record the DNS Server IP Addresses	
LAN Properties		
LAN IP Address (IP Address of the vUCC) **Note**: Identified as LAN IP Address # 1 in Initial Configuration page of Initial Configuration Wizard.	Record the IP address of the local (LAN) interface. This must be a valid IP address on the local LAN. **Note**: You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this address from vSphere Client. Right-click on the vUCC and click **Edit Settings**. Click the **Options** tab, click **Properties** and enter the LAN IP Address.ppliance	

Table 10: Collect vUCC Properties of Application

Configuration Items	Field Description	Site Configuration Data
LAN Netmask	Record the Netmask of the LAN.	
WAN Properties		
WAN IP Address	Record the IP address of the external (WAN) interface. This must be a valid IP address on external WAN. **Note**: You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this address from vSphere Client. Right click on the vUCC and click **Edit Settings**. Click the **Options** tab, click **Properties** and enter the WAN IP Address.	
WAN Netmask	Record the Netmask of the WAN.	
WAN Gateway IP Address	Record the Gateway IP Address of the WAN.	

Table 11: Collect Advanced Deployment Properties

Configuration Items	Field Description	Site Configuration Data
Remote access for administration	List the public IP addresses that are allowed to access the system and perform remote administration.	______________________ ______________________ ______________________ ______________________
Mitel Application Management Center (AMC)	Record IP address or proxy address for the AMC	
MCD IP address **Note**: Identified as LAN IP Address # 2 in Initial Configuration page of Initial Configuration Wizard.	By default, this address defaults to the vUCC LAN IP address +1. If you want to override the default MCD IP address that is applied during initial configuration, record the desired IP address.	

Table 12: Collect vUCC Initial Provisioning Wizard Data

Configuration Items	Field Description	Site Configuration Data
E-mail and Servers		
Administrator Email Address	Record the email address of the system administrator.	

Table 12: Collect vUCC Initial Provisioning Wizard Data

Configuration Items	Field Description	Site Configuration Data
Primary DNS IP Address	Specify the IP address of the SMTP Server.	
Secondary DNS IP Address	Specify the IP address of the DNS IP Address.	
SMTP Mail Server	Record the host name of the SMTP Mail server	
Network Time Server Source	Identify the Network Time Server Source for the system (for example: centos.pool.ntp.org).	
System Language	Identify the MAS default language. The selected language is applied to the My Unified Communication portals and the Telephone User Interfaces (TUIs) for the MAS application end-users.	
Voice Mail Secondary Language	Identify the language of the secondary NuPoint prompts. When users call into the NuPoint system through the Message Center auto attendant or Receptionist application, they are asked to select the language of the NuPoint prompts for the duration of their call. Users can select either the primary or secondary prompt language. The primary (first) language is determined by the Language setting above; the second language is determined by the setting in this field. For example, the first language could be English, the second language, French.	
Numbering Plan		
Extension Length	Specify the required extension length (3 to 5 digit extension numbering)	
Voice Mail Hunt Group Ext	Default is 7000	
Voice Mail Starting Port Ext	Default is 7001 (up to 7007)	
Voice Mail HCI Hunt Group Extension	Default is 7400	
Voice Mail Record A Call Hunt Group Extension	Default is 7500	
MCA Hunt Group Extension	Default is 7850	
MCA Starting Point Extension	Default is 7851 (up to 7854)	
Incoming Calls		
Main Business Number	Enter the phone number of the site. External callers dial this number to place incoming calls on these SIP trunks.	

Table 12: Collect vUCC Initial Provisioning Wizard Data

Configuration Items	Field Description	Site Configuration Data
OR		
Incoming Call Handling Extension	Specify the answerpoint extension number.	
Auto Receptionist Hunt Group Extension	Specify the extension number.	
Start Port Extension	Specify the starting port extension.	
Advanced Incoming Call Configuration		
Number of Digits to Absorb		
Digits to Insert		
SIP Provider		
SIP Provider	Identify your SIP Service Provider. **Note**: The wizard lists the most common Service Providers for your region for selection. A "Generic" SIP peer profile is also available. If required, you can specify a custom peer profile CSV file saved from the SIP Peer Profile form in the MCD System Administration Tool (see "Obtain a Custom SIP Peer Profile (optional)" on page 46for instructions)	
IP Address or FQDN	Enter the IP address or Fully Qualified Domain Name of your Service Provider	
SIP Registration	Is registration required?	
Registration User Name	Record the username and password for your SIP Service account. Obtain these credentials from your SIP Service Provider.	
User Name		
Password		
Number of MCD SIP Trunk Licenses	Record the number of required MCD SIP trunk licenses. The ICW provisions the number of trunks licensed in the ARID up to the maximum capacity. See the Engineering Guidelines for capacities. **Note:** You need to configure the vUCC ULM with at least two MCD SIP Trunk Licenses in order to successfully complete the Initial Configuration Wizard.	

Table 12: Collect vUCC Initial Provisioning Wizard Data

Configuration Items	Field Description	Site Configuration Data
Number of MBG SIP Trunk Channel Licenses	Record the number of licenses required. **Note:** If using internal SIP trunking, you need to configure the vUCC ULM with at least two MBG SIP Trunk Channel licenses in order to successfully complete the Initial Configuration Wizard.	
SIP Provider Advanced Provisioning		
Subscription User Name	Record the optional user name and password for the telephony server to subscribe to the SIP Peer that is performing KPML digit detection.	
Subscription Password		
SIP Provider Proxy		
SIP Trunk Proxy	Select **Internal** if the SIP trunk proxy is supported on the vUCC system. Select **External** if the SIP trunk proxy is supported on a separate optional Mitel Border Gateway (MBG).	□ Internal □ External □ No SIP Trunk Proxy
SIP Trunk Proxy Server Address	If you are using an external SIP trunk proxy, record the SIP trunk proxy server address.	
Local Network Details	Will SIP Service Provider be located on a different local network? If Yes, record the IP addresses.	□ Yes
Local Network Address		
Local Netmask		
Local Network Router Address		
WAN Router Address		
Optional Services		
Optional Services	Identify the required optional services	□ Hot Desking
		□ Mitel Collaboration Advanced
		□ Music on Hold
Hot desking: allows a number of users to share one or more phones. Hot desking is ideal for telecommuters, sales agents, and other employees who spend only part of their time in the office. With hot desking, a company does not have to provide a dedicated phone for each of these employees. Instead, the company can make a pool of shared phones available on a first-come, first-served basis. A hot desk user can log into any available hot desk-enabled phone on the system. After a user logs into a hot desk phone, the system applies the user's profile to the phone and it functions as the user's desk phone.		

Table 12: Collect vUCC Initial Provisioning Wizard Data

Configuration Items	Field Description	Site Configuration Data
Hot desk users	Record the number of phones that you want to support hot desking. Indicate the number of hot desk phones for each phone model	5304 IP ________ 5320 IP ________ 5330e IP ________ 5340 IP ________ 5340e IP ________ 5360 IP ________
Mitel Collaboration Advanced: allows users to set up audio and web conferences for online meetings, training sessions, and presentations. Users can share their desktops or individual applications during the conferences. Video recordings of the web sessions can be made for playback.		
Conferencing FQDN	Record the Fully Qualified Domain Name (FQDN) of the Mitel Collaboration Advanced server.	
Conference WAN IP Address:	MCA public IP address on the WAN.	
Music on Hold: provides callers with music or information while they are waiting for a call to be completed. It’s played whenever a call is on Hold, transferred to a busy or ringing station, or camped-on to a station. The customer site must provide the music or information source file.		
Music on Hold File	Identify the filename and location of the music source file. Refer to the MAS and vUCC Engineering Guidelines for file requirements.	
Mitel Application Suite		
Active Directory Integration (optional)	Record the Active Directory Server IP address.	
Administrator Password		
Replaces the password that you used to access the wizard. It allows you to log into the server manager administration interface.	A strong password is recommended. A strong password would contain all the following: upper case letter, lower case letter, number, non-alphanumeric character and be at least seven characters long.	

Obtain a Custom SIP Peer Profile (optional)

If required, you can save a custom SIP Peer Profile CSV file from an existing MCD system database and import it into the vUCC system from the Initial Configuration Wizard.

Note: You must use the **Save File** function from the **Profile Information** tab to create the file. Do not export the SIP Peer Profile form to a CSV file.

1. Log into the MCD System Administration tool. See “Logging into the Mitel Communications Director (MCD) Tools” on page 122.
2. In the top left corner, select **View Alphabetically**.
3. In the left forms menu, select **SIP Peer Profile**.
4. Select the desired SIP Peer Profile.
5. Click the **Profile Information** tab.
6. Click **Change**.
7. Complete the Creator, Service Provider Name, and Vendor Notes fields.
8. Click **Save File**.
9. Save the CSV file to a network drive. During the Initial Configuration Wizard, you can import this custom SIP Peer Profile into the vUCC system.

Review Installation and Provisioning Workflow

The following figures summarize the installation and provisioning workflow for vUCC.

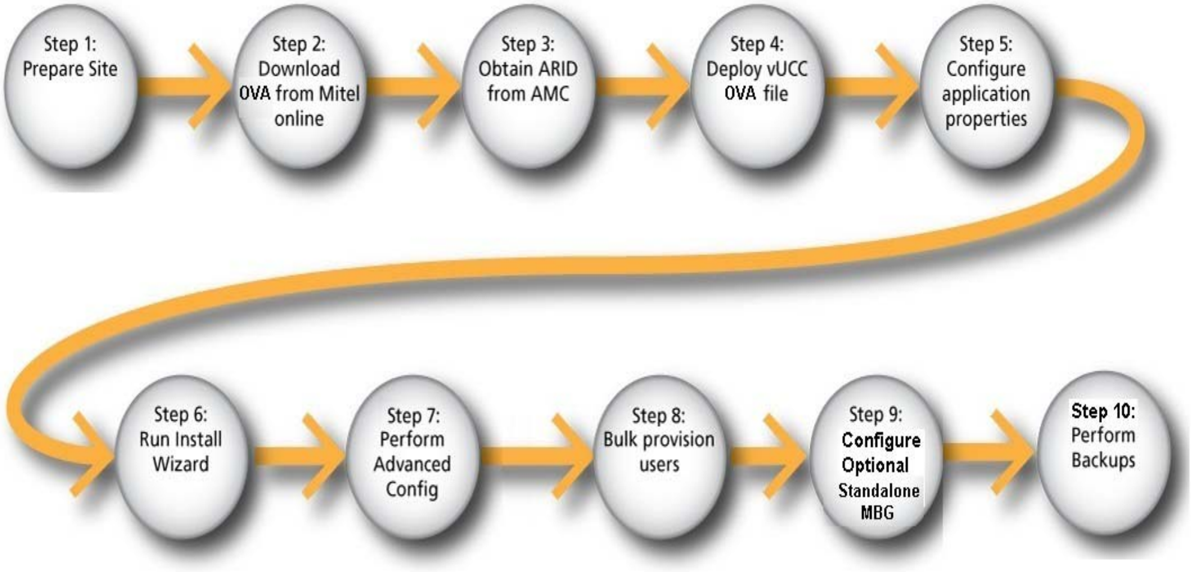


Figure 8: vUCC Deployment on New Site

Chapter 4

Deploy UCC Virtual Appliance

Introduction

VMware Installation Resources

This chapter describes the deployment of the Unified Communication and Collaboration (vUCC) virtual appliance. It does not describe the setup and operation of the VMware vSphere environment. Refer to the VMware documentation for instructions on how to set up the vSphere environment:

- See the VMware vSphere main documentation page at
  - http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

  for links to the following information:
  - New Features and Release Notes
  - Compatibility and Configuration Limits
  - ESXi and vCenter Server Product Documentation
  - Command-Line Interfaces
  - Optional vSphere Products and Modules
- See the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php for supported hardware platforms.

Note the following deployment requirements:

- vUCC must be deployed using the vSphere Client connected to vCenter. You cannot deploy vUCC using the vSphere Client that is connected directly to an ESXi server.
- vCloud Director can be used for deployment but you must first convert the OVA file to OVF format. Refer to the Mitel Virtual Appliance Deployment Solutions Guide for conversion instructions.

Deployment Overview

Perform the following steps to deploy the vUCC:

□ Complete Site Planning (see previous chapter)

□ Prepare Site

□ Create ARID and Licenses in AMC

□ Download vUCC OVA file

□ Deploy vUCC vApp

Complete Site Planning

Before you begin deployment, review the previous chapter, “Plan Customer Site" starting on page 27. Ensure that you have recorded the site configuration information in Table 10.

Prepare Site

Requirements

❐ The vUCC requires access to the internet in order to obtain its licenses from the Applications Management Center (AMC). Internet connectivity is required to license the product and must be maintained to support the system licensing.

❐ The available virtual appliance resources for the vUCC deployment must meet or exceed the minimum requirements listed in the *MAS and vUCC Engineering Guidelines* .

Set Up Active Directory Server (Optional)

If required, set up the Active Directory server prior to deploying the vUCC. Ensure that you have recorded the Active Directory Server IP address in Table 10 on page 39.

Deploy and Configure Optional External vMBG SIP Proxy

For UCaaS deployments, configure and deploy the optional external vMBG SIP Proxy server before you deploy and provision the vUCC. The Initial Configuration Wizard prompts you for the standalone vMBG IP address during the wizard.

Refer to the *Mitel Border Gateway Installation and Maintenance Guide with Web Proxy* on the Mitel Customer documentation site at http://edocs.mitel.com for deployment and configuration instructions.

Create ARIDs and Assign Licenses in AMC

Create Application Record Identifications (ARIDs) for this vUCC installation in your AMC license account and assign the required licenses to them. When you deploy the vUCC, you will use the software base Application Record ID to activate the system and user licenses.

About the Mitel Application Management Center (AMC)

Licensing is supported through the Mitel Application Management Center (AMC). The Mitel AMC manages the software licensing and entitlement of the Software Assurance Program. After you obtain an Application Record ID (ARID) from the AMC, the AMC uses your Application Record ID (ARID) to provide you with access to licenses, software releases, and upgrades.

The Mitel Software Assurance (SWAS) Program is a subscription-based service that provides customers with access to new software releases, software upgrades, and product support services for all users (ports) on a given application record.

When you place a new order for products with the Mitel Customer Care Center, the order information is entered into the AMC system. The AMC places the purchased licenses into your licensing account. You assign the licenses to one or more product application records.

When you install vUCC, it generates a unique Hardware ID that includes the MAC address of the server. When you connect to the AMC over the internet, the Hardware ID and the Application Record ID are synchronized with the AMC to obtain the licensing information.

Requesting a New AMC Account

To request an AMC account, send an e-mail containing the following information to amc_accounts@mitel.com:

- Name of your certified Technician
- Full company name
- Company mailing address
- Phone 1/Phone 2
- Fax number
- Admin e-mail (address of the person who should receive notification of service expiry dates)
- Tech e-mail (address of the person who should receive notification of upgrade releases and other technical notices)
- Company URL (if any)
- Your Mitel SAP account number
- Specify if you would like your user ID and password delivered to you by fax, phone, or both (for security reasons user IDs and passwords are not sent by e-mail).

Note: Please allow two business days for your AMC account to be created.

Accessing your AMC Account

To access your account for the first time:

1. Go to the Mitel web site (http://www.mitel.com) and log in to your Mitel OnLine account.
2. Point to **Purchasing**. Under **Licensing** click **AMC**.
3. Click Go to the Applications Management Center (AMC).
4. Sign in with your unique AMC username and password. On subsequent visits, you access your AMC account directly after signing in to Mitel OnLine.
5. For information about using the AMC, click the online Help link in your AMC account.

UCC Licensing Procedure

The Application Management Center distributes the platform and application user licenses that are contained within a UCC license bundle to the members of a Unified Licensing Manager (ULM) group. During the licensing process, you create a ULM group ARID for the vUCC deployment.

Note: To successfully complete the Initial Configuration Wizard, you must assign at least one Standard or Premium UCC User license, one SIP Trunking License, and one SIP Trunking Channel License to the vUCC ULM ARID. The Initial Configuration Wizard requires these licenses in order to complete configuration of the system.

Overview

The following is an overview of the main steps required to deploy UCC licenses:

- Authorized Partner creates customer account.
- Authorized Partner registers (purchases) and assigns UCC licenses on AMC.
- Authorized Partner creates an Application Record ID for the vUCC base software.
- Authorized Partner assigns the vUCC base software license to the vUCC Base ARID
- Authorized Partner creates an associated ULM ARID for the vUCC base ARID.
- Authorized Partner assigns MCD SIP trunk licenses, MBG SIP trunk licenses, UCC User and SWAS licenses to the ULM ARID.
- If the site requires a standalone vMBG for SIP trunking, the Authorized Partner purchases the vMBG base under the same customer and applies it to the vMBG ARID. The Authorized Partner then selects it and adds the vMBG ARID to the ULM group ("Business" for CPE and IaaS sites; "Enterprise" for UCaaS deployments).
- Installer deploys vUCC. During deployment, the licenses are automatically downloaded from the AMC to the system.

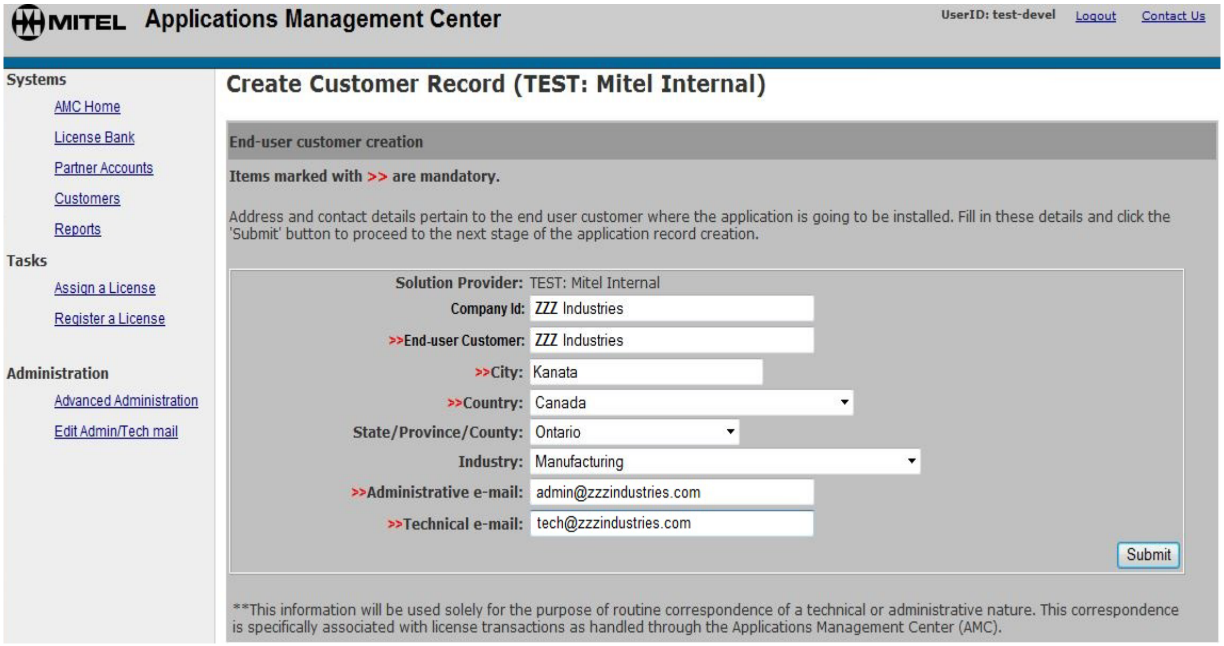
Deploying UCC Licenses

A detailed procedure for deploying UCC licenses follows:

1. Log into the Applications Management Center:
   - Enter your login User ID
   - Enter your Password.

Note: While you are using the AMC interface, if you click the browser back button, you may need to refresh your browser to display the screen again.

2. Create a Customer Account for each vUCC customer. Do not put multiple customers in a single customer account.
   - Under **Systems**, click **Customers**.
   - Click the **Create Customer** button.
   - Enter the end-customer information. Record the Customer Name and Customer ID.
   - Enter the email address of the account manager responsible for this customer.
   - Enter the email address of the technician responsible for supporting this customer.
   - Click **Submit**.
   - Click **Confirm**.



Create Customer Record (TEST: Mitel Internal)

End-user customer creation

Items marked with >> are mandatory.

Address and contact details pertain to the end user customer where the application is going to be installed. Fill in these details and click the 'Submit' button to proceed to the next stage of the application record creation.

Solution Provider:	TEST: Mitel Internal
Company Id:	ZZZ Industries
>>End-user Customer:	ZZZ Industries
>>City:	Kanata
>>Country:	Canada
State/Province/County:	Ontario
Industry:	Manufacturing
>>Administrative e-mail:	admin@zzzindustries.com
>>Technical e-mail:	tech@zzzindustries.com

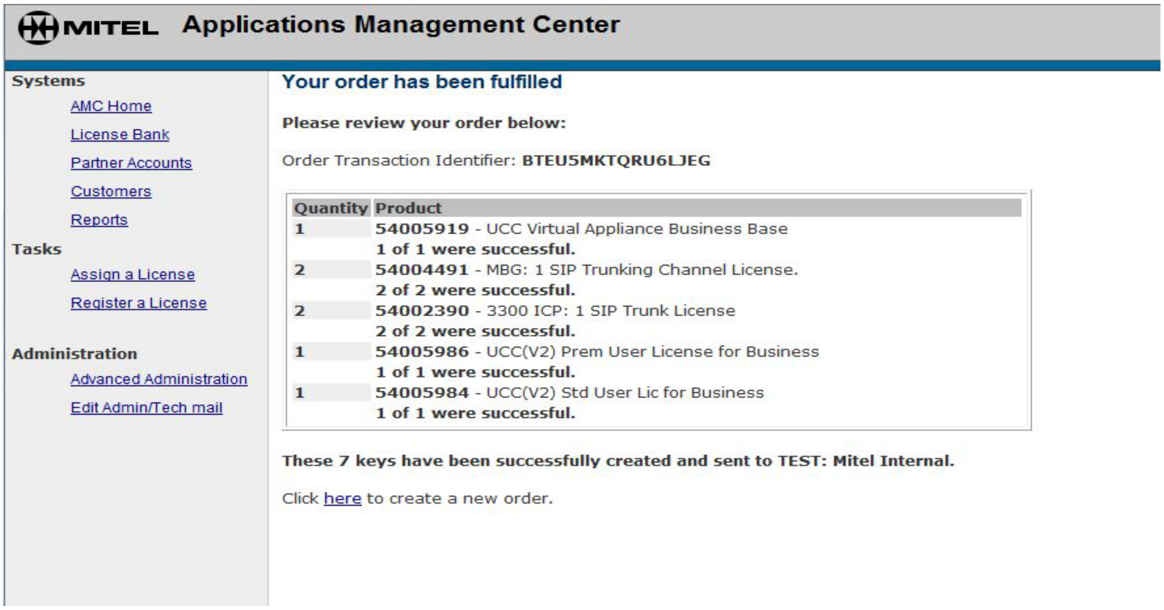
**This information will be used solely for the purpose of routine correspondence of a technical or administrative nature. This correspondence is specifically associated with license transactions as handled through the Applications Management Center (AMC).

Figure 9: Creating a Customer

3. Register (purchase) products and licenses for the vUCC deployment. The following is an example for the vUCC appliance using the clear base:
   - Click **Register a License**.
   - Enter a Purchase Order reference number.
   - Click **+** beside Mitel Virtual UCC Appliance Products. Enter the desired number of vUCC Virtual Appliance base software products, UCC User Licenses, and software

assurance products. To locate a part number or license description in the displayed list, use the browser Find function.

- Click **+** beside Mitel 3300 ICP/Mitel Communications Director Products. Enter at least two "54002390 MCD Trunk Licenses".
- Click **+** beside Mitel Standard Linux Standalone Products.Enter at least two "5405591 SIP Trunking Channel Proxy Licenses".
- Click **+** beside Mitel Unified Collaboration and Communication Products. Enter the desired number of UCC User Licenses. You must enter at least one "54005984 UCC: 1 Standard License for Business (V2)" or one 54005981 UCC: 1 Premium License for Business (V2)".
- Click **Next**.
- Click **Confirm**.



Your order has been fulfilled

Please review your order below:

Order Transaction Identifier: **BTEU5MKTQRU6LJEG**

Quantity	Product
1	**54005919** - UCC Virtual Appliance Business Base **1 of 1 were successful.**
2	**54004491** - MBG: 1 SIP Trunking Channel License. **2 of 2 were successful.**
2	**54002390** - 3300 ICP: 1 SIP Trunk License **2 of 2 were successful.**
1	**54005986** - UCC(V2) Prem User License for Business **1 of 1 were successful.**
1	**54005984** - UCC(V2) Std User Lic for Business **1 of 1 were successful.**

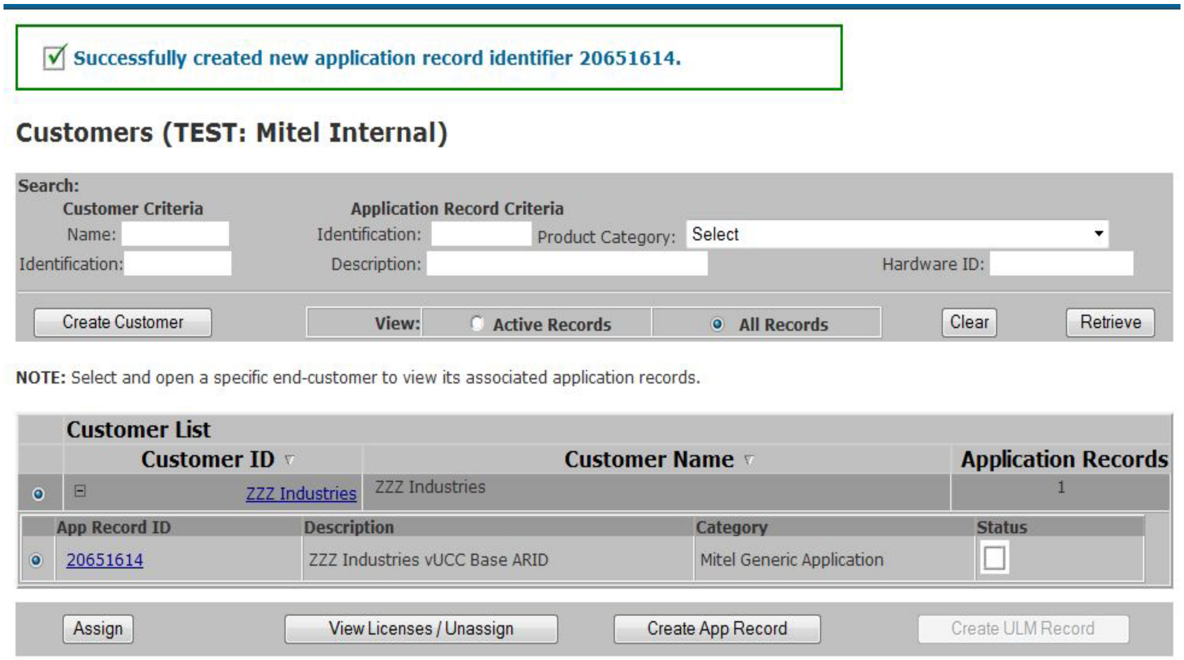
These 7 keys have been successfully created and sent to TEST: Mitel Internal.

Click here to create a new order.

Figure 10: Order Confirmation

4. Create an Application Record ID for the vUCC base software:

- Click **Customers**. Enter the customer name and click **Retrieve**.
- Select the Customer ID.
- Click **Create App Record**. Enter a description for the vUCC base software Application Record. For example: "ZZZ Industries vUCC Base ARID".
- Click **Submit**. Click **Next**. The system displays the newly created ARID at the top of the screen. Record the vUCC ARID. When you deploy the vUCC, the Initial Configuration Wizard prompts you to enter this ARID.



☑ Successfully created new application record identifier 20651614.

Customers (TEST: Mitel Internal)

NOTE: Select and open a specific end-customer to view its associated application records.

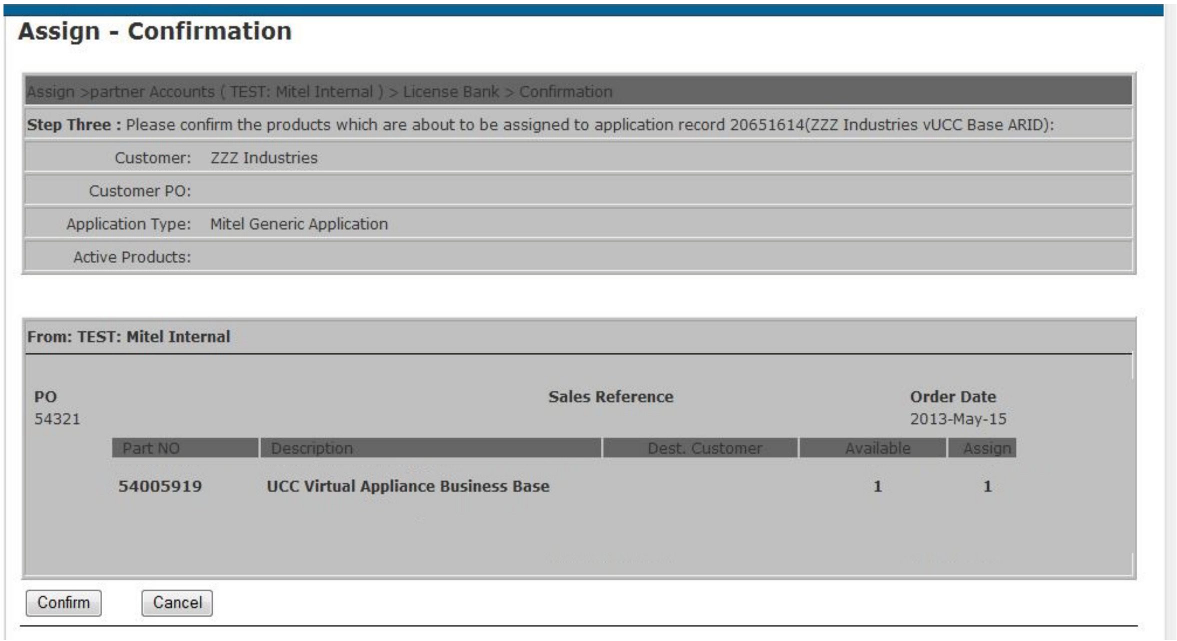
Customer List

	Customer ID	Customer Name	Application Records
●	⊟ ZZZ Industries	ZZZ Industries	1

	App Record ID	Description	Category	Status
●	20651614	ZZZ Industries vUCC Base ARID	Mitel Generic Application	□

Figure 11: vUCC Base ARID Created

5. Assign the vUCC base software license to the vUCC Base ARID:
   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
   - Click **+** beside the customer's ID.
   - Select the option button next to the vUCC Base ARID and then click **Assign**.
   - Enter the Purchase order number in the Search Criteria and click **Retrieve**.
   - Click **+** to expand the Purchase order.
   - Assign the Business vUCC business base software license to the base ARID.
   - Click **Assign**.



Assign - Confirmation

Assign >partner Accounts (TEST: Mitel Internal) > License Bank > Confirmation

Step Three : Please confirm the products which are about to be assigned to application record 20651614(ZZZ Industries vUCC Base ARID):

Customer: ZZZ Industries

Customer PO:

Application Type: Mitel Generic Application

Active Products:

From: TEST: Mitel Internal

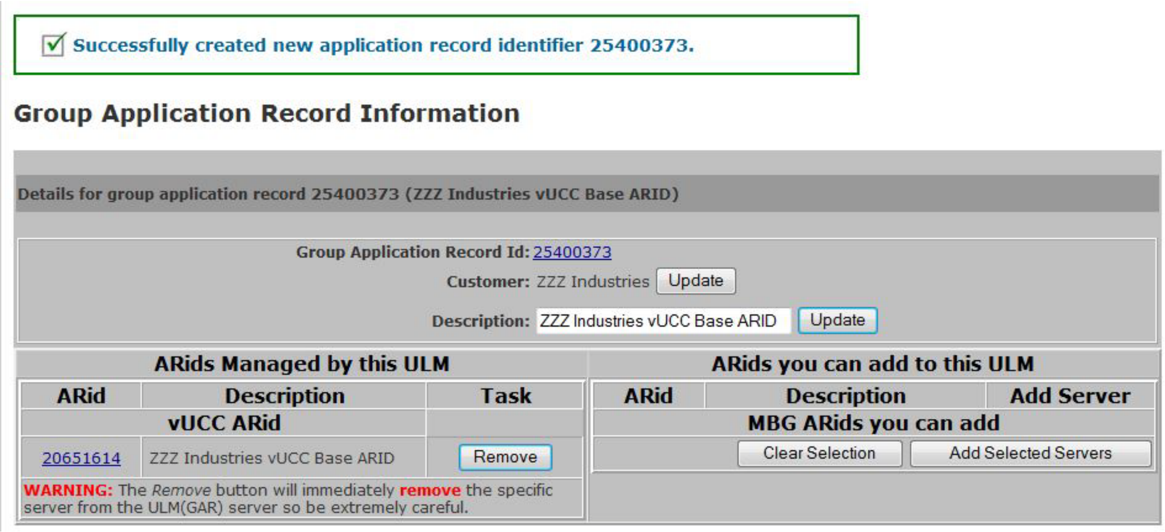
PO	Sales Reference	Order Date
54321		2013-May-15

Part NO	Description	Dest. Customer	Available	Assign
54005919	UCC Virtual Appliance Business Base		1	1

Figure 12: Assign Base Licenses to Base ARID

- Click **Confirm** to assign the licenses.
- Review the licenses and record the ARID.
- Click **Done** or click **Email**. Click **E-Mail Report** to notify to the administrator. You can send the notification to your technician or customer by including their email addresses.

6. In the Customer profile, select the vUCC base ARID and create an associated ULM ARID:
   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
   - Click **+** beside the customer’s ID.
   - Select the option button next to the vUCC Base ARID.
   - Click the **Create ULM Record** button.
   - Enter a description for the vUCC ULM Application Record. For example: "ZZZ Industries vUCC ULM ARID".
   - Click **Submit**.
   - Click **Next**. The system displays the newly created ARID at the top of the screen. Record the vUCC ULM ARID.
   - Click **Return to License Manager**.



☑ Successfully created new application record identifier 25400373.

Group Application Record Information

Details for group application record 25400373 (ZZZ Industries vUCC Base ARID)

Group Application Record Id: 25400373

Customer: ZZZ Industries

Description: ZZZ Industries vUCC Base ARID

ARids Managed by this ULM		
ARid	Description	Task
vUCC ARid		
20651614	ZZZ Industries vUCC Base ARID	Remove

WARNING: The *Remove* button will immediately **remove** the specific server from the ULM(GAR) server so be extremely careful.

ARids you can add to this ULM		
ARid	Description	Add Server
MBG ARids you can add		

Figure 13: Create the Group ULM ARID

7. Assign the MCD SIP trunk licenses, MBG SIP trunk licenses, UCC User and SWAS licenses to the vUCC ULM ARID:
   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
   - Click **+** beside the customer's ID.
   - Select the option button next to the vUCC ULM ARID and then click **Assign**.
   - Enter the Purchase order number in the Search Criteria and click **Retrieve**.
   - Click **+** to expand the Purchase order.
   - Assign the licenses to the ULM ARID.
   - Click **Assign**.
   - Click **Allocate** to assign the licenses.
   - Review the licenses and record the ARID.
   - Click **Confirm**.
   - Click **Done** or click **Email**. Click **E-Mail Report** to notify to the administrator. You can send the notification to your technician or customer by including their email addresses.

Download vUCC OVA File

Download the vUCC OVA file from Mitel Online:

1. Launch your browser on the vSphere Client PC.
2. Log into Mitel Online at https://www.ebiz.mitel.com.
3. Click **Technical** and then click **Software Downloads**.
4. Click **vUCC**.
5. Click the appropriate vUCC Software Download version.

6. Review the Release Notes.
7. Verify that the versions of the software and applications are correct.
8. Download the required OVA file by clicking the link in the table. When you click a link, you are presented with a software **Disclaimer**.
9. Click "I Agree [Download using Software Download Manager (Recommended)]".
10. If you don't already have the Download Manager installed on your local PC, you are prompted to install it. The Download Manager is an Active X application that optimizes the software download speed. After you install the Download Manager, it is available for subsequent software downloads.
11. Save the UCC OVA file to a network drive or to a folder on your vSphere Client PC.
12. Proceed to "Deploy UCC Virtual Appliance" on page 58.

Deploy UCC Virtual Appliance

You deploy the vUCC as an image in OVF package format (file ending in OVA),   The vUCC OVA file contains the VMware tools, MSL operating system, vMAS, vMCD, and vMBG software as a pre-installed image.

Note the following requirements:

❒ vUCC is deployed in Server Gateway mode on the network edge although it can be deployed behind a corporate firewall with appropriate port forwarding rules set on the firewall. vUCC is not supported in Server-only mode.

❒ vUCC must be deployed using the vSphere Client connected to vCenter. You cannot deploy vUCC using the vSphere Client that is connected directly to an ESXi server.

❒ vCloud Director can be used for deployment but you must first convert the OVA file to OVF format. Refer to the Mitel Virtual Appliance Deployment Solutions Guide for conversion instructions.

❒ You must install vUCC in the vSphere environment using **Thick** provisioning. Thin provisioning can cause voice quality issues due to disk sharing.

❒ You must select the destination network that is associated to the local network interface (LAN) and to the external network interface (WAN). The destination network MUST be different or else a network loop is created.

❒ On the IP Allocation screen, you must select **Fixed** for the IP allocation policy.

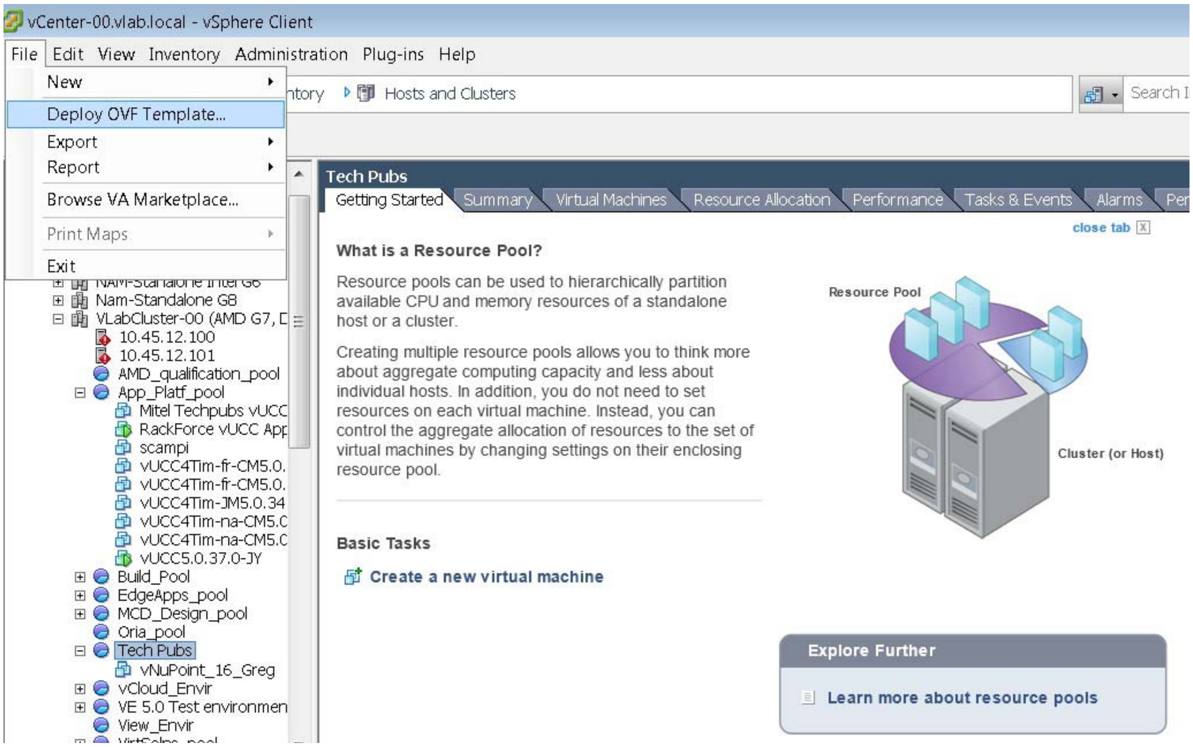
To deploy vUCC on a vCenter Server complete the following steps:

1. Launch the vSphere Client application on the network PC.
   - Click **Start > All Programs**.
   - Click **Vmware > VMware vSphere Client**.
   - Enter the IP address or hostname of the vCenter Server.
   - Enter your VMware vSphere Client username and password.
   - Click **Login**.

Note: Ensure that your PC display resolution is set to 100%. If it is set to a higher resolution, for example 125%, some IP Address fields in the VMware deployment wizard may be truncated.

2. In the vSphere Client application screen, click **File > Deploy OVF template . . .**:

Note: The screens shown in this procedure are examples only.



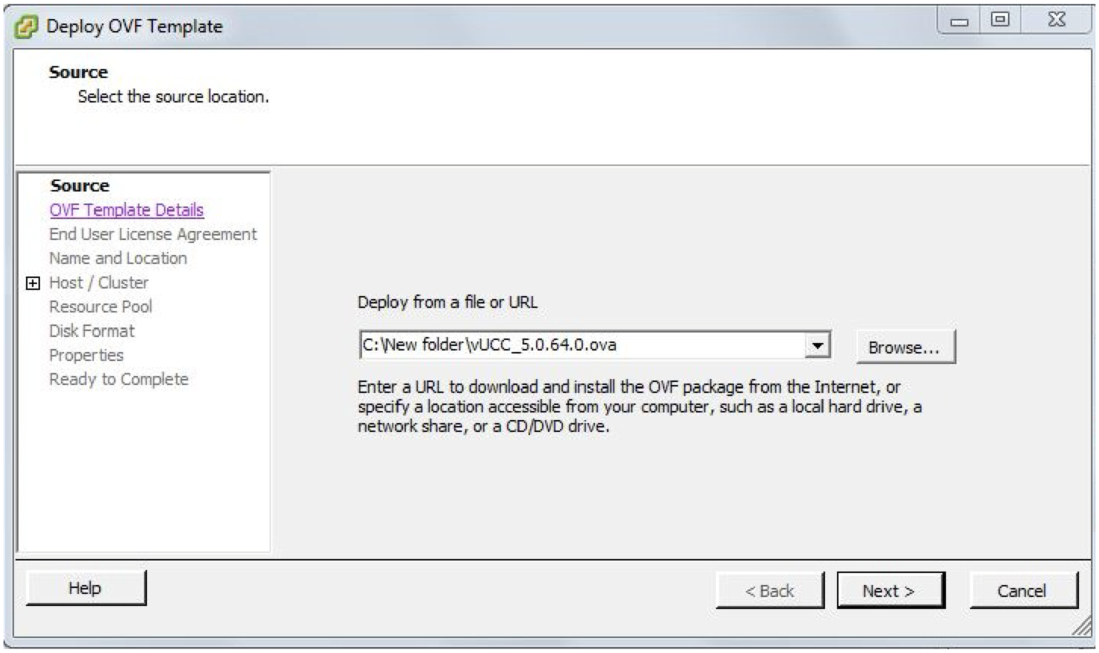
What is a Resource Pool?

Resource pools can be used to hierarchically partition available CPU and memory resources of a standalone host or a cluster.

Creating multiple resource pools allows you to think more about aggregate computing capacity and less about individual hosts. In addition, you do not need to set resources on each virtual machine. Instead, you can control the aggregate allocation of resources to the set of virtual machines by changing settings on their enclosing resource pool.

Figure 14: Deploy OVF Template

3. The *Deploy OVF Template* screen opens:


Deploy OVF Template

Source
Select the source location.

Deploy from a file or URL: C:\New folder\vUCC_5.0.64.0.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Figure 15: Deploy OVF Template

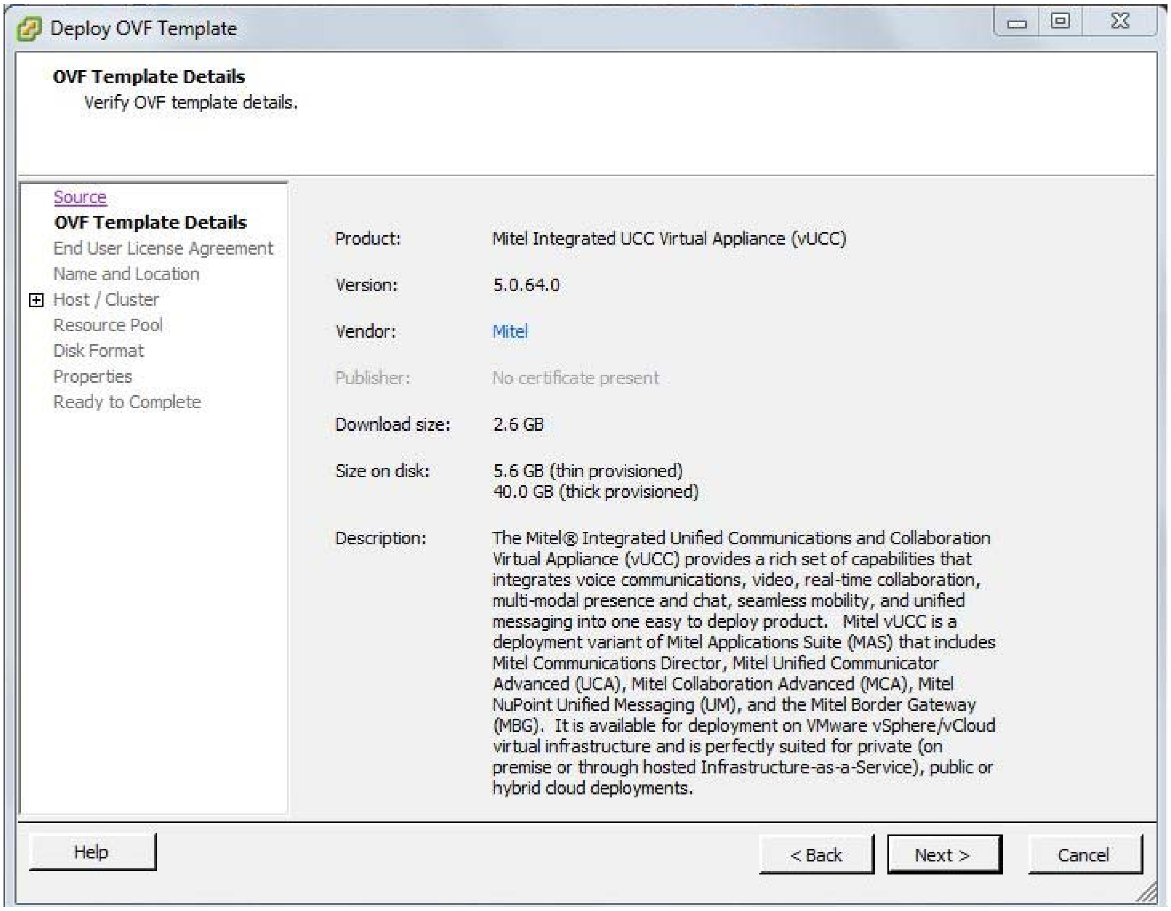
4. Specify the Source Location for the OVF template file (OVA file extension):

- **Deploy from file**
  if the OVF template file was downloaded to the local computer or to a network share drive, then click **Browse** to locate the file.
- **Deploy from URL**
  if the OVF template file is on the internet or accessible through a web browser; enter the URL of the location of the file.

Note: The filename of the OVF template cannot contain any spaces.

5. Click **Next**. The OVF Template Details screen is displayed. The Version field identifies the vUCC software version.

Note: The Version, Download Size, and Size on Disk values are examples only in the following screen capture. They will likely be different values during your installation. By default the screen displays the estimated disk size for a small business deployment.



OVF Template Details
Verify OVF template details.

Product: Mitel Integrated UCC Virtual Appliance (vUCC)

Version: 5.0.64.0

Vendor: Mitel

Publisher: No certificate present

Download size: 2.6 GB

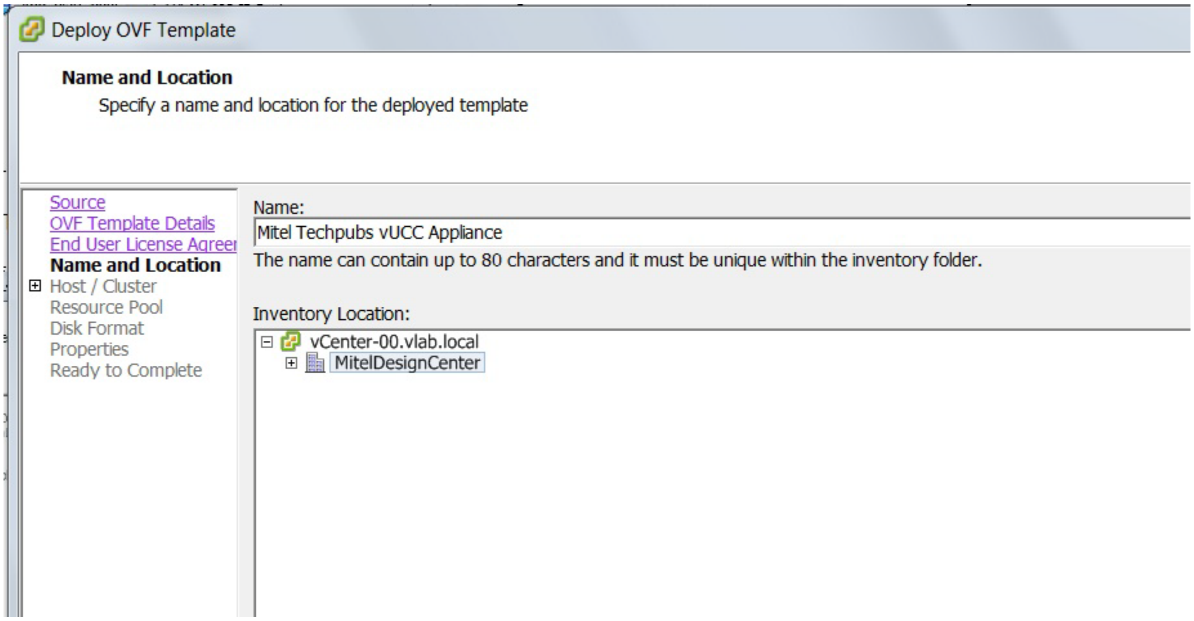
Size on disk: 5.6 GB (thin provisioned)
40.0 GB (thick provisioned)

Description: The Mitel® Integrated Unified Communications and Collaboration Virtual Appliance (vUCC) provides a rich set of capabilities that integrates voice communications, video, real-time collaboration, multi-modal presence and chat, seamless mobility, and unified messaging into one easy to deploy product. Mitel vUCC is a deployment variant of Mitel Applications Suite (MAS) that includes Mitel Communications Director, Mitel Unified Communicator Advanced (UCA), Mitel Collaboration Advanced (MCA), Mitel NuPoint Unified Messaging (UM), and the Mitel Border Gateway (MBG). It is available for deployment on VMware vSphere/vCloud virtual infrastructure and is perfectly suited for private (on premise or through hosted Infrastructure-as-a-Service), public or hybrid cloud deployments.

Figure 16: Verify OVF Template Details

6. Click **Next**. The end user license agreement screen displays.

7. Click **Accept** to accept the end-user license agreement, then click **Next**. The "Deploy OVF Template Name and Location" screen displays:


Deploy OVF Template

Name and Location

Specify a name and location for the deployed template

Name: Mitel Techpubs vUCC Appliance

The name can contain up to 80 characters and it must be unique within the inventory folder.

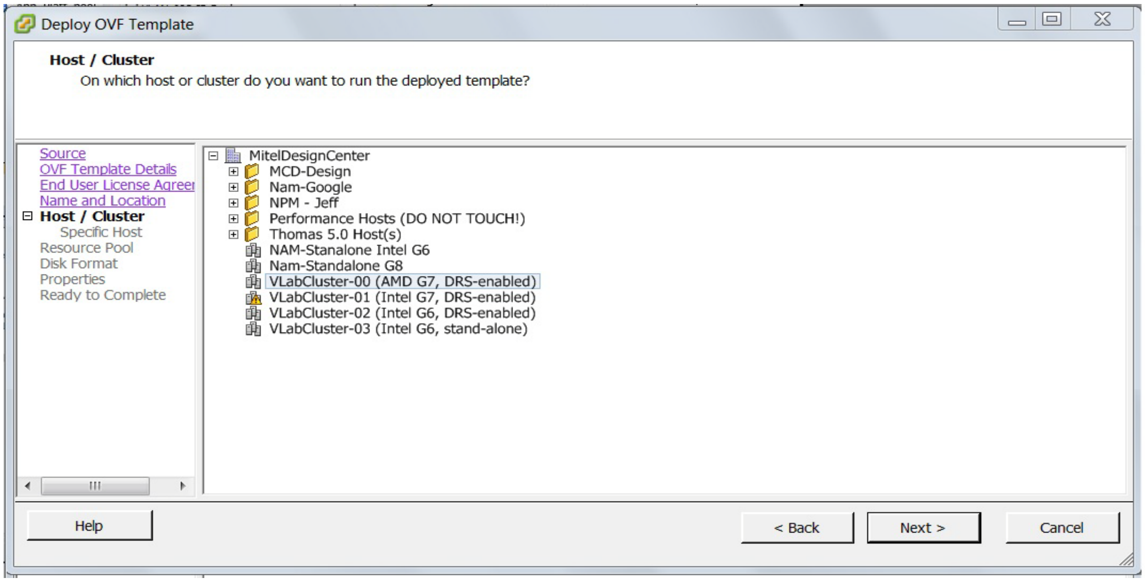
Inventory Location: vCenter-00.vlab.local > MitelDesignCenter

Figure 17: Deploy OVF Template Name and Location

8. Enter a meaningful name for the vUCC instance, or accept the default name. You must select an inventory location.

9. Click **Next**.

10. Select the Host/Cluster for the vUCC instance. Click **Next**.


Deploy OVF Template

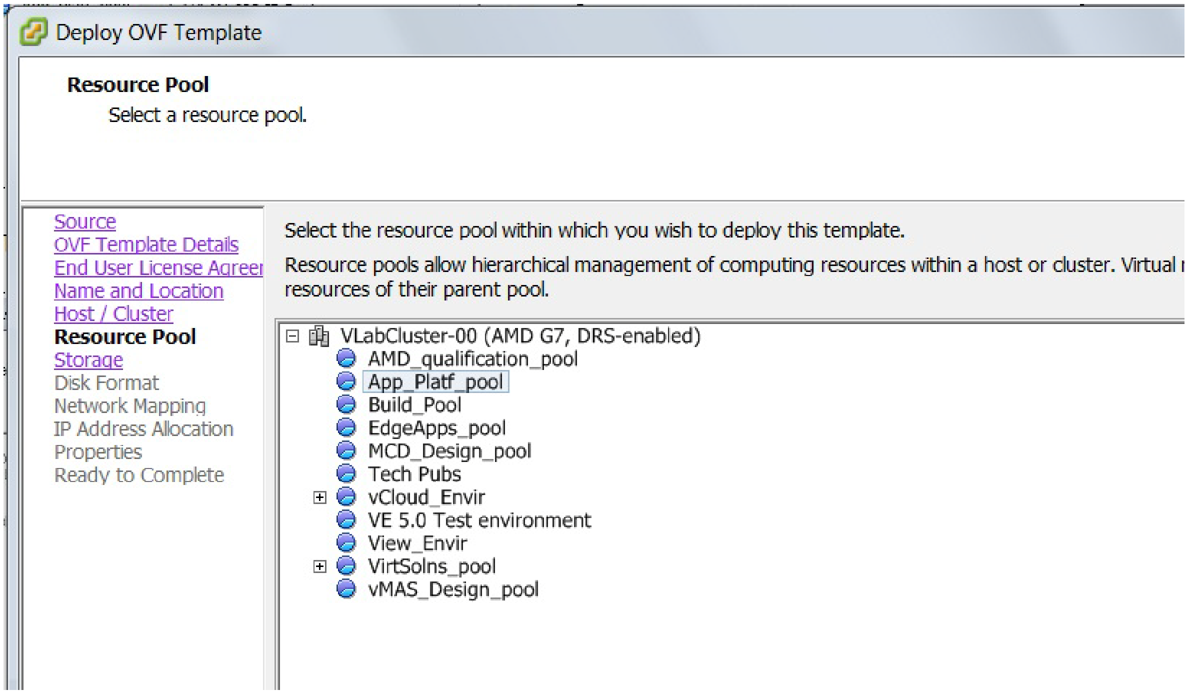
Host / Cluster

On which host or cluster do you want to run the deployed template?

MitelDesignCenter
- MCD-Design
- Nam-Google
- NPM - Jeff
- Performance Hosts (DO NOT TOUCH!)
- Thomas 5.0 Host(s)
- NAM-Stanalone Intel G6
- Nam-Standalone G8
- VLabCluster-00 (AMD G7, DRS-enabled)
- VLabCluster-01 (Intel G7, DRS-enabled)
- VLabCluster-02 (Intel G6, DRS-enabled)
- VLabCluster-03 (Intel G6, stand-alone)

Figure 18: Select Host/Cluster

11. Select the vCenter Server Resource Pool for the vUCC instance. You must deploy the vUCC instance in vCenter Server. Click **Next**.



Deploy OVF Template

Resource Pool

Select a resource pool.

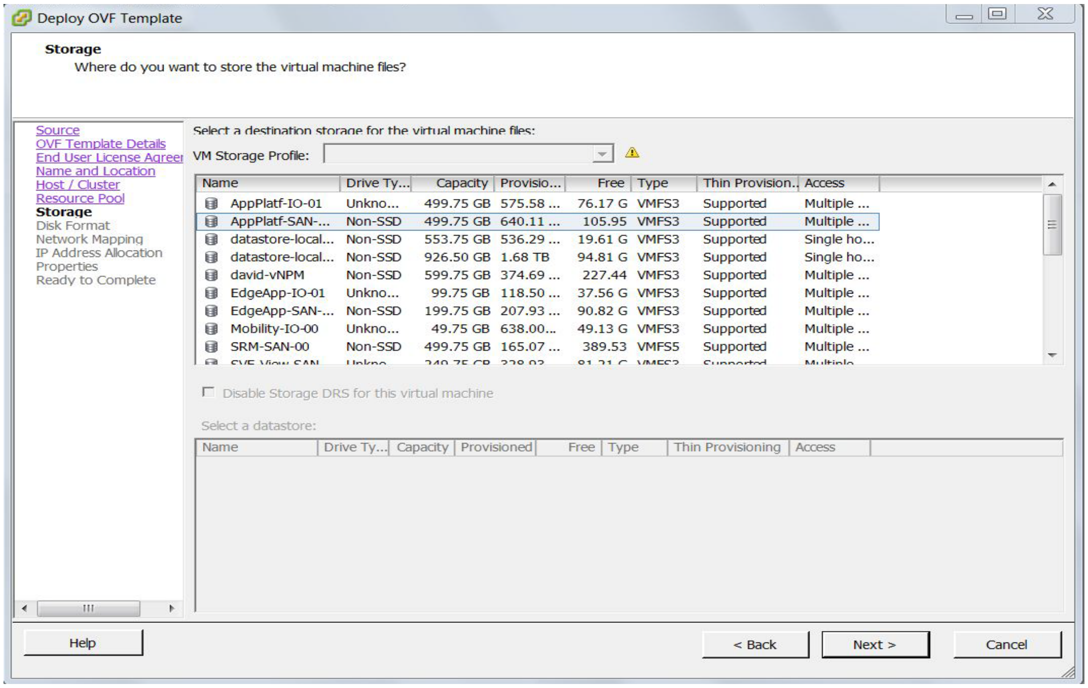
Select the resource pool within which you wish to deploy this template.

Resource pools allow hierarchical management of computing resources within a host or cluster. Virtual resources of their parent pool.

- VLabCluster-00 (AMD G7, DRS-enabled)
  - AMD_qualification_pool
  - App_Platf_pool
  - Build_Pool
  - EdgeApps_pool
  - MCD_Design_pool
  - Tech Pubs
  - vCloud_Envir
  - VE 5.0 Test environment
  - View_Envir
  - VirtSolns_pool
  - vMAS_Design_pool

Figure 19: Select Resource Pool

12. Select the Datastore where the virtual appliance files will be stored. This option only appears if multiple Datastores are available. Click **Next**.



Deploy OVF Template

Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

VM Storage Profile:

Name	Drive Ty...	Capacity	Provisio...	Free	Type	Thin Provision..	Access
AppPlatf-IO-01	Unkno...	499.75 GB	575.58 ...	76.17 G	VMFS3	Supported	Multiple ...
AppPlatf-SAN-...	Non-SSD	499.75 GB	640.11 ...	105.95	VMFS3	Supported	Multiple ...
datastore-local...	Non-SSD	553.75 GB	536.29 ...	19.61 G	VMFS3	Supported	Single ho...
datastore-local...	Non-SSD	926.50 GB	1.68 TB	94.81 G	VMFS3	Supported	Single ho...
david-vNPM	Non-SSD	599.75 GB	374.69 ...	227.44	VMFS3	Supported	Multiple ...
EdgeApp-IO-01	Unkno...	99.75 GB	118.50 ...	37.56 G	VMFS3	Supported	Multiple ...
EdgeApp-SAN-...	Non-SSD	199.75 GB	207.93 ...	90.82 G	VMFS3	Supported	Multiple ...
Mobility-IO-00	Unkno...	49.75 GB	638.00...	49.13 G	VMFS3	Supported	Multiple ...
SRM-SAN-00	Non-SSD	499.75 GB	165.07 ...	389.53	VMFS5	Supported	Multiple ...
SVE-View-SAN	Unkno...	249.75 GB	328.93	81.21 G	VMFS3	Supported	Multiple

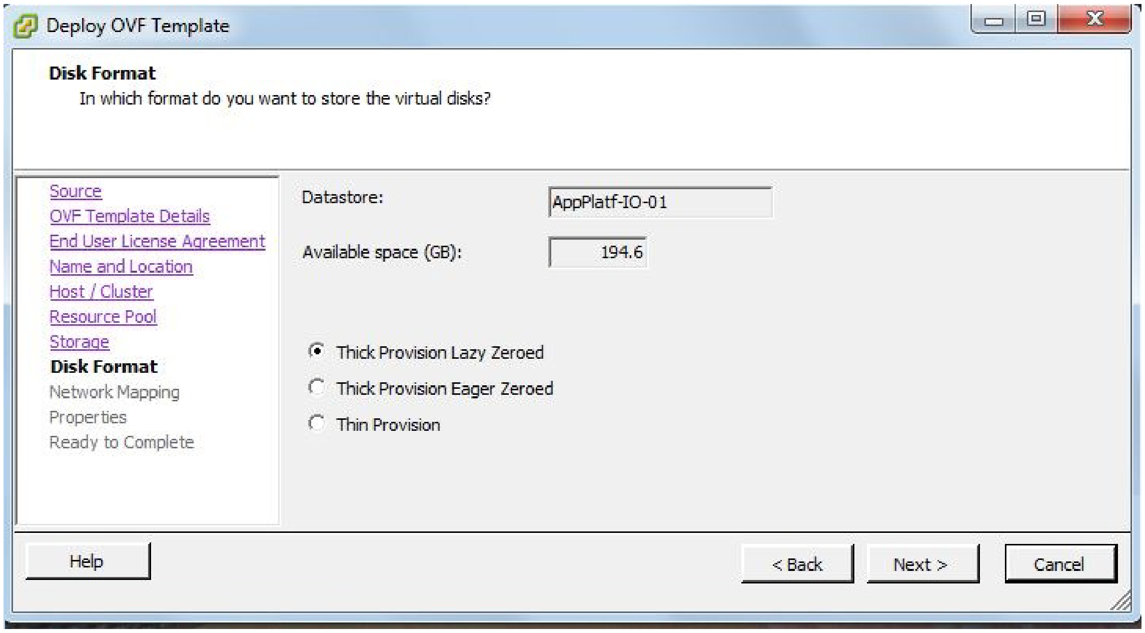
☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Ty...	Capacity	Provisioned	Free	Type	Thin Provisioning	Access

Figure 20: Select Datastore

13. In the Disk Format screen, select the **Thick Provision Lazy Zeroed** option. Refer to the *Virtual Appliance Deployment Solutions Guide* and *VMware Performance Best Practices* guide for details regarding the formatting options. Click **Next**.



Disk Format

In which format do you want to store the virtual disks?

Datastore: AppPlatf-IO-01

Available space (GB): 194.6

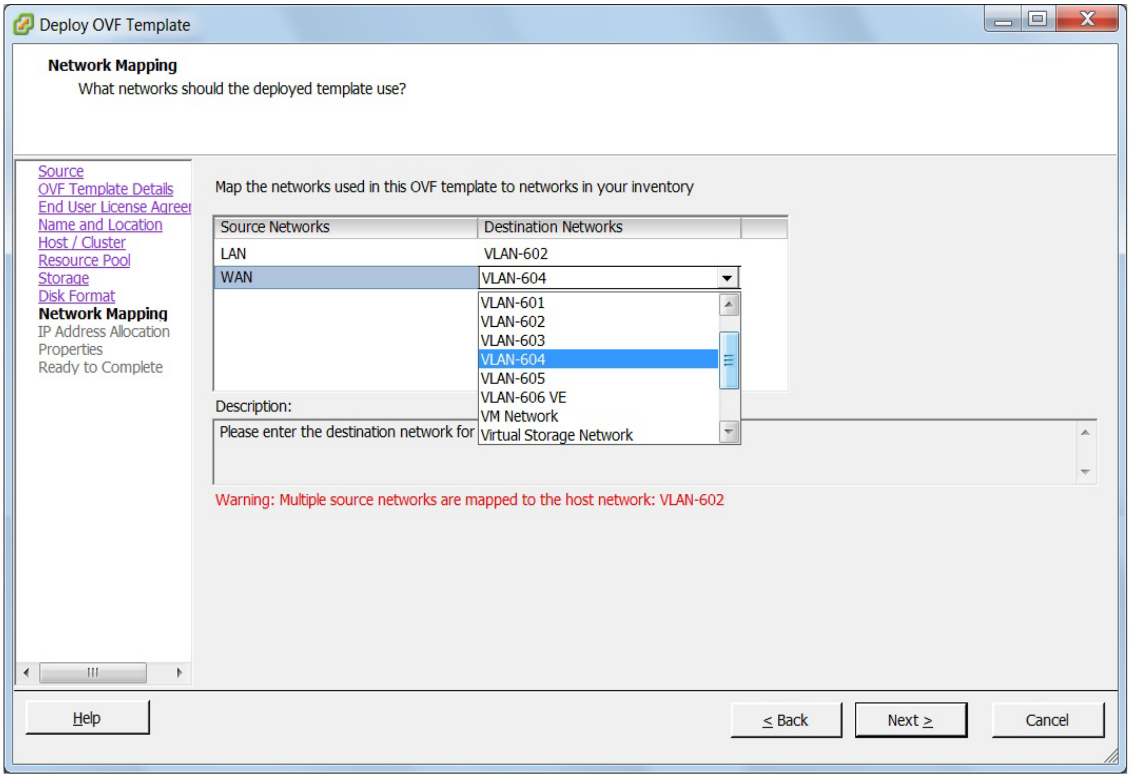
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Figure 21: Select Disk Format

14. Select the destination LAN and WAN networks for the OVF template. These are the "Associated Networks" that are assigned in the LAN and WAN IP Pools.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
LAN	VLAN-602
WAN	VLAN-604

Description:

Please enter the destination network for

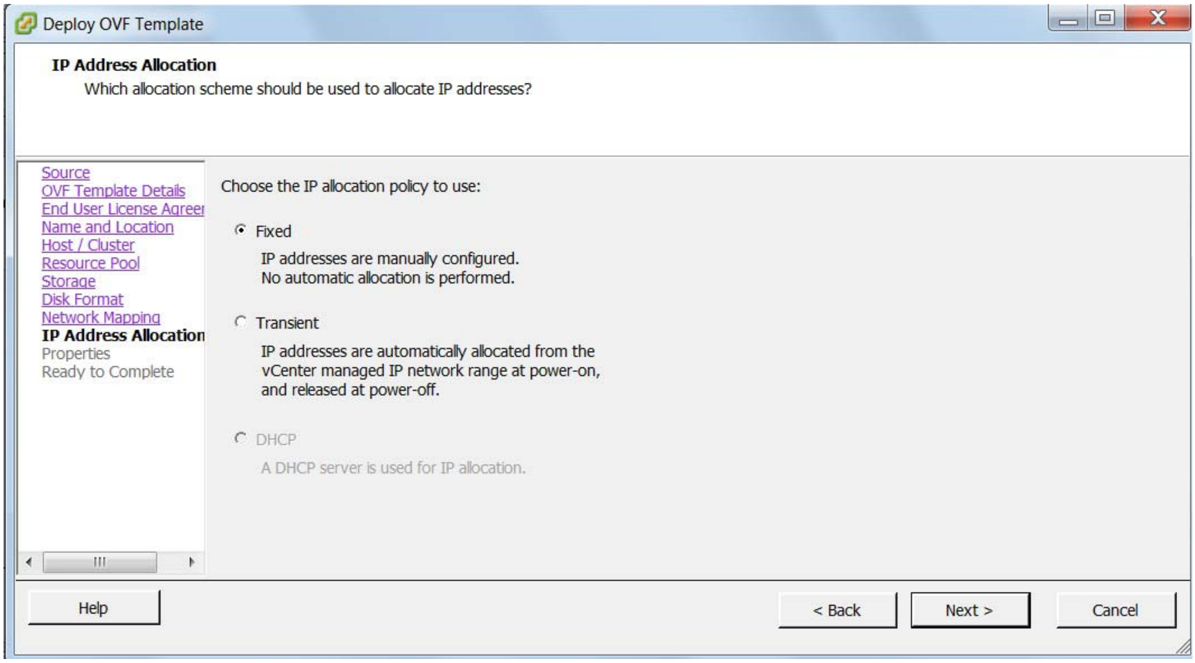
Warning: Multiple source networks are mapped to the host network: VLAN-602

Figure 22: Network Mapping Screen

15. In the IP Address Allocation screen, select the appropriate IP allocation policy:

- Select Fixed for deployments on vCenter

- Select Transient for deployments on vCloud Director.



IP Address Allocation

Which allocation scheme should be used to allocate IP addresses?

Choose the IP allocation policy to use:

● Fixed

IP addresses are manually configured.
No automatic allocation is performed.

○ Transient

IP addresses are automatically allocated from the vCenter managed IP network range at power-on, and released at power-off.

○ DHCP

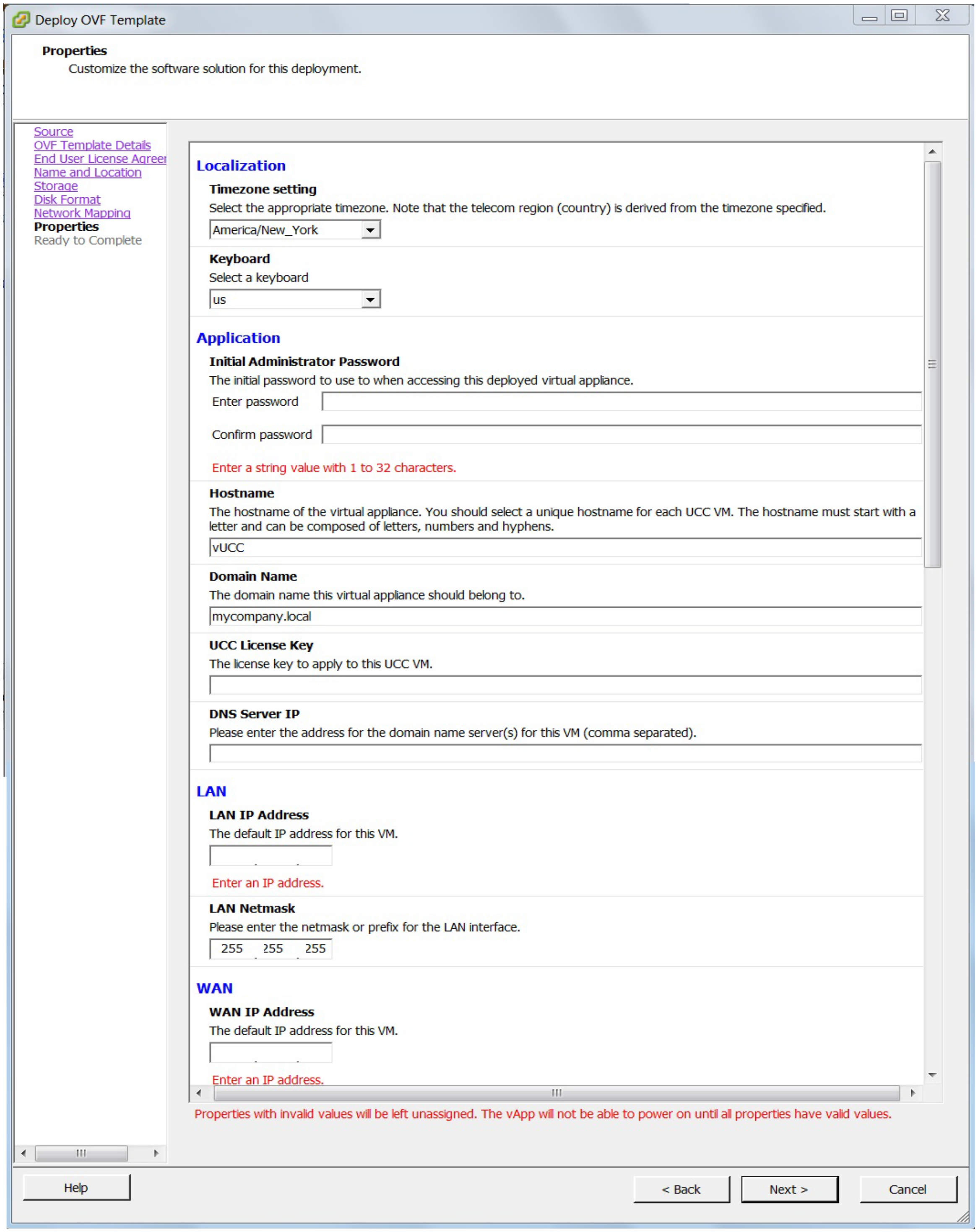
A DHCP server is used for IP allocation.

Figure 23: IP Address Allocation

16. Click **Next**. The Properties screen is displayed. Complete the fields in this screen using the information that you recorded in the "vUCC Properties of Application" section of Table 10 on page 39.

Note: You can only use the Properties screen to set the LAN IP and WAN IP addresses for the initial deployment of the appliance. After initial boot-up, you must use the MAS server console interface to modify the LAN IP or WAN IP addresses. See for page 131 for instructions.

Note: You must specify both the LAN IP and WAN IP address. Otherwise, the vUCC virtual appliance will not power on.



Properties

Customize the software solution for this deployment.

Localization

Timezone setting

Select the appropriate timezone. Note that the telecom region (country) is derived from the timezone specified.

America/New_York

Keyboard

Select a keyboard

us

Application

Initial Administrator Password

The initial password to use to when accessing this deployed virtual appliance.

Enter password

Confirm password

Enter a string value with 1 to 32 characters.

Hostname

The hostname of the virtual appliance. You should select a unique hostname for each UCC VM. The hostname must start with a letter and can be composed of letters, numbers and hyphens.

vUCC

Domain Name

The domain name this virtual appliance should belong to.

mycompany.local

UCC License Key

The license key to apply to this UCC VM.

DNS Server IP

Please enter the address for the domain name server(s) for this VM (comma separated).

LAN

LAN IP Address

The default IP address for this VM.

Enter an IP address.

LAN Netmask

Please enter the netmask or prefix for the LAN interface.

255 . 255 . 255

WAN

WAN IP Address

The default IP address for this VM.

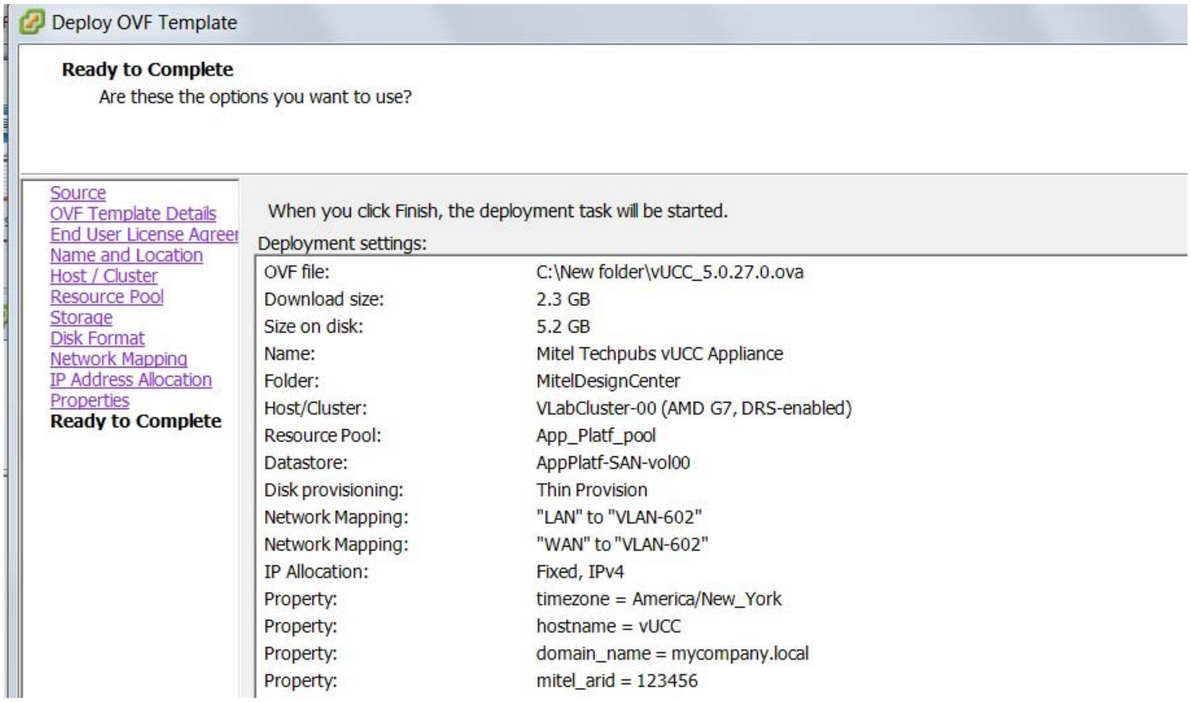
Enter an IP address.

Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.

Figure 24: Complete vUCC Application Configuration Properties

Note: To create a blank template for cloning, leave the following fields empty: Administrator Password, Hostname, Domain Name, LAN and WAN IP addresses. After you create the clones, you must complete these fields before you can proceed with deployment. See “About Cloning” on page 69 for additional details. You cannot clone an active (deployed) vUCC.

17. Click **Next**. The "Deploy OVF Template Ready to Complete" screen appears.



Deploy OVF Template

Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

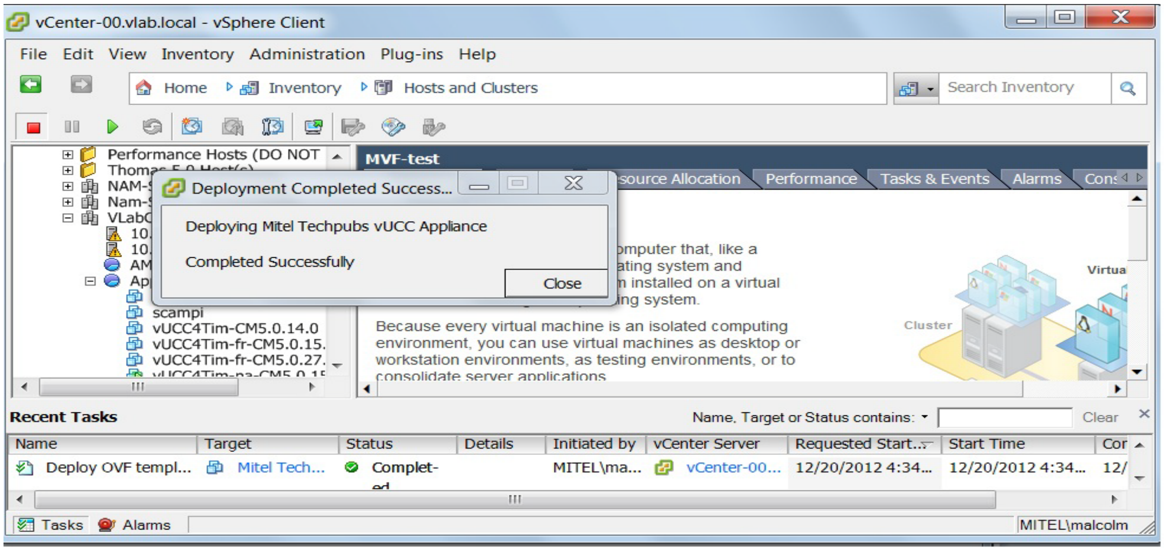
Deployment settings:

OVF file:	C:\New folder\vUCC_5.0.27.0.ova
Download size:	2.3 GB
Size on disk:	5.2 GB
Name:	Mitel Techpubs vUCC Appliance
Folder:	MitelDesignCenter
Host/Cluster:	VLabCluster-00 (AMD G7, DRS-enabled)
Resource Pool:	App_Platf_pool
Datastore:	AppPlatf-SAN-vol00
Disk provisioning:	Thin Provision
Network Mapping:	"LAN" to "VLAN-602"
Network Mapping:	"WAN" to "VLAN-602"
IP Allocation:	Fixed, IPv4
Property:	timezone = America/New_York
Property:	hostname = vUCC
Property:	domain_name = mycompany.local
Property:	mitel_arid = 123456

Figure 25: Deploy OVF Template Ready to Complete Screen

18. Review the information and click **Finish**. vSphere starts the deployment of vUCC on the server. A progress bar is displayed. The time required to deploy the vUCC depends upon your network infrastructure.

19. When the dialog indicating that the deployment is complete appears, click **Close**. The vUCC appears in the inventory list in the left side navigation pane.



Deployment Completed Success...

Deploying Mitel Techpubs vUCC Appliance

Completed Successfully

Close

mputer that, like a ating system and n installed on a virtual ing system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Recent Tasks

Name, Target or Status contains: Clear

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start...	Start Time	Cor
Deploy OVF templ...	Mitel Tech...	Complet-ed		MITEL\ma...	vCenter-00...	12/20/2012 4:34...	12/20/2012 4:34...	12/

Figure 26: vUCC Deployed Successfully

20. Proceed to “Configuration Overview” on page 73.

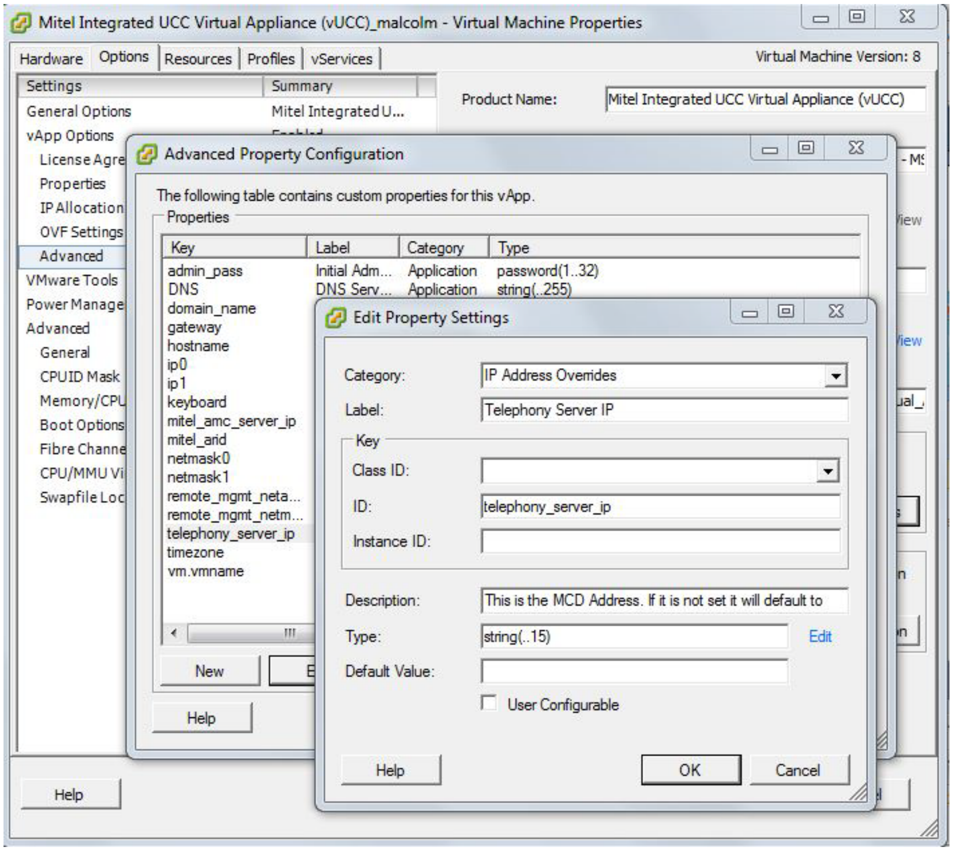
Modifying Advanced Deployment Properties

The addresses of the following deployment properties are not configurable from the Properties screen during initial deployment:

- **Mitel AMC Server IP**: Defaults to the IP address of the Mitel AMC Licensing server.
- **Remote Administration Access**: Not configured.
- **Mitel Communication Director**: Defaults to the vUCC LAN IP address +1. For example, if the vUCC LAN IP address is 10.45.102.88, the MCD address defaults to 10.45.102.89.

If necessary, you can modify the deployment properties from the vSphere Client using the following procedure:

1. In the vSphere Client screen, select the vUCC virtual appliance.
2. Ensure that the virtual appliance is shut down. You cannot edit advanced properties while the virtual appliance is running.
3. Right-click and select **Edit Settings**.
4. Click **Options**.
5. Under "vApp Options", click **Advanced**.
6. Click the **Properties** button. The Advanced Property Configuration screen opens.
7. Select the required key, click **Edit**, enter the required value in the Default Value field and click **OK** to apply:
   - **mitel_amc_server_ip**: If want to proxy the Mitel AMC server, enter the IP address of the proxy server.
   - **remote_mgmt_netaddr**: Enter the IP address of the remote management station. Remote management is optional. It is recommended that you allow access to a single IP address and set the remote_mgmt_netmask field to 255.255.255.255.
   - **remote_mgmt_netmask**: Enter the netmask of remote management stations.
   - **telephony_server_ip**: Enter the IP address of the MCD system.



Product Name: Mitel Integrated UCC Virtual Appliance (vUCC)

The following table contains custom properties for this vApp.

Key	Label	Category	Type
admin_pass	Initial Adm...	Application	password(1..32)
DNS	DNS Serv...	Application	string(..255)
domain_name			
gateway			
hostname			
ip0			
ip1			
keyboard			
mitel_amc_server_ip			
mitel_arid			
netmask0			
netmask1			
remote_mgmt_neta...			
remote_mgmt_netm...			
telephony_server_ip			
timezone			
vm.vmname			

Category: IP Address Overrides

Label: Telephony Server IP

Class ID:

ID: telephony_server_ip

Instance ID:

Description: This is the MCD Address. If it is not set it will default to

Type: string(..15)

Default Value:

☐ User Configurable

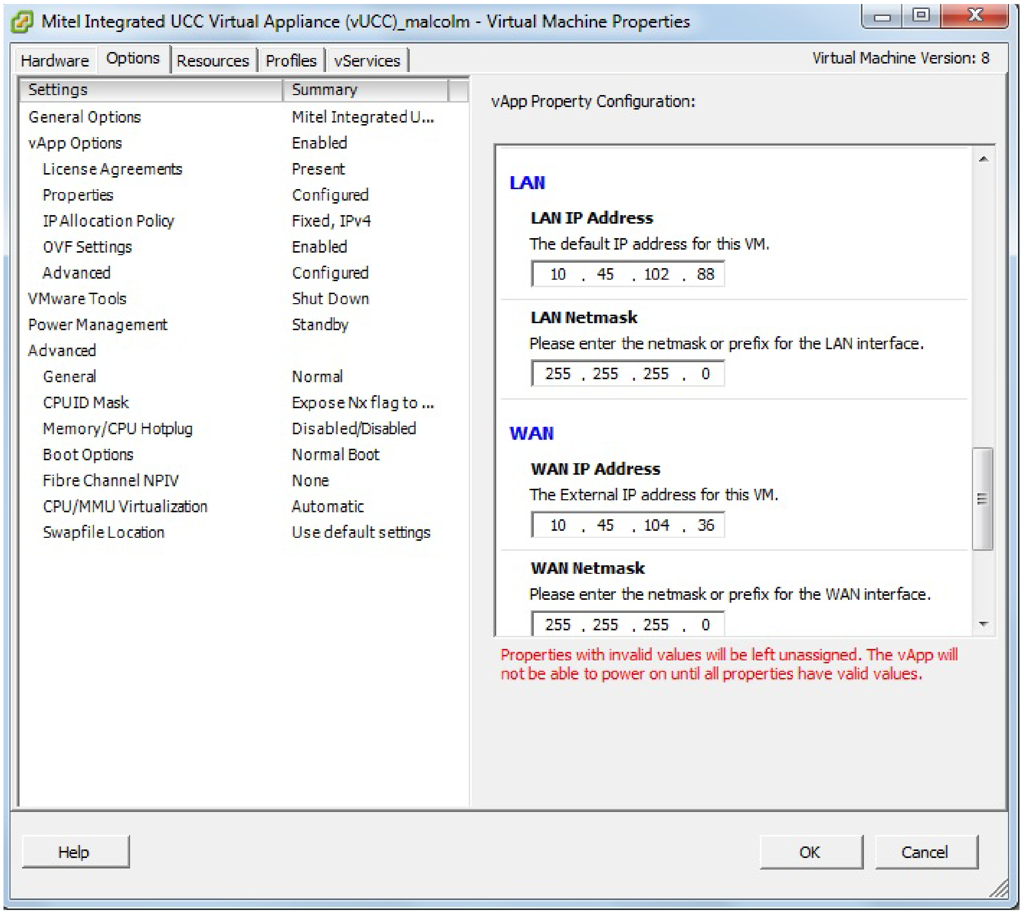
Figure 27: Advanced Property Configuration Screens

About Cloning

If you need to deploy multiple vUCC sites, you can create a VMware blank template of the UCC virtual appliance and clone it as a starting point for the new sites.

Note: This is the only supported method of cloning. After you create a clone, you must run the wizard on it. Cloning from a configured vUCC is not supported.

1. Create the VMware template. Refer to VMware documentation for instructions.
2. Deploy the VMware template. Leave the Administrator Password, Hostname, Domain Name, LAN and WAN IP addresses blank at deployment time. Do not power on the VMware template after you have deployed it.
3. Create the new vUCC by cloning from the template.
4. Prior to powering on the new vUCC, specify its IP addresses and application configuration from the VM "Edit Settings > Option > vApp Options > Properties" tab.



Mitel Integrated UCC Virtual Appliance (vUCC)_malcolm - Virtual Machine Properties

Virtual Machine Version: 8

Settings	Summary
General Options	Mitel Integrated U...
vApp Options	Enabled
License Agreements	Present
Properties	Configured
IP Allocation Policy	Fixed, IPv4
OVF Settings	Enabled
Advanced	Configured
VMware Tools	Shut Down
Power Management	Standby
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Memory/CPU Hotplug	Disabled/Disabled
Boot Options	Normal Boot
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

vApp Property Configuration:

LAN

LAN IP Address

The default IP address for this VM.

10 . 45 . 102 . 88

LAN Netmask

Please enter the netmask or prefix for the LAN interface.

255 . 255 . 255 . 0

WAN

WAN IP Address

The External IP address for this VM.

10 . 45 . 104 . 36

WAN Netmask

Please enter the netmask or prefix for the WAN interface.

255 . 255 . 255 . 0

Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.

Figure 28: Specify vUCC Virtual Machine Properties

5. After you power on the new vUCC, enter the https://<*vUCC LAN IP Address*> in your browser to launch the Initial Configuration Wizard.
6. Run the Initial Configuration Wizard to configure the system (see “Run the Wizard” on page 76).

Chapter 5

Configure System

Configuration Overview

To configure the vUCC, complete the following tasks:

- □ “Configure Remote Access to vUCC
- □ “Power on vUCC” on page 74
- □ “Run the Wizard” on page 76
- □ “Perform Advanced Configuration” on page 90
- □ “Configure Optional Standalone vMBGs” on page 101
- □ “Provision Users” on page 108
- □ “Perform Backups” on page 110

Caution:You must complete the Mitel Integrated Wizard before you log into an MCD Administration session. The first time that you log into the MCD System Administration Tool. it prompts you to change your password. After you change the MCD System Administration Tool password you will be unable to run the wizard.

Configure Remote Access to vUCC

If required, you can set up a remote access to the vUCC to allow the wizard to be run remotely over the Internet. Prior to powering on the vUCC:

1. In the vSphere Client screen, select the vUCC.
2. Right-click and select **Edit Settings**.
3. Click **Options**.
4. Under "vApp Options", click **Advanced**.
5. Click the **Properties** button. The Advanced Property Configuration screen opens.
6. Select the required key, click **Edit**, enter the required value in the Default Value field and click OK to apply
    - **remote_mgmt_netaddr**: Enter the IP address of the remote management station. Remote management is optional. It is recommended that you allow access to a single IP address and set the remote_mgmt_netmask field to 255.255.255.255.
    - **remote_mgmt_netmask**: Enter the netmask of remote management stations.

Note: The above procedure gives you remote access to the vUCC server manager and Integrated Configuration Wizard. It does not provide remote access to the MCA System Administration Tool.

Power on vUCC

1. Right-click on the newly created vUCC (for example: vUCC 5.2.3.0 build) and select **Open Console**. The vUCC virtual appliance console opens within the vSphere Client.

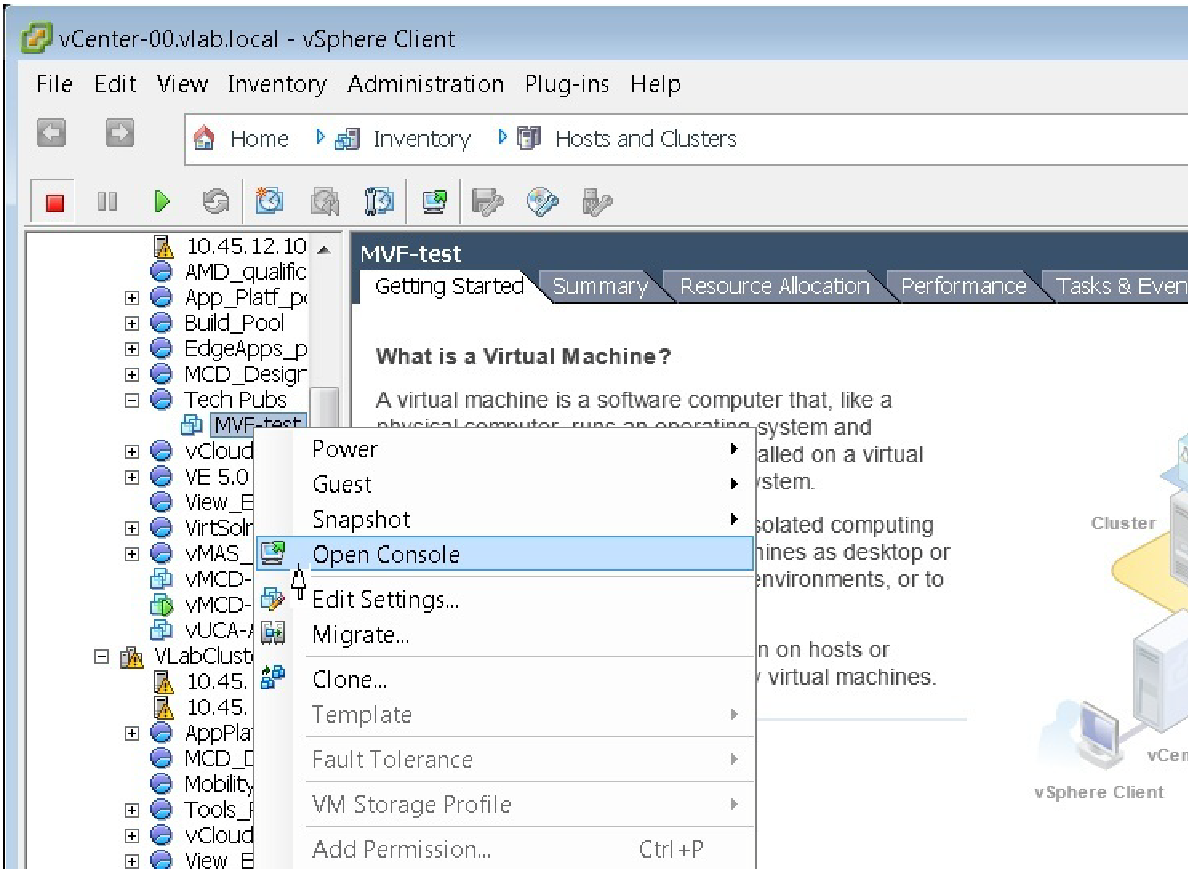


Figure 29: Opening the MSL Server Console

2. Power on the vUCC VM by clicking the green button in the toolbar.

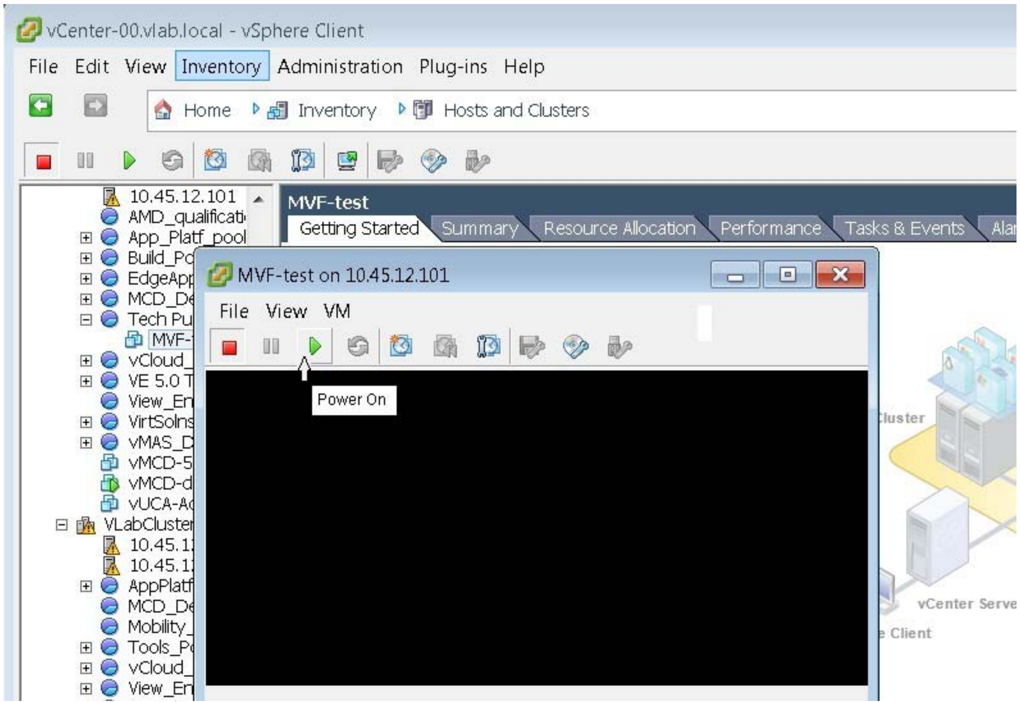
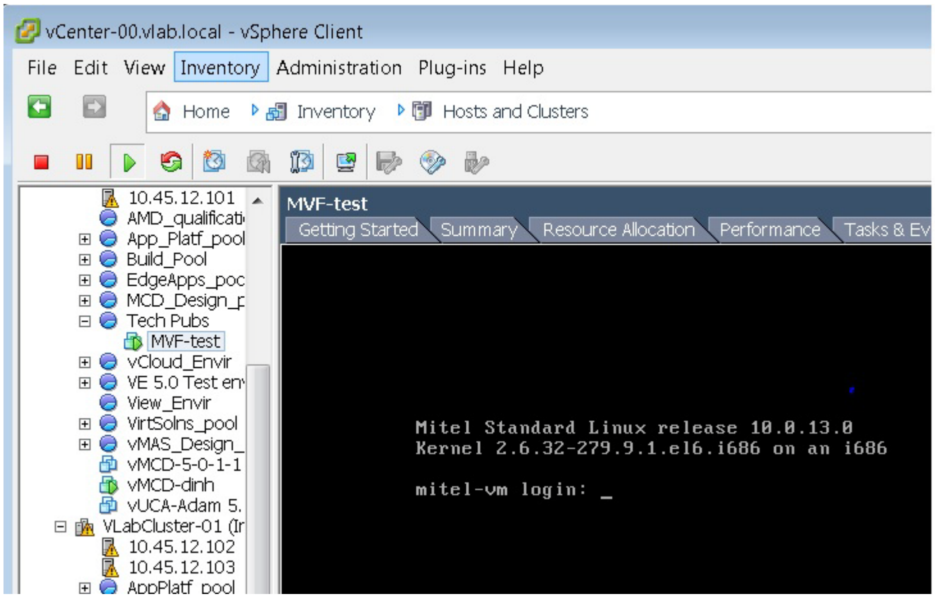

vCenter-00.vlab.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
MVF-test
Getting Started Summary Resource Allocation Performance Tasks & Events
MVF-test on 10.45.12.101
File View VM
Power On
10.45.12.101
AMD_qualificati
App_Platf_pool
Tech Pu
VLabCluster
vCenter Serve
Client

Figure 30: Power on vUCC

3. Click **Console**. The system boot up progress messages are displayed in the Console screen. When the system is finished booting up, the **mitel-vm login:** _ prompt is displayed. Do not log in at this prompt. Instead, you will log into the MAS server manager via your web browser and run the Initial Configuration Wizard.



```
Mitel Standard Linux release 10.0.13.0
Kernel 2.6.32-279.9.1.el6.i686 on an i686

mitel-vm login: _
```

Figure 31: System Boot Complete

4. Proceed to “Run the Wizard” on page 76.

Run the Wizard

Note that the values shown in the following screens are examples only.

1. Before you begin, ensure that you have assigned the following minimum number of licenses to the vUCC base ARID:
   - one Standard or Premium UCC User license,
   - two MCD SIP Trunking Licenses, and
   - if using internal SIP trunking, two MBG SIP Trunking Channel Licenses.

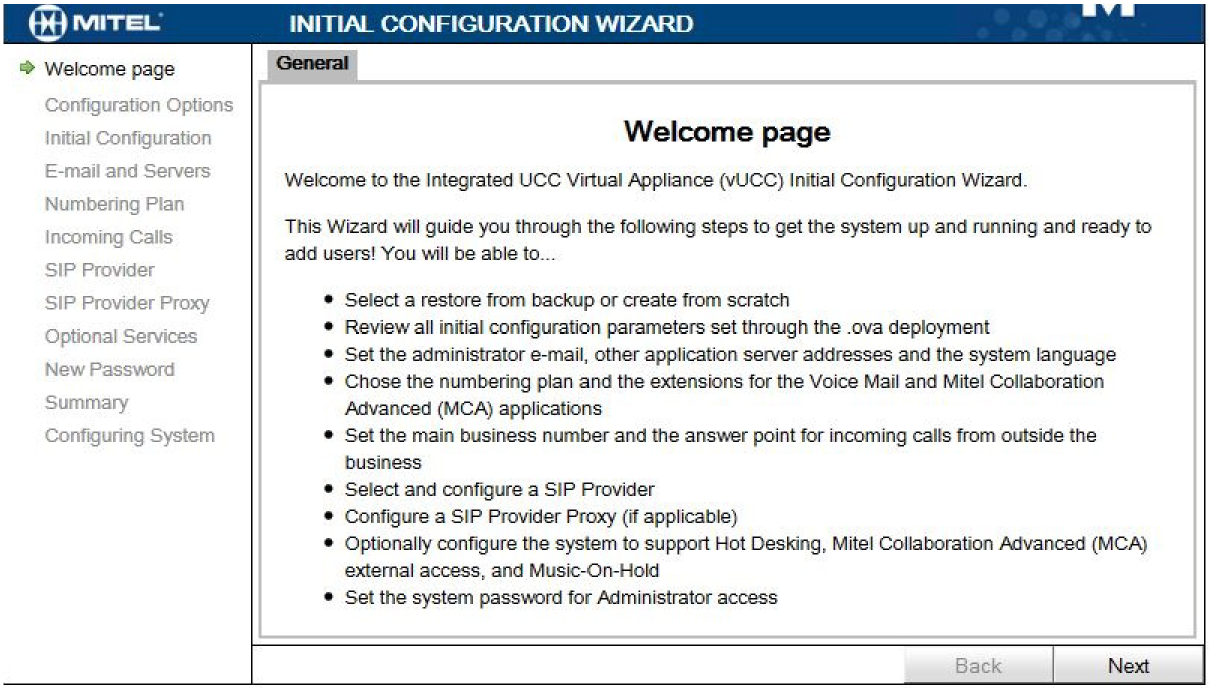
   The Initial Configuration Wizard requires these licenses in order to complete configuration of the system.

2. On a PC on the same subnet as the vUCC open your browser and enter the following in the address bar:
   https://*<LAN IP Address of the vUCC>*

Note: See Table 10, “Collect vUCC Properties of Application,” on page 39 for the LAN IP Address of the vUCC.

Note: Prior to running the Configuration Wizard, the *<LAN IP Address of the vUCC>* directs you to the Initial Configuration Wizard. After you successfully complete the wizard, it directs you to the My Unified Communications portal (end-user) interface

3. The Initial Configuration Wizard Welcome screen opens.
   - The wizard applies defaults to a majority of the vUCC configuration settings. See “System Defaults” on page 135 for details.
   - During the wizard, use the information that you collected in the *vUCC Site Specific Provisioning* section of Table 10 on page 39 to complete the fields that are not defaulted.



Welcome page

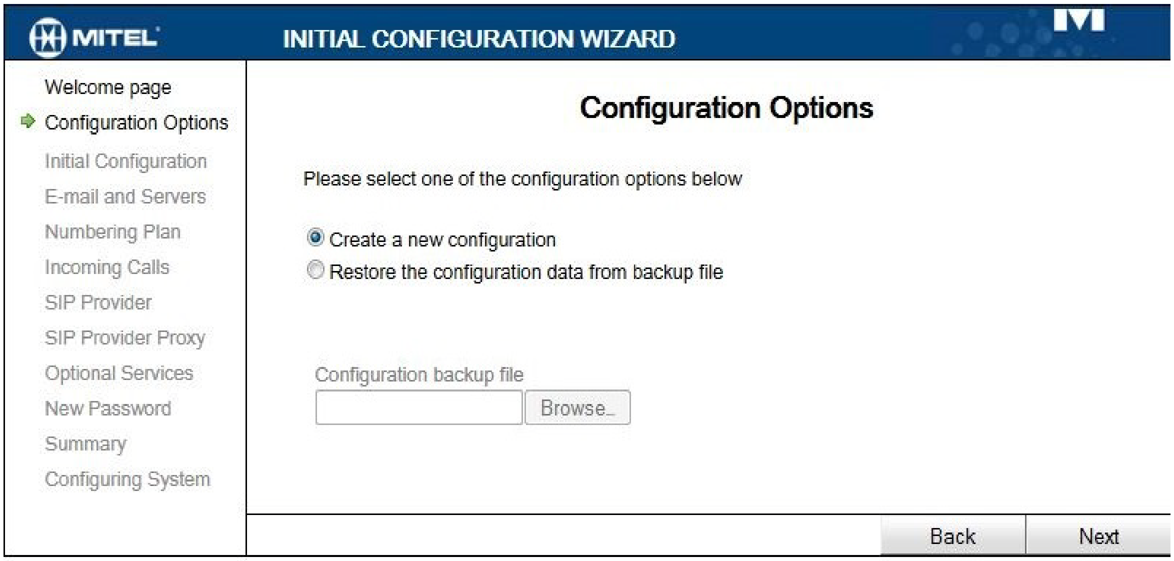
Welcome to the Integrated UCC Virtual Appliance (vUCC) Initial Configuration Wizard.

This Wizard will guide you through the following steps to get the system up and running and ready to add users! You will be able to...

- Select a restore from backup or create from scratch
- Review all initial configuration parameters set through the .ova deployment
- Set the administrator e-mail, other application server addresses and the system language
- Chose the numbering plan and the extensions for the Voice Mail and Mitel Collaboration Advanced (MCA) applications
- Set the main business number and the answer point for incoming calls from outside the business
- Select and configure a SIP Provider
- Configure a SIP Provider Proxy (if applicable)
- Optionally configure the system to support Hot Desking, Mitel Collaboration Advanced (MCA) external access, and Music-On-Hold
- Set the system password for Administrator access

Figure 32: Initial Configuration Wizard - Welcome

4. Click **Next.** The Configuration Options screen is displayed. Since you are deploying a new vUCC site, click **Create a new configuration**.



Configuration Options

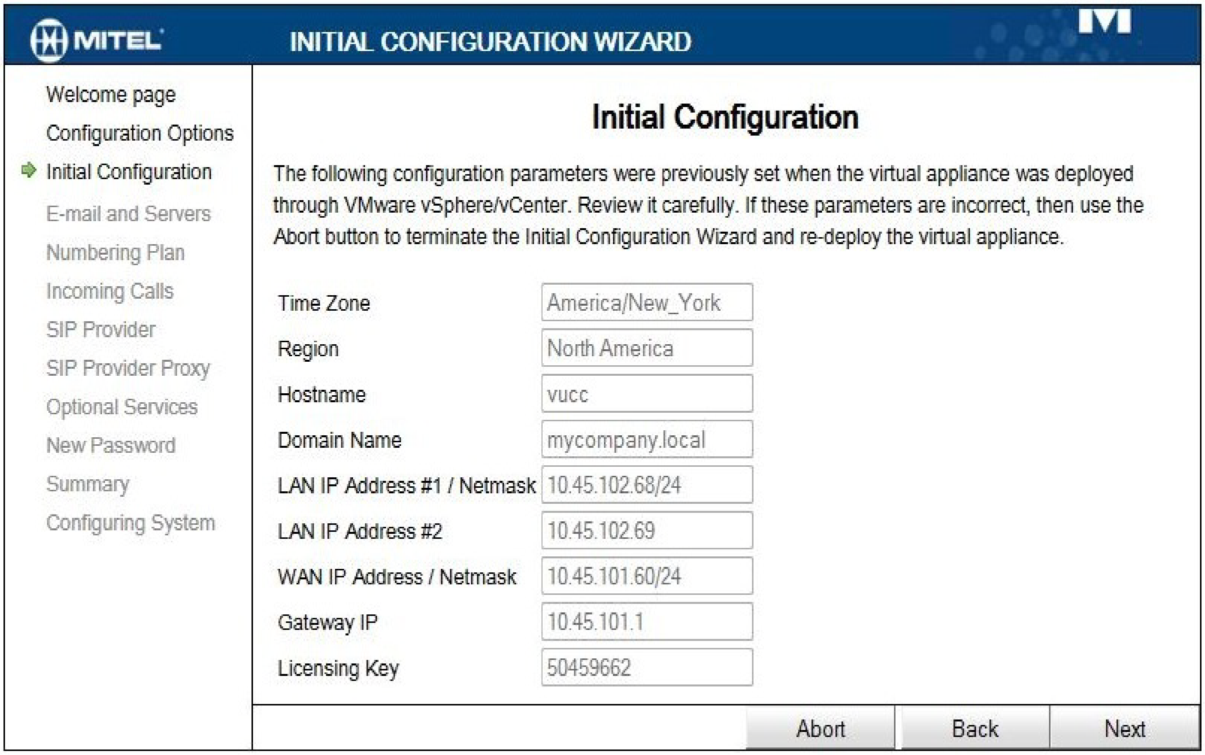
Please select one of the configuration options below

● Create a new configuration
○ Restore the configuration data from backup file

Configuration backup file

Figure 33: Configuration Options

5. Click **Next**. The Review Initial Configuration screen is displayed. Review the IP network addresses that you configured during the deployment of the OVA.



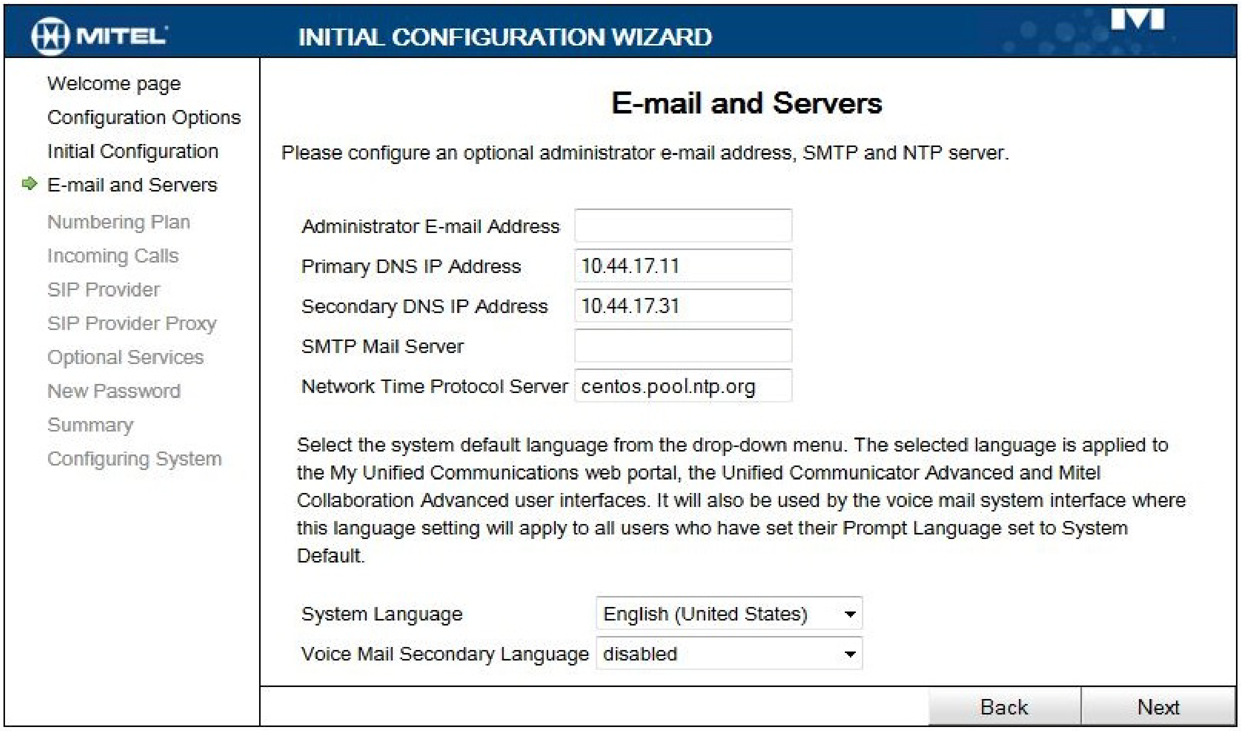
Initial Configuration

The following configuration parameters were previously set when the virtual appliance was deployed through VMware vSphere/vCenter. Review it carefully. If these parameters are incorrect, then use the Abort button to terminate the Initial Configuration Wizard and re-deploy the virtual appliance.

Time Zone	America/New_York
Region	North America
Hostname	vucc
Domain Name	mycompany.local
LAN IP Address #1 / Netmask	10.45.102.68/24
LAN IP Address #2	10.45.102.69
WAN IP Address / Netmask	10.45.101.60/24
Gateway IP	10.45.101.1
Licensing Key	50459662

Figure 34: Review Initial Configuration

6. Click **Next.** After the system validates the LAN IP Address # 2 and Licensing key, the E-mail and Servers screen is displayed. Complete the following:
   - *Administrative E-mail Address*:
   - *Corporate DNS IP Address:*
   - *Secondary DNS IP Address*:
   - *SMTP mail server*:
   - *Network Time Server*:
   - *System Language*: Identify the MAS default language. The selected language is applied to the My Unified Communication portals and the Telephone User Interfaces (TUIs) for the MAS application end-users
   - *Voice Mail Secondary Language*: Identify the language of the secondary NuPoint prompts.



E-mail and Servers

Please configure an optional administrator e-mail address, SMTP and NTP server.

Administrator E-mail Address	
Primary DNS IP Address	10.44.17.11
Secondary DNS IP Address	10.44.17.31
SMTP Mail Server	
Network Time Protocol Server	centos.pool.ntp.org

Select the system default language from the drop-down menu. The selected language is applied to the My Unified Communications web portal, the Unified Communicator Advanced and Mitel Collaboration Advanced user interfaces. It will also be used by the voice mail system interface where this language setting will apply to all users who have set their Prompt Language set to System Default.

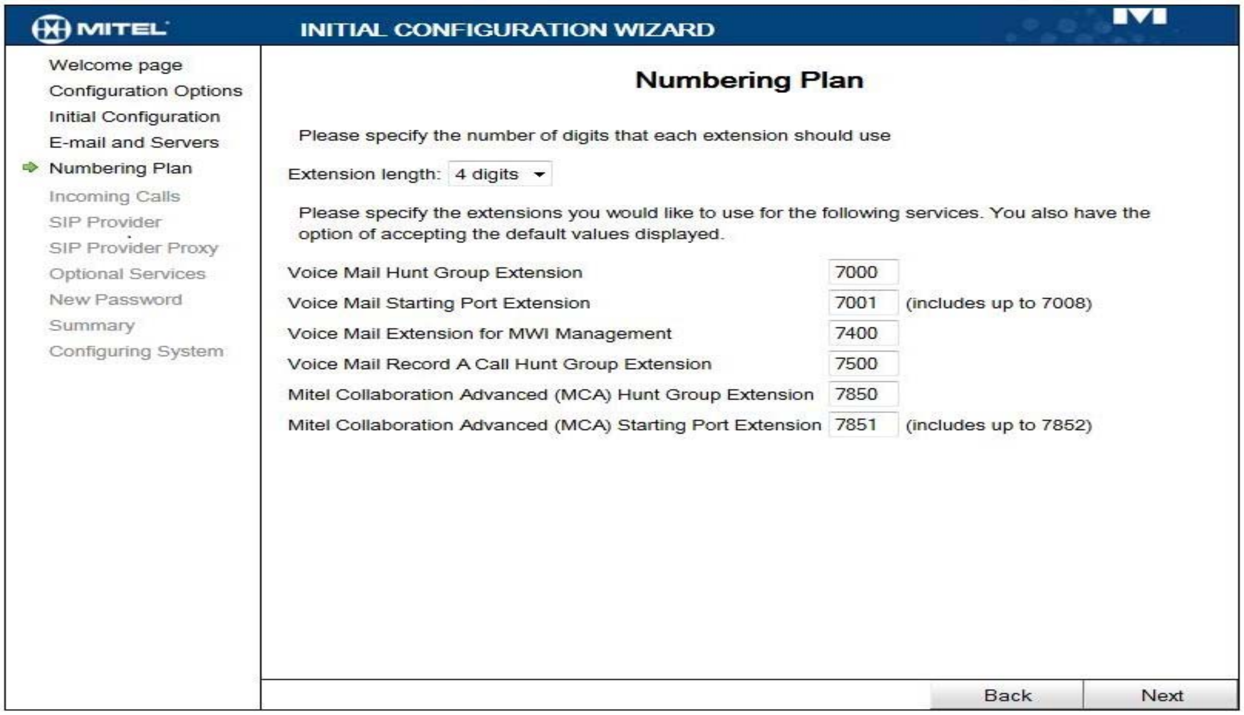
System Language	English (United States)
Voice Mail Secondary Language	disabled

Figure 35: E-mail and Servers

7. Click **Next**. The Numbering Plan screen is displayed.

   Extension Length: Set the length from (3 to 5 digits) of the system extension numbers.

   Hunt groups are used to route incoming calls to a group of designated extensions or application ports. A hunt group consists of a hunt group extension number (pilot number) and a group of member extension numbers or ports. Calls to the hunt group extension ring the first idle member in the group. Enter the hunt group extension numbers and starting port extensions for the hunt groups or use the default settings provided.



Numbering Plan

Please specify the number of digits that each extension should use

Extension length: 4 digits

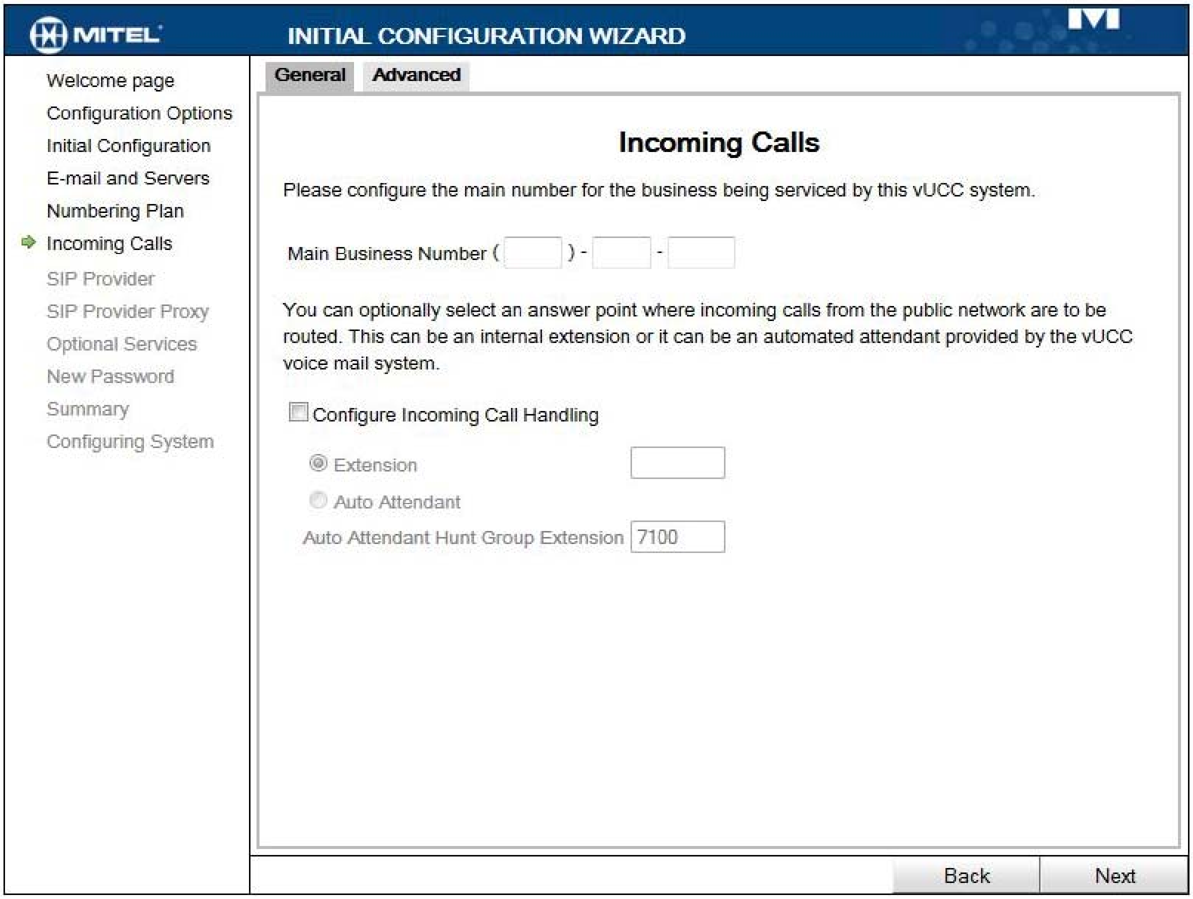
Please specify the extensions you would like to use for the following services. You also have the option of accepting the default values displayed.

Voice Mail Hunt Group Extension	7000	
Voice Mail Starting Port Extension	7001	(includes up to 7008)
Voice Mail Extension for MWI Management	7400	
Voice Mail Record A Call Hunt Group Extension	7500	
Mitel Collaboration Advanced (MCA) Hunt Group Extension	7850	
Mitel Collaboration Advanced (MCA) Starting Port Extension	7851	(includes up to 7852)

Figure 36: Numbering Plan

8. Click **Next**. The Incoming Calls screen is displayed. Incoming calls on the SIP trunks can ring a Main Business Number or a system extension.

   - *Main Business Number*: Enter the phone number of the site. External callers dial this number to place incoming calls on these SIP trunks.
     OR
   - Check the Configure Incoming Call Handling box
     - select **Extension** and enter the number that is to receive incoming calls. Note that the wizard creates an additional deviceless extension that is programmed as an External Hot Desk User (EHDU) extension. This additional extension allows a UCA softphone to be used as an answer point. For example, if 1000 is programmed as an answer point then 1*00 will be programmed as this additional extension (that is, the last digit is dropped). The EHDU extension is twinned to the answer point. Note that after you complete the wizard, you must log into MAS USP and configure the EHDU number for the Auto Attendant extension.
       OR
     - Select **Auto Attendant** and enter the Hunt Group Extension number to be used for the voice mail system's auto attendant. Note that two voice mail extensions are used to support this service.



Incoming Calls

Please configure the main number for the business being serviced by this vUCC system.

Main Business Number ( ) - -

You can optionally select an answer point where incoming calls from the public network are to be routed. This can be an internal extension or it can be an automated attendant provided by the vUCC voice mail system.

□ Configure Incoming Call Handling

● Extension

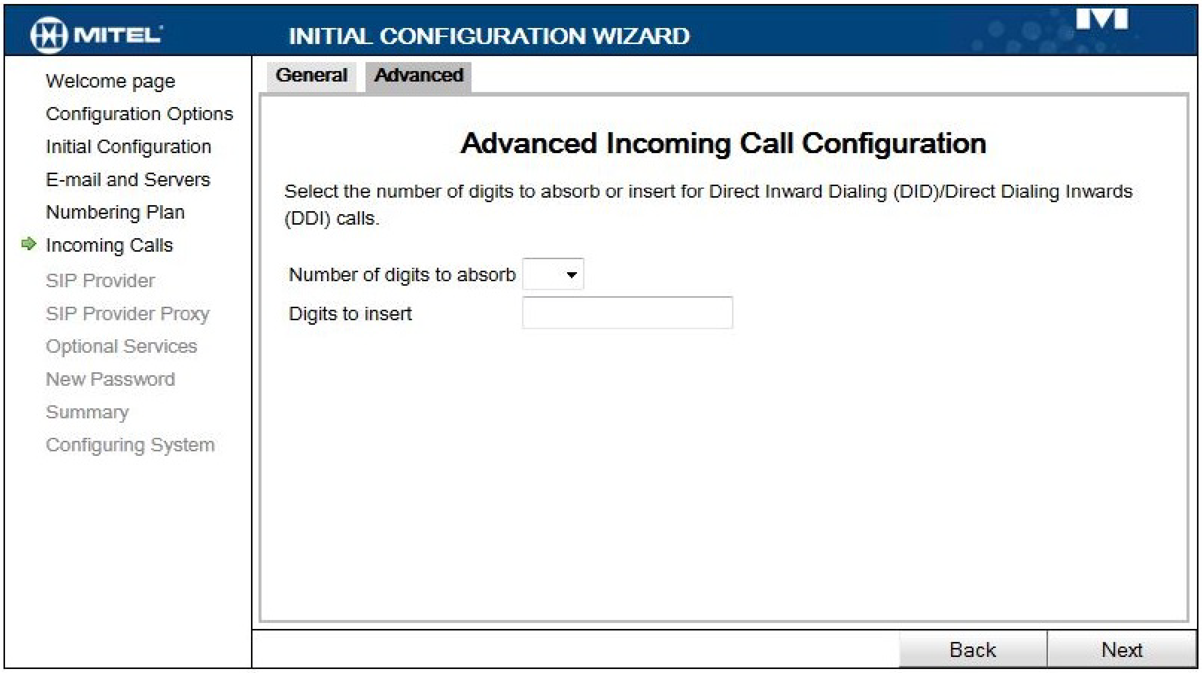
○ Auto Attendant

Auto Attendant Hunt Group Extension 7100

Figure 37: Incoming Calls

9. Click the **Advanced** tab**.** The Advanced Incoming Call Configuration Screen opens. To program Direct Inward Dialing (DID)/Direct Dialing Inwards to a range of directory numbers:

    - In the "Number of digits to absorb" field, enter the number of leading digits to remove from the incoming DID number. For example, to remove the entire DID number 613 592 5661, enter 10. Note that Dial-in trunks used as incoming trunks must always have an entry in the Absorb column. (You must enter "0" if no digits are to be absorbed. If you leave this field as Blank, calls will fail).
    - In the "Digits to insert" field, enter the actual digits to insert as leading digits to form a directory number (for example, 3333). For vUCC systems, the maximum number of digits is 4. Both the Answer Point and Digit Modification columns are left blank if the trunk is outgoing only. If a Dial-In trunk does not require digit modification, enter "0" in the Absorb field and leave the Insert field blank. Note that the Extension field and the DID Digit Modification fields are mutually exclusive. If one option is completed, the other must be left blank.



Advanced Incoming Call Configuration

Select the number of digits to absorb or insert for Direct Inward Dialing (DID)/Direct Dialing Inwards (DDI) calls.

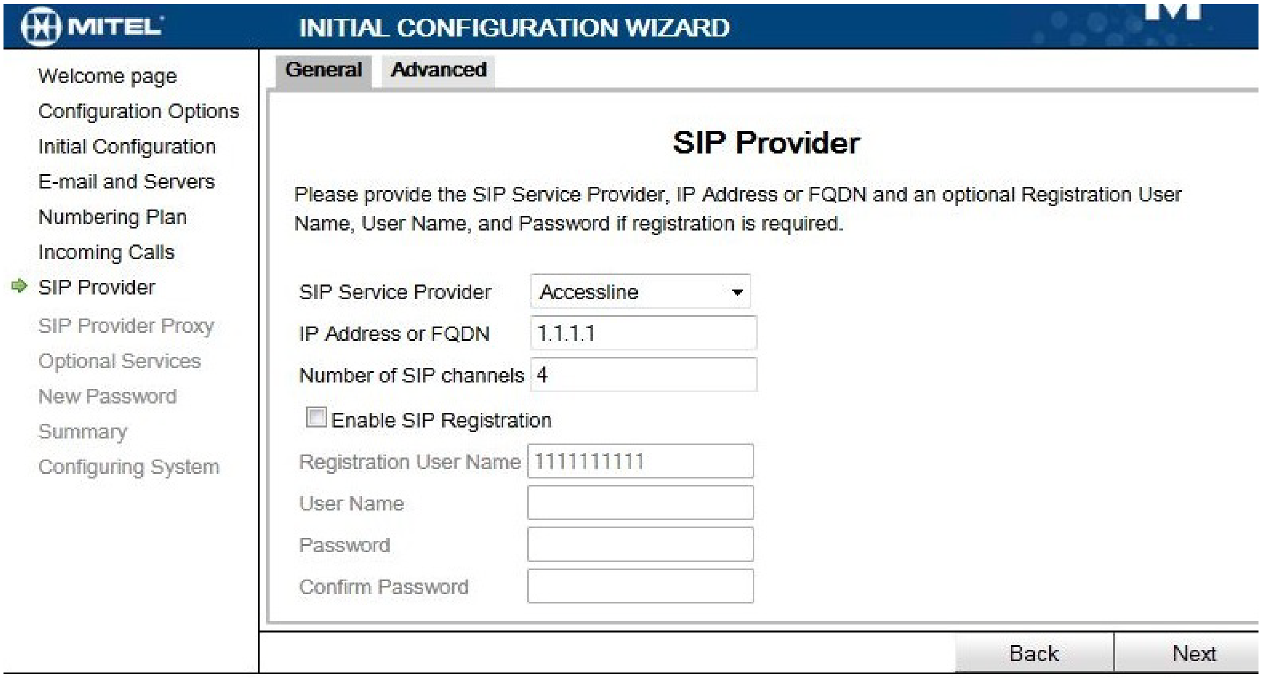
Number of digits to absorb

Digits to insert

Figure 38: Advanced Incoming Call Configuration

10. Click **Next**. The SIP Service Provider screen is displayed. Complete the following:

- *SIP Service Provider*: Select your Service Provider. The most common Service Providers for your region are listed in drop down menu for selection. A "Generic" SIP peer profile is also available.
  You can also specify custom peer profile CSV file saved from the SIP Peer Profile form in the MCD System Administration Tool.
  - Save a SIP Peer Profile file (see “Obtain a Custom SIP Peer Profile (optional)” on page 46)
  - Select **Custom** from the drop-down menu
  - Browse to the CSV file and click **Import**.
- *IP Address or FQDN*: Enter the IP address or Fully Qualified Domain Name of your Service Provider
- *Number of SIP channels*: This field displays the number of SIP channels licensed for the system.
- *Enable SIP Registration*: Click this check box if your service provider requires registration.
- *Registration User Name*: For Service Providers that require system registration, enter the name that the system must use to register for services. The Registration User Name is typically a single user name but it can also reference a range of DID numbers from the service provider. Obtain this credential from your service provider. Enter "bnc" (bulk number contact) to register al DIDs assigned to this system under a single name (FRC6140). This field accepts a maximum of 60 characters.
- *User Name*: Enter the user name of your SIP Service account. Obtain your user name and password from your service provider.
- *Password and Confirm Password*: Enter the password that you received from your service provider.



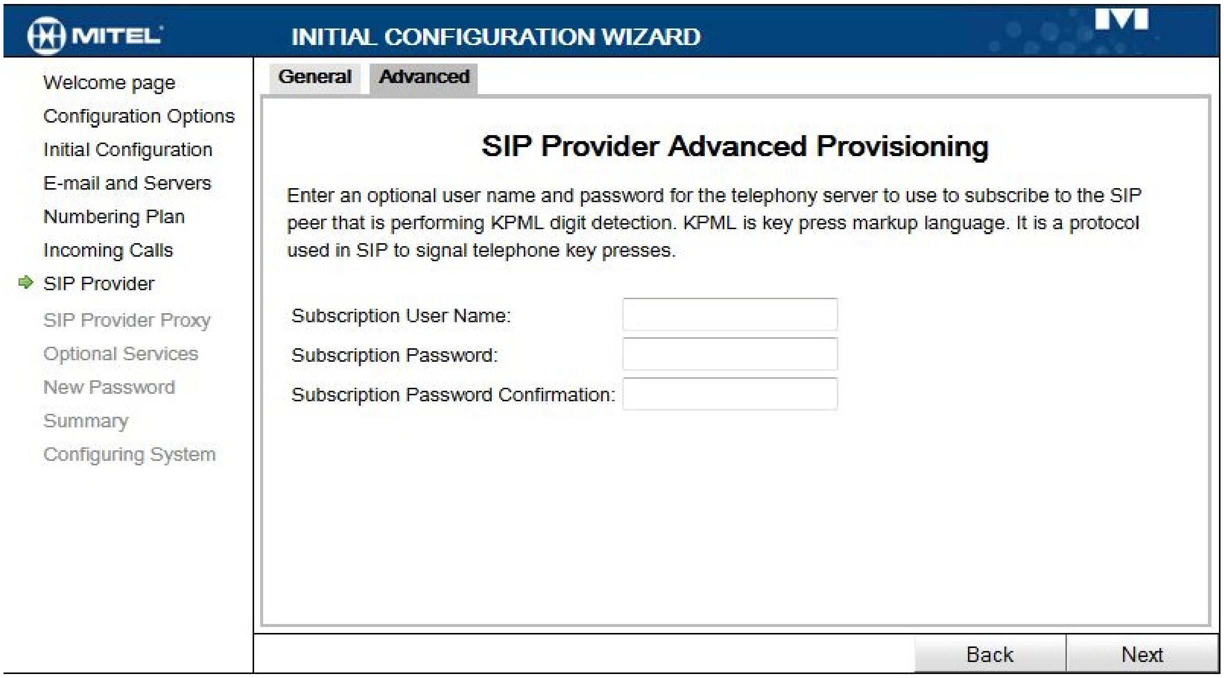
SIP Provider

Please provide the SIP Service Provider, IP Address or FQDN and an optional Registration User Name, User Name, and Password if registration is required.

SIP Service Provider	Accessline
IP Address or FQDN	1.1.1.1
Number of SIP channels	4
□ Enable SIP Registration	
Registration User Name	1111111111
User Name	
Password	
Confirm Password	

Figure 39: SIP Service Provider

11. Click the **Advanced** tab. Enter the following:
    - *Subscription User Name*
    - *Subscription Password*
    - *Subscription Password Confirmation*



SIP Provider Advanced Provisioning

Enter an optional user name and password for the telephony server to use to subscribe to the SIP peer that is performing KPML digit detection. KPML is key press markup language. It is a protocol used in SIP to signal telephone key presses.

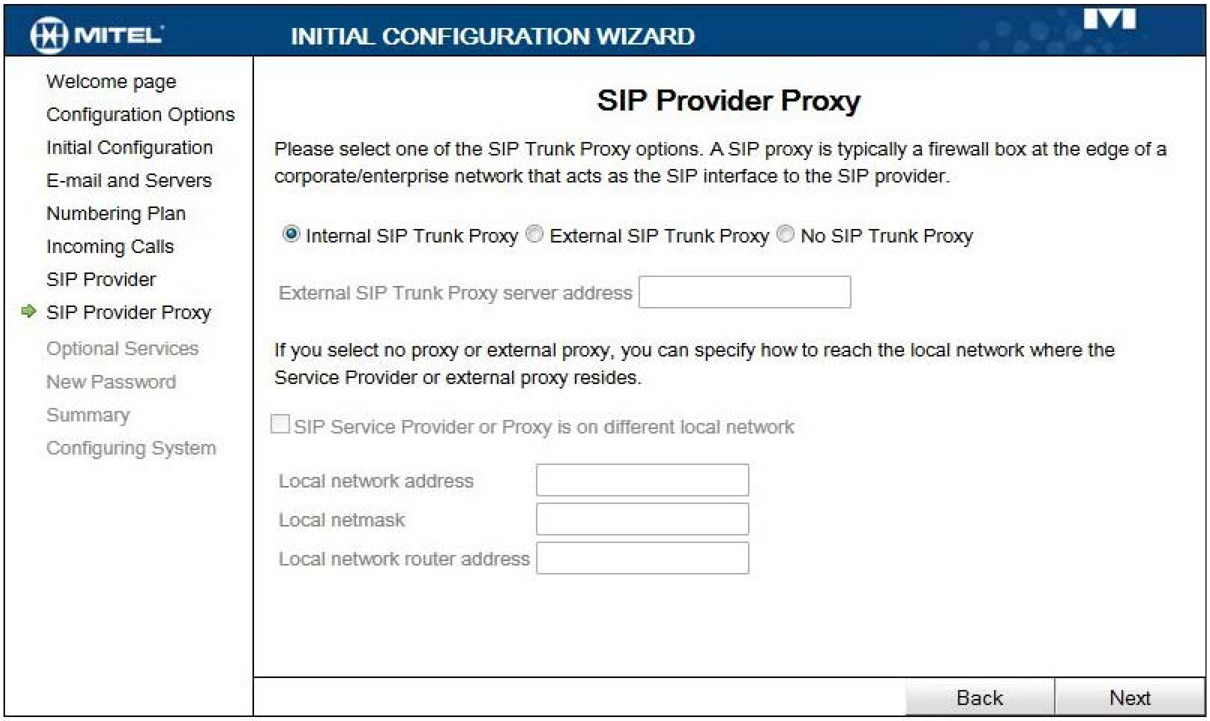
Subscription User Name:

Subscription Password:

Subscription Password Confirmation:

Figure 40: SIP Provider Advanced Provisioning

12. Click **Next**. The SIP Trunk Proxy screen opens.
    - Select a SIP Trunk Proxy option:
        - *Internal SIP Trunk Proxy*: Select this option if the SIP trunk proxy is supported internally on the vUCC system.
        - *External SIP Trunk Proxy*: Select this option if the SIP trunk proxy is supported on a separate optional Mitel Border Gateway (MBG). For this option, you must enter the addresses required to specify a route to the MBG.
        - *No SIP Trunk Proxy:* Select this option if a SIP trunk proxy is not required on the system.
    - Select the "SIP Service Provider or Proxy is on a different local network" option if either are located on a different local network. Enter the local network address, netmask, and network router address for the local network.



SIP Provider Proxy

Please select one of the SIP Trunk Proxy options. A SIP proxy is typically a firewall box at the edge of a corporate/enterprise network that acts as the SIP interface to the SIP provider.

● Internal SIP Trunk Proxy ○ External SIP Trunk Proxy ○ No SIP Trunk Proxy

External SIP Trunk Proxy server address

If you select no proxy or external proxy, you can specify how to reach the local network where the Service Provider or external proxy resides.

□ SIP Service Provider or Proxy is on different local network

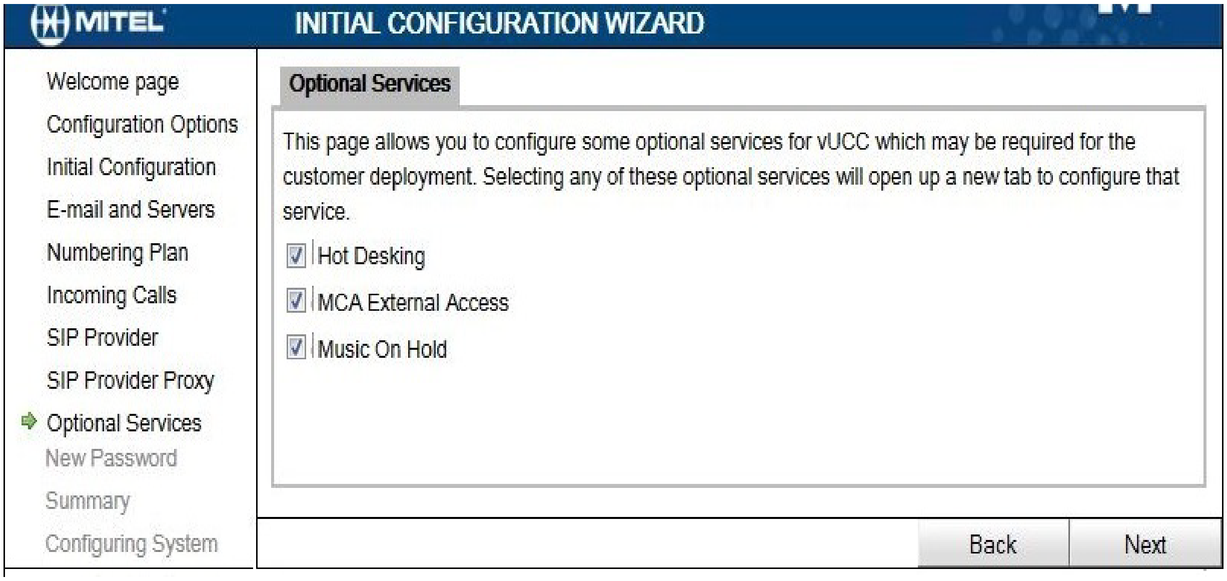
Local network address

Local netmask

Local network router address

Figure 41: SIP Trunk Proxy

13. Click **Next**. The Optional Services screen opens. Check the desired optional services on the **Optional Services** tab and then click **Next**.



This page allows you to configure some optional services for vUCC which may be required for the customer deployment. Selecting any of these optional services will open up a new tab to configure that service.

☑ Hot Desking

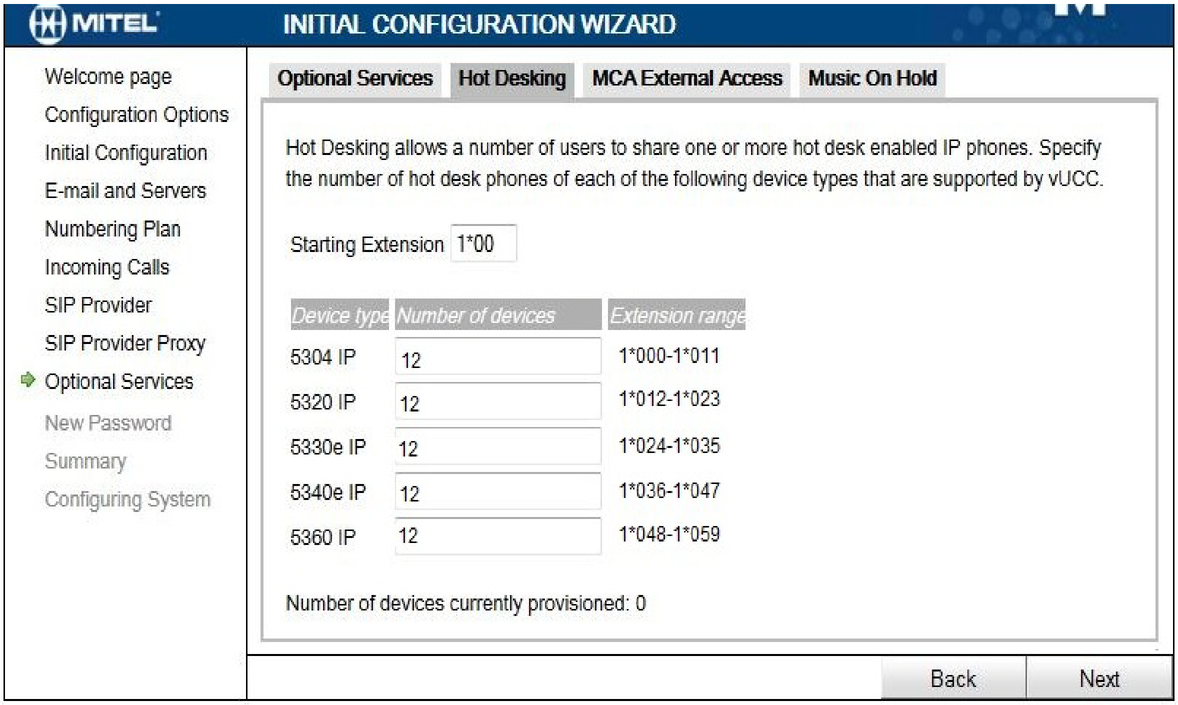
☑ MCA External Access

☑ Music On Hold

Figure 42: Configure Optional Services

14. For the hot desking feature, configure the hot desk enabled phones for the site. A hot desk user can log into any hot desk enabled phone and the system applies the user's profile to the phone:

    - Enter the starting extension number of the range of numbers that the system will assign to the hot desk enabled phones. Hot desk enabled phones are typically assigned non-standard extension numbers (for example 1∗000). The hot desk extensions must be different from the extension numbers that you entered in the Numbering Plan screen (that is, the numbers must not overlap).
    - Enter the number of phones that you want to support hot desking next to the desired models.
    - The extension numbers are assigned consecutively to the phones. In the example shown below, in the first row twelve 5304 IP phones are enabled as hot desk devices with extension numbers 1∗000 to 1∗011.
    - The number of hot desk devices currently configured on the system are listed. This number will always be zero on initial configuration of a new system.



Hot Desking allows a number of users to share one or more hot desk enabled IP phones. Specify the number of hot desk phones of each of the following device types that are supported by vUCC.

Starting Extension 1*00

Device type	Number of devices	Extension range
5304 IP	12	1*000-1*011
5320 IP	12	1*012-1*023
5330e IP	12	1*024-1*035
5340e IP	12	1*036-1*047
5360 IP	12	1*048-1*059

Number of devices currently provisioned: 0

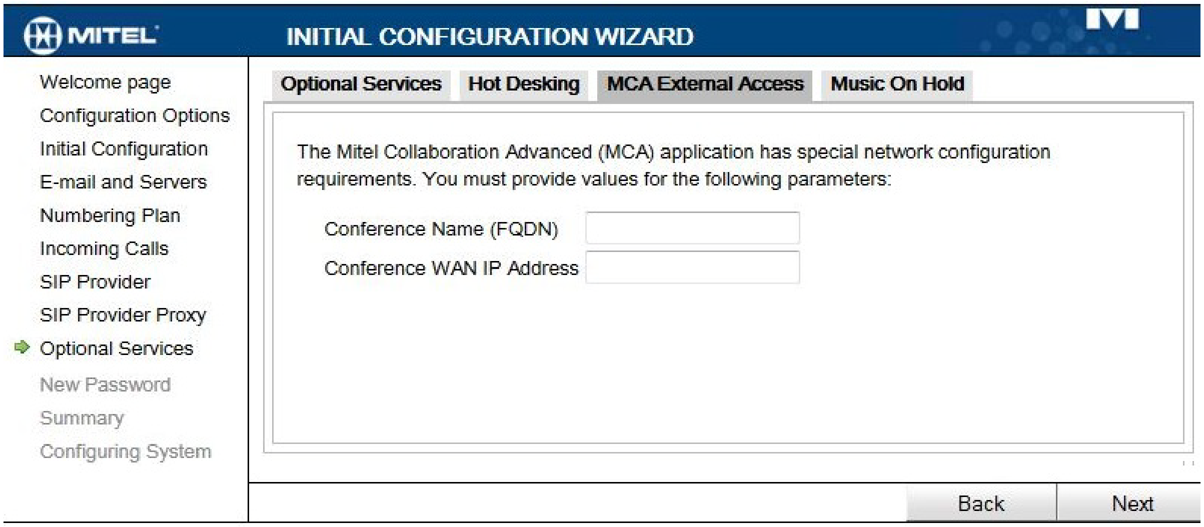
Figure 43: Hot Desking

15. Click **Next**. For MCA External Access services, specify the following:

- *Conference Name (FQDN)*: Enter the Fully Qualified Domain Name (FQDN) of the Mitel Collaboration Advanced server. The FQDN must resolve to a public IP address that is externally accessible. The internal DNS must resolve the FQDN to the local IP address of MCA server. For more information, refer to "Firewall and DNS Server Configuration" in the *Mitel Collaboration Advanced Configuration and Maintenance Manual.*

Note: The External MCA Web Conference FQDN Name cannot begin with a number. If the FQDN begins with a number, the Initial Configuration Wizard will fail to deploy the vUCC appliance as MCA will consider the FQDN invalid.

- *Conference WAN IP Address*: Enter the IP address that users will use to access the Web page of the MCA interface. The address must be accessible to everyone who will be invited to attend a web conference, both inside and outside of your local network.



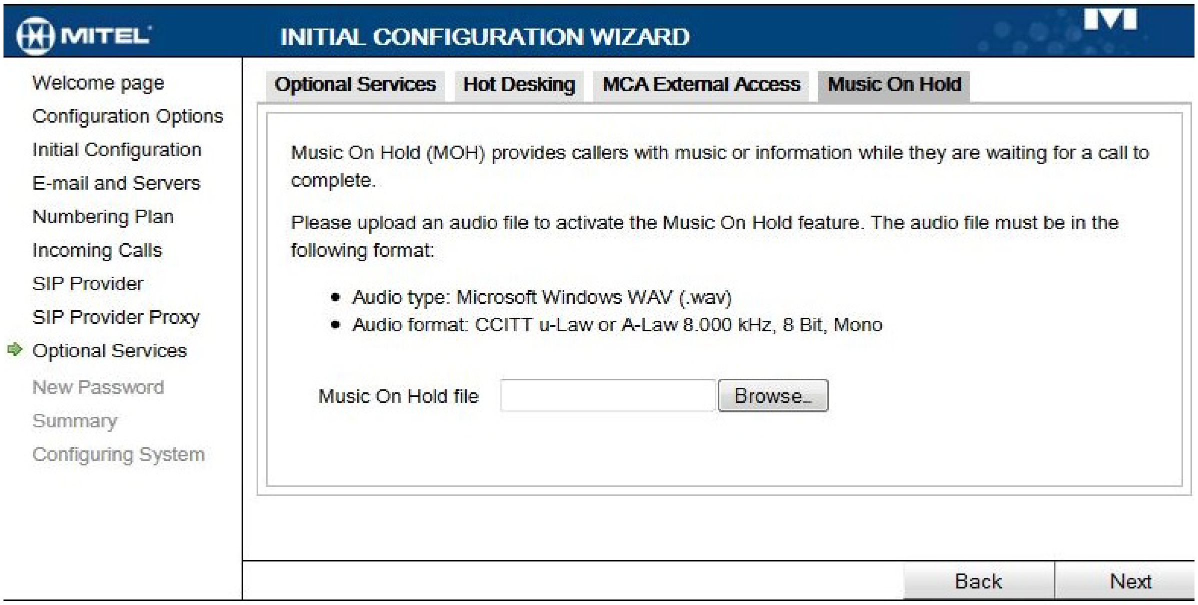
The Mitel Collaboration Advanced (MCA) application has special network configuration requirements. You must provide values for the following parameters:

Conference Name (FQDN)

Conference WAN IP Address

Figure 44: MCA External Access

16. Click **Next**. The Configure Music on Hold tab is displayed. Browse to the file.



Music On Hold (MOH) provides callers with music or information while they are waiting for a call to complete.

Please upload an audio file to activate the Music On Hold feature. The audio file must be in the following format:

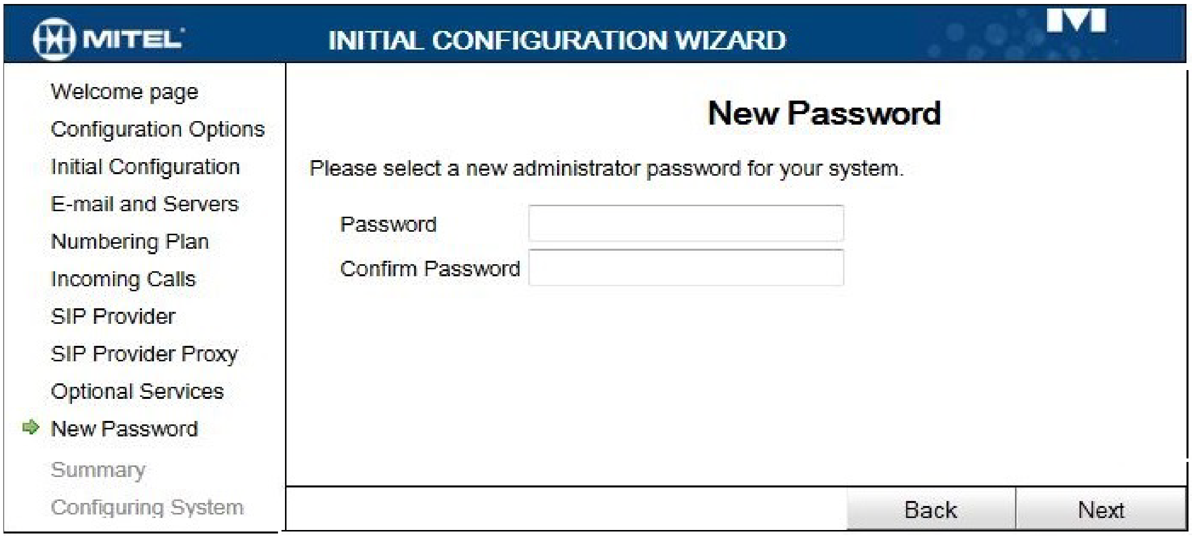
- Audio type: Microsoft Windows WAV (.wav)
- Audio format: CCITT u-Law or A-Law 8.000 kHz, 8 Bit, Mono

Music On Hold file

Figure 45: Configure Music on Hold

17. Click **Next**. Enter a new administrator password. This new password replaces the one that was used to access the wizard. It allows you to log into the server manager administration interface and into the MCD administration tools.

Note: This New Password is applied to the MAS server manager, MAS server console, and MCD administration tools. However, if you later change the password from a MAS administration interface, the change is not applied to the MCD administration tools. Likewise, if you change the password from the MCD System Administration tool, the change is not applied to the MAS administrator interfaces. This is because the MAS and MCD admin accounts are separate and independent.



New Password

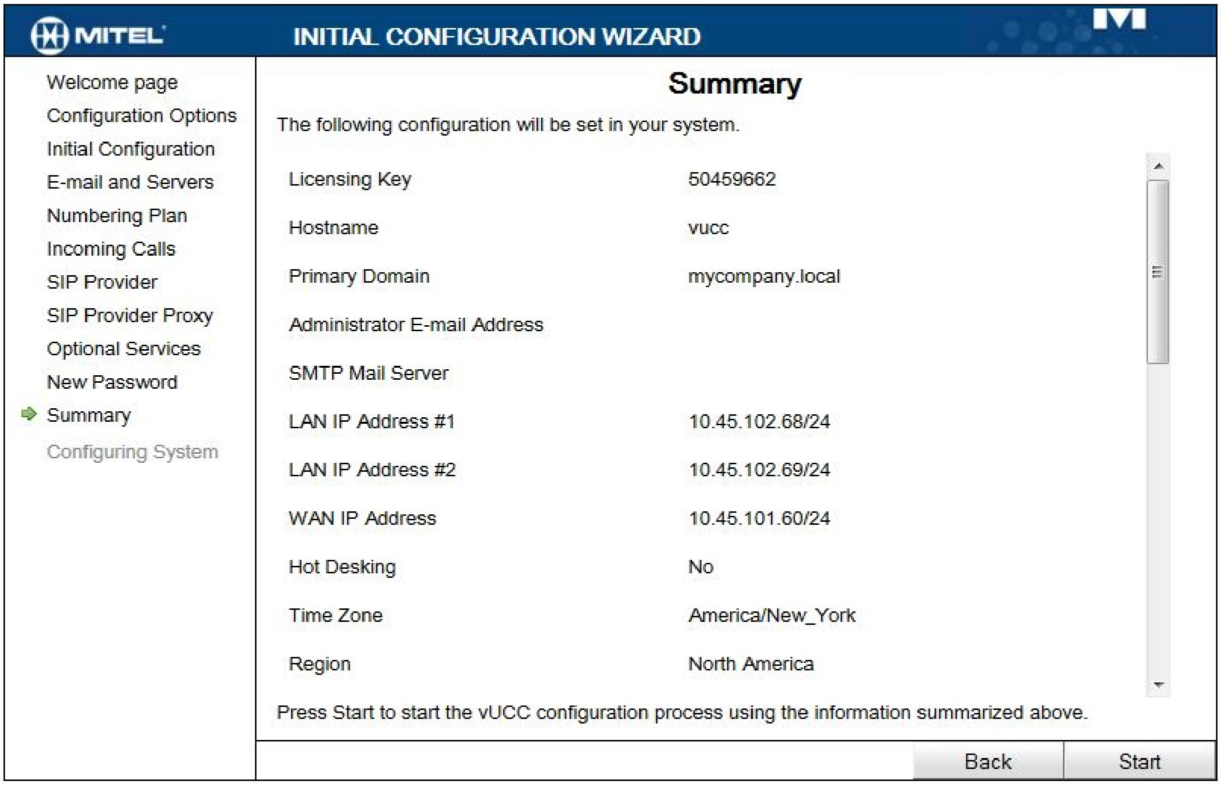
Please select a new administrator password for your system.

Password

Confirm Password

Figure 46: New Password

18. Click **Next**. Review the settings summary. Ensure that you have entered your settings correctly before proceeding.



Summary

The following configuration will be set in your system.

Licensing Key	50459662
Hostname	vucc
Primary Domain	mycompany.local
Administrator E-mail Address	
SMTP Mail Server	
LAN IP Address #1	10.45.102.68/24
LAN IP Address #2	10.45.102.69/24
WAN IP Address	10.45.101.60/24
Hot Desking	No
Time Zone	America/New_York
Region	North America

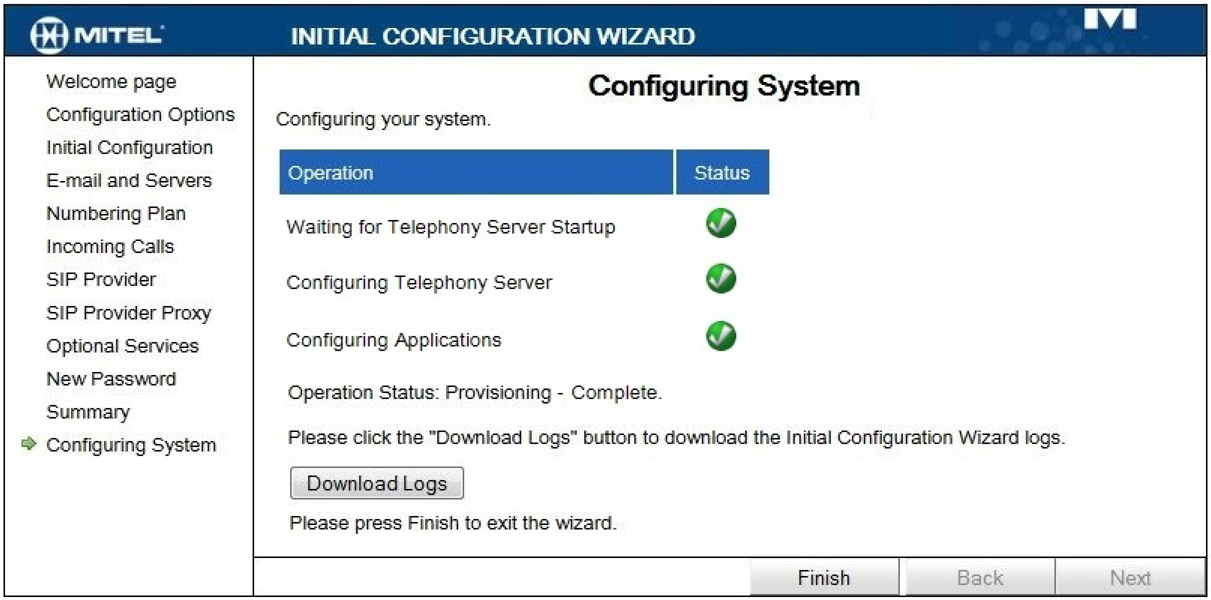
Press Start to start the vUCC configuration process using the information summarized above.

Figure 47: Summary screen

19. Click **Next**. The final screen displays the configuration progress.

WARNING:It can take up to 10 minutes for the configuration to complete. While configuration is in progress, do not exit your browser window.

20. Upon successful completion, a green check appears in the Status column for each of the listed operations. If the wizard fails to configure the system, check the logs to determine the issue. You must restart the wizard and re-enter your data correctly.



Configuring System

Configuring your system.

Operation	Status
Waiting for Telephony Server Startup	✓
Configuring Telephony Server	✓
Configuring Applications	✓

Operation Status: Provisioning - Complete.

Please click the "Download Logs" button to download the Initial Configuration Wizard logs.

Please press Finish to exit the wizard.

Figure 48: Configuring System

21. Click **Finish**. If an error occurs, click **Download Logs** to obtain the logs for troubleshooting.

22. Synchronize the UCA server with MCA software versions (required to support video):
    - In MAS server manager, under **Applications**, click **Unified Communications Server**
    - Click **Configure Mitel UC Server**.
    - Click the **Collaboration** tab.
    - Click the Local MCA Server link.
    - Click **Sync Now**. The MCA Server and Client software versions are updated.

23. Proceed to “Perform Advanced Configuration” on page 90.

Perform Advanced Configuration

The following functionality requires additional configuration in the application programming interfaces:

- Integrated Directory Services
- Direct Inward Dialing
- Customer Emergency Services IDs (CESID)
- Zones
- Advanced Unified Messaging
- Configure MSL DHCP Server.

Caution:You must complete the Mitel Integrated Wizard before you log into an MCD Administration session. The first time that you log into the MCD System Administration Tool. it prompts you to change your password. After you change the MCD System Administration Tool password you will be unable to run the wizard.

Note: The Mitel Customer Documentation web site provides additional documentation for advanced configuration that is not covered in this section. See “About the Documentation Set” on page 5 for a list of the available documentation.

Configure Integrated Directory Services

You can integrate the user database of a corporate directory service with the vUCC database to minimize data entry and administration. The user data on the corporate directory server is synchronized with the vUCC database using Lightweight Directory Access Protocol (LDAP). If single point provisioning is enabled, then the user data is also distributed to the MCD. Synchronization occurs in one direction only—from the directory server to vUCC.

1. Log into the server.
2. Under Configuration click **Integrated Directory Services**.
3. Follow the instructions in the Integrated Directory Services (IDS) online help.

Note: For information on performing LDAP Search Queries, go to the following URL: http://technet.microsoft.com/en-us/library/aa996205(v=exchg.65).aspx

Provision Direct Inward Dialing

Direct Inward Dialing (DID) allows incoming calls on designated trunks to directly access predefined extensions (or other answer points) on a vMCD system. In UCaaS deployments, where vMBG provides SIP Proxy resources for multiple vUCCs, you must provision the vMCDs with Direct Inward Dialing (DID) to the system extensions.

Obtain Direct Inward Dialing numbers from your SIP Service Provider. You can assign Direct Inward Dial numbers to a range of consecutive extension numbers (for example all users on the system) during the Initial Configuration Wizard. However, if you want to assign Direct Inward Dialing to just a few specific users, for example, executives, sales staff, and department heads, program DID to individual user directory numbers (see the following procedure).

Program Direct Inward Dialing to Individual User Directory Numbers:

1. Log into the MCD System Administration tool. See “Logging into the Mitel Communications Director (MCD) Tools” on page 122.
2. In the top left corner, select **View Alphabetically**.
3. For incoming calls on DID numbers, link the DID number to a system speed dial number that directs the calls to the user’s directory number:
    - In the left forms list, click **System Speed Dials**.
    - Click **Add**.
    - Enter the DID number (for example: 613 592 5661), in the Speed Call Number field.
    - Enter the directory number of the user’s prime phone (for example 3333) in the Actual Number field.
    - Select S/C in the Type field.
    - Leave Overrides Toll Control at No.
    - Click **Save**.
4. To modify the number for the user’s outgoing calls, associate the user-specific DID number with the user’s directory number in the Associated Directory Number form:
    - In the left forms list, click **Associated Directory Numbers**.
    - Enter the user’s directory number (for example, 3333).
    - Set the Associated Type to CPN Substitution.
    - Enter the outgoing number (for example, 613 592 3333) that you want to substitute for the directory number.
        - If the user has a Personal Ring Group or Multi-Device User group create an Associated Directory Number for the Prime Contact Number only.
        - If the user has several separate devices (for example, Office Extension, Teleworker, Dynamic Extension), create an Associate Directory Number for each directory number.
    - Click **Save**.

Provision CESIDs

A Customer Emergency Services ID (CESID) is used to provide location information for a phone extension on a private network, when a caller makes an emergency call. The information can help direct emergency crews to a caller's location. CESID programming and maintenance is a required component of Emergency Services.

CESIDs are public network Listed Directory Numbers (LDNs) that you obtain from your local carrier or SIP Service Provider. When an emergency call is made, the system sends the CESID of the extension out to the PSTN. The CESID is used by the service provider to route the call to the local Public Safety Answering Point (PSAP) and then by the PSAP to call up information such as the address, building, floor, area, and call-back number.

- CESIDs can be manually or automatically updated to maintain current CESID information in the system.
- CESIDs and their assigned location information are stored in an Automatic Location Information (ALI) database.
- CESIDs are not dialable numbers and the data contained in them is only used for out-bound Emergency calls. CESID numbers are never displayed to a third party during a routine call.

For vUCC, the default CESID is the main business number for the system.

Note: Different state or provincial regulations may govern the CESID requirements at your location. Some require a unique CESID for every telephone, and others allow the sharing of CESIDs if the telephone users are within sight of one another. One dialable call-back number is required for each CESID.

Coordinating CESIDs with the ALI Database

The CESID sent to the PSAP to identify the location of the emergency caller must be the same number that resides in the Automatic Location Information (ALI) database for that location. The ALI database is independent of the MCD and may reside at the local PSAP, at the telephone company Central Office, or at an independent location. It is essential that CESID numbers and the ALI database remain synchronized when moves, adds, and changes take place. Any changes made to a user's location or data associated with a CESID must be communicated to the ALI database administrator. Ensure that local changes affecting ALI information are kept from going into service until the ALI database has been updated. The System Administrator must ensure that CESID related changes are communicated to the ALI database. A minimum of one L2 connectivity detection protocol (STP, or CDP) must be uniformly and consistently configured on all the L2 switches that the devices are connected to. The administrator must define the same protocol of choice for every MCD in the network.

CESID Conditions

- CESIDs are not associated with location independent entities such as ACD agents and regular Hot Desk users. If an ACD agent or regular Hot Desk user makes an emergency services call, the CESID associated with the originating set is sent.
- For EHDUs logged on to private trunks (such as a Suite EHDU), the CESID associated with the user’s mobile DN is sent. For EHDUs logged on to public trunks (such as cell phones), the external party’s public number is sent as the CESID. For EHDUs logged in over public trunks that provide no calling line identification, the EHDU configured external number is sent as the CESID.

Note: An EHDU external number configured with *, # or P characters cannot be used for the CESID. For EHDUs logged in internally (such as a Minet device), the CESID associated with the originating set is sent.

- Class of Restriction and Interconnect Restrictions remain in effect for emergency services calls. Specific users may be restricted from accessing the designated Emergency Services number.
- SMDR output is changed in the event of an emergency services call; the prime directory number of the originating station is output.

Automatic CESID Updating

The following conditions apply to automatic CESID updating:

- Automatic CESID updating is not supported on hubs where multiple devices report connectivity to the same L2 port, or on L2 switches that do not have STP or CDP enabled. The system detects and logs this condition upon device registration.
- The MCD portion of the Mitel Emergency Services solution does not support handling of "special circumstance" DNs. Some DN users have special needs: for example, a DN may be associated with a wheelchair user or with an area where dangerous chemicals are stored. The PSAP may have a record associating a user or DN with this type of special circumstance. If such a device is moved, the MCD treats it like any other device move and attempts to automatically update the CESID Assignment form. This causes the PSAP database to be out of sync with the MCD. To avoid this situation, the administrator should ensure that such DNs are not moved.
- Automatic CESID updating does not function during a database backup or restore.
- A log is generated if the system detects a conflict between STP and CDP data.

Automatic CESID updating should not be enabled for

- Devices in Teleworker mode or devices that are connected outside of the corporate firewall. 911 calls placed from such devices may report an incorrect CESID, or may be outside of the PSAP's coverage area. Devices are not compatible with the Mitel Emergency Services solution when they are operating outside the corporate network serviced by the MCD. The reasons are as follows:
    - A Teleworker device operating outside the corporate network may or may not trigger a device move;
    - The system will not be able to accurately assign a CESID to such a device outside the network;
    - The MCD will not be able to route the 911 correctly. Note that the system will not block Teleworker devices from making 911 calls. However, it is not recommended that users make 911 calls from devices operating in Teleworker mode outside the corporate firewall. It is best if the administrator changes the CESID Updating state manually for Teleworker enabled devices.
- Generic SIP phones
- UCA softphones. UCA softphones cannot detect L2 connectivity data.

CESID Programming Guidelines

Defining default zone CESIDs - You can define a default CESID for each zone in the network. This will allow the system to identify the location of the caller, when an emergency call is routed to a different zone and no CESID is available for the calling DN.

911 and CESID - For a 911 call to be compliant with FCC guidelines, the call must report a CESID to the PSAP. At a minimum, you must define a CESID for each DN in the MCD CESID Assignment form. In order to ensure that CESIDs are updated when a device is moved and can be correctly reported to the PSAP, you must promptly investigate and address all CESID-related alarms. You may have to return a phone to its original location if the move was not authorized or update the CESID Assignment and/or L2 to CESID Mapping forms. Alternatively, you can update the "L2 to CESID Mapping" form in advance of a device move.

Defining the primary protocol - Carefully consider the difference between the protocols (STP and CDP), and designate one as your primary protocol. Remember that the L2 STP Port Identifier may not correspond to the physical port number on the L2 switch (with VLANs, the L2 port number may be virtual). You designate a primary protocol for Detecting IP Device Moves in the CESID Assignment form.

Switching between CDP and STP in the network - The system may detect a false device move if the primary protocol is changed while a device is connected to an L2 switch.

Enabling Layer 2 (L2) protocol - Ensure that all L2 switches in the network have the primary protocol enabled. If there is an L2 switch that does not have the protocol enabled, devices may move from one port to another on that switch and the system will be unable to detect the device move because no L2 data will be reported.

New installations - In a new vUCC installation scenario it is recommended that you allow the system to auto-discover the L2 Port MAC and L2 Port, as devices are registered, rather than manually entering the information. Auto-discovery ensures that the values are correct (particularly for VLANs), while manual entry can be prone to error. After the information has been auto-discovered, you can go into the CESID Assignment form or the L2 to CESID Mapping form and enter the CESID for each entry. You may also want to go to other network drops where a phone might be moved to and allow the device to register there as well so that the ports can be auto-discovered. Note that any network drops that do not have a Mitel IP device connected to them will remain undiscovered by the MCD. You can either wait for a CESID alarm to be generated when a device connects to an unknown L2 port, or you can pro actively auto-discover L2 data by plugging devices into L2 ports.

Upgrades - When you restore a database that contains accurate and complete CESID assignments, the L2 to CESID mapping for known devices will be fully and automatically discovered upon device registration. For this to happen, the CESID Assignment data must be accurate prior to the backup and upgrade.

Backup and restore - Device move detection, automatic CESID updating, and alarming do not function during a database backup or restore. This is because all database files needed to detect device moves and update CESIDs are locked during a backup and restore. For this reason, you should perform backups and restores during times when devices are least likely to be moved. To ensure that no devices are moved, it may be helpful to notify users of backups and restores and instruct them not to move devices, if possible, during these times.

Maintaining CESID Logs - The CESID Logs form overwrites data, from the oldest to newest entries, after 5000 CESID logs have been posted. If you wish to have traceability of the logs, perform regular database backups, or print or export this information.

Replacing L2 switches - If an L2 switch is replaced in the network (for example, a non-functional switch is replaced with a new one), the MCD recognizes the event as a device move after the sets re-register through the new L2 switch (because the sets are reporting a new L2 connectivity point). Assuming that no new L2 to CESID mappings were manually created for the new switch, the system clears the CESID values in the CESID Assignment form (only for the devices registered to the new L2 switch) and raises a CESID alarm.

Therefore, when a switch is replaced (old with new), you must reprogram the CESID assignments for the sets that were connected to the replacement switch. Also, you must delete the old L2 to CESID mappings for the replaced switch, because they are no longer relevant. Alternately, you may wish to set the DNs connected to the retiring L2 switch to Manual CESID updating (as opposed to Automatic - see CESID Assignment form), to prevent the CESIDs from being deleted.

Another replacement scenario is when two L2 switches are swapped in the network. Again, the MCD and IP devices register this swap as device moves, even though it was the switches that were moved and not the devices. In this case, the system automatically updates the CESID Assignment for each moved device (assuming that CESID Assignment was complete prior to the swap). The problem here is that the automatic CESID updating will likely be inaccurate because the L2 swapping will cause the L2 to CESID mapping to become incorrect. For this reason, it is recommended that you delete the CESID assignments before swapping the L2 switches, update the L2 to CESID mapping, and then allow the correct CESID assignments to be auto-discovered.

Retiring an L2 switch - When an L2 switch is retired, delete the relevant entries from the L2 to CESID mapping form, since these are no longer being used.

Physically moving a network drop - For automatic CESID updating, the system will not be able to detect when a network drop is physically moved from one location to another (assuming the L2 port connection point remains the same). You should be wary of any physical port location changes (for example, those done during a re-wiring project). It may happen that if a network drop is physically moved, it will move into a location serviced by a different CESID. It is the system administrator's responsibility to ensure that network drops aren't moved without permission, and to update CESIDs when they are.

Connecting IP devices to a hub - It is recommended that devices be connected directly to an L2 switch. Avoid connecting IP devices to a hub that is, in turn, connected to an L2 switch. Apart from Quality of Service reasons, IP devices connected directly to a hub will all report the same L2 Port MAC/Port, and the system will not be able to automatically update the CESID for any devices registering to that hub.

Swapping Ethernet cables on an L2 switch - It is recommended that you do not swap Ethernet cables on L2 switches (for example, when troubleshooting a malfunctioning port). The system will see this switch as a device move. The device will report a new L2 connectivity point, even though it was not physically moved. Depending on the configuration, this could result in an automatic CESID update (likely with the wrong CESID), a CESID alarm, or the deletion of the device's CESID. If you must swap Ethernet cables on an L2 switch, be aware of the effect this will have on device detection and CESID assignment.

Addressing CESID alarms and logs - If a device is moved, and the system is unable to assign a CESID to the device at its new location, the system will raise an alarm, and log the problem. The user should monitor the system alarms for such an event, and when it occurs, use the logs, the CESID Assignment form, the L2 to CESID Mapping, and/or the Device Connectivity forms to determine the nature of the problem. Once the problem is understood, you should update the CESID Assignment or L2 to CESID Mapping form. This will ensure that the device has the correct CESID and will clear the alarm once all CESIDs have been assigned (for DNs in Automatic CESID Handling mode.)

Teleworkers - Mitel IP devices that are running in Teleworker mode and are connected outside the corporate network through the Mitel Standard Linux (MSL) gateway will not be blocked from making 911 calls, however an incorrect CESID may be reported.

Assigning CESIDs

You can assign CESIDs to each directory number (DN) on your network, using the MCD CESID Assignment form:

1. Log into the MCD System Administration tool. See “Logging into the Mitel Communications Director (MCD) Tools” on page 122.
2. In the top left corner, select **View Alphabetically**.
3. In the left forms menu, select **CESID Assignment**.
4. Assign a CESID number to each primary extension number. The MAC address of the Layer 2 switch port and the Layer 2 switch port identifier are detected by the system when an IP phone registers.
    - *CESID*: Enter the CESID to be sent to the PSAP in the event of an emergency call. Up to 12 digits can be programmed.
    - *CESID Comments*: Enter location information for the person at this extension.
    - *CESID Updating*: Leave setting to "Automatic".
    - *Route Emergency Calls*: Leave setting at "Through System Only".

Note: Automatic CESID updating should not be enabled for devices in Teleworker mode or devices that are connected outside of the corporate firewall. Emergency calls placed from such devices may report an incorrect CESID, or may be outside of the PSAP's coverage area. Devices are not compatible with the Mitel Emergency Services solution when they are operating outside the corporate network serviced by the MCD.

CESID Alarms and Logs

For information on CESID alarms and logs:

1. Log into the MCD System Administration tool. See “Logging into the Mitel Communications Director (MCD) Tools” on page 122.
2. Click the ? help button in the top right of the System Administration Tool interface. The MCD System Administration Tool help opens.
3. In the table of contents, click **System Applications**, click **General Business Solutions**, click **Emergency Services**, click **CESID Support** and then click **CESID logs**.

Configure Network Zones

Network zones are used for bandwidth management, compression, location based routing, and emergency services. Zone 2 is reserved for SIP Trunking.

- For specific vUCC zone configuration information, refer to the MAS and vUCC Engineering Guidelines.
- For general instructions on how to configure network zones:
  - Log into the MCD System Administration tool. See “Logging into the Mitel Communications Director (MCD) Tools” on page 122.
  - In the top left corner, select **View Alphabetically**.
  - In the left forms menu, select **Network Zones**.

Configure Unified Messaging (UM)

Unified Messaging (UM) allows you to integrate your NuPoint Unified Messaging voice mail system with your e-mail client for increased access to messages. When you assign an Entry, Standard, or Premium UCC (v2) license to a user, both Standard and Advanced UM are supported.

Integrate NuPoint Application with Mail Server

You must integrate the vUCC NuPoint Unified Messaging application with the external mail server (Exchange, Lotus Domino, or Google Apps).

1. Log into the MAS Server Manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 121).
2. Under **Applications**, click **NuPoint Web Console**.
3. Click the ? help button in the top right of the user interface. The NP-UM Web help opens.
4. In the table of contents, click **Optional Features**, click **Unified Messaging**.
5. Follow the instructions to configure Standard and Unified Messaging.

Assign Users with Unified Messaging

All users who are assigned with vUCC Entry, Standard, or Premium licenses support Standard and Advanced Unified Messaging by default:

1. Log into the MAS Server Manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 121).
2. Under **Applications**, click **Users and Services**.
3. In the directory list, select the user and click **Edit**.
4. Click **NuPoint Unified Messaging**.
5. Assign a mailbox to the user. The default Feature COS 14 enables Standard and Advanced Unified Messaging. The Standard and Advanced Unified Messaging check boxes are selected by default.
6. Click **Save**.
7. Unified Messaging users can configure the encoding format for their audio files on the Settings tab of their Web View interface.

Assign Classes of Restriction

Class of Restriction (COR) prevents a phone user from calling certain numbers. A user can have three COR services (Day/Night1/Night2).

By default, vUCC assigns COR 2 to all users. COR 2 allows users to place Local and Long Distance calls but restricts them from placing Overseas calls. To allow users to place Overseas calls, assign COR 3.

To change the COR setting for a user:

1. Log into the MCD System Administration tool. See “Logging into the Mitel Communications Director (MCD) Tools” on page 122.
2. In the top left corner, select **View Alphabetically**.
3. In the left forms menu, select **Station Assignment**.
4. Select the user’s extension and click **Change**.
5. Assign Class of Restriction numbers to the Day, Night1, and Night2 fields:

COR Number	Allows users to make. . . .
1	Emergency, Local, and Toll Free calls only
2	Emergency, Local, Toll Free, and Long Distance calls only.
3	Emergency, Local, Toll Free, Long Distance, Overseas calls, and Mobile calls (default).
4	Emergency calls only.
5	Emergency calls only.
6	Emergency, Local, Toll Free, Long Distance and Mobile calls.
7	Not used
8	Emergency and Toll Free calls.
9	All types of calls except Barred calls.

6. Click **Save**.

Import a Custom vMCD Database

To import a customized MCD database into the vUCC

1. Deploy the vUCC OVA file. See “Deploy UCC Virtual Appliance” on page 47 for instructions.
2. Run the Initial Configuration Wizard. See “Run the Wizard” on page 76.
3. Log into the System Administration Tool of the MCD system that has the desired database.
4. Export the forms listed in Table 13 to CSV files. Refer to the System Administration Tool online help for export instructions.
5. Make the modifications indicated in Table 13 to the CSV files.
6. Log into the System Administration Tool of the vUCC MCD and import the CSV files. Import the files in the indicated order.

Table 13: Export and Customize MCD CSV Files

Import Order	MCD Programming Form/ CSV File	Required changes prior to import . .
1	Class of Service	vUCC uses COS 80 to 86 for the NuPoint Unified Messenger and Mitel Collaboration Advanced hunt groups. If COS 80 to 86 are in use in the CSV import file, you must free up these COSs by assigning different, unused COS numbers to the groups or devices.
2	Feature Access Codes_blank.csv	You must blank out the current Feature Access Code values from the vUCC MCD database before you can import the Feature Access Codes CSV file. Import the Feature Access Codes_blank.csv to blank out the codes.

Table 13: Export and Customize MCD CSV Files

Import Order	MCD Programming Form/ CSV File	Required changes prior to import . .
3	Feature Access Codes	No changes required
4	System Options Assignment	
5	Class of Restriction Groups	
6	ARS Digit Modification Plans	
7	Route Assignment	Change the SIP Peer Profile name to "Sipsp" and delete Routes 7 to 9 prior to importing this form
8	Route List	No changes required
9	ARS Maximum Dialed Digits	
10	ARS Digits Dialed	
11	Multiline Advisory Messages	
12	SIP Device Capabilities	
13	SMDR Options	
14	SNMP Configuration	
15	User Authorization	

7. Set the desired default Class of Services (COS) in the MAS application:
   - Log into the vUCC Server Manager and launch the Users and Services application.
   - Click the **Network Element** tab.
   - Select the **System Name** of the MCD and click **Edit**.
   - Modify the COS settings and click **Save**.
8. Provision users on the system. See “Provision Users” on page 108.
9. Assign the Class of Restriction (COR) for each user to the required setting (by default, MAS applies COR 2). See “Assign Classes of Restriction” on page 98.

Configure MSL DHCP Server

To configure the internal MSL DHCP server to support devices on the LAN:

1. Log into the MAS Server Manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 121).
2. Under **Configuration**, click **DHCP**.
3. Click the **DHCP Service** tab.
4. Click **Edit**.
   - Check the **Enable DHCP Service** and **Allow BootP boxes**.
   - Click **Update**.

5. Click the **Subnets** tab.
   - Click Add Subnet.
   - Enter the Name, Subnet IP address, and Subnet Mask of the subnet.
   - Click **Save**.
   - Click Add Range.
   - In the Range start field, enter the IP address at the start of the range.
   - In the Range end field, enter the IP address at which to end the range.
   - In the Lease time field, enter the number of seconds to hold DHCP leases or accept the default setting.
   - Click **Save**.
6. Click the **Options** tab.
   - Click Add Option.
   - Set Scope to "Subnet".
   - Click **Standard Option**. Set the option field to "3 routers".
   - Click **Next**.
   - In the Value field, enter the local gateway IP address.
   - Click **Save**.

Configure Optional Standalone vMBGs

You can deploy and configure separate optional standalone vMBGs to

- support Secure Recording Connector for phones on the LAN, or
- aggregate (collect) SIP trunks from a SIP service provider for distribution among multiple vUCC systems.

See the *Mitel Border Gateway Installation and Maintenance Guide* on the Mitel Customer Documentation web site at http://edocs.mitel.com for installation instructions.

Secure Recording Connector Support

MBG provides a secure recording connector (SRC) service that allows third-party Call Recording Equipment (CRE) to record Mitel-encrypted voice streams. The SRC service is supported only in LAN only (Server) mode.

To support Secure Recording Connector for phones on the LAN, install the optional standalone vMBG in server-only mode on the LAN with no exposure to the Internet.

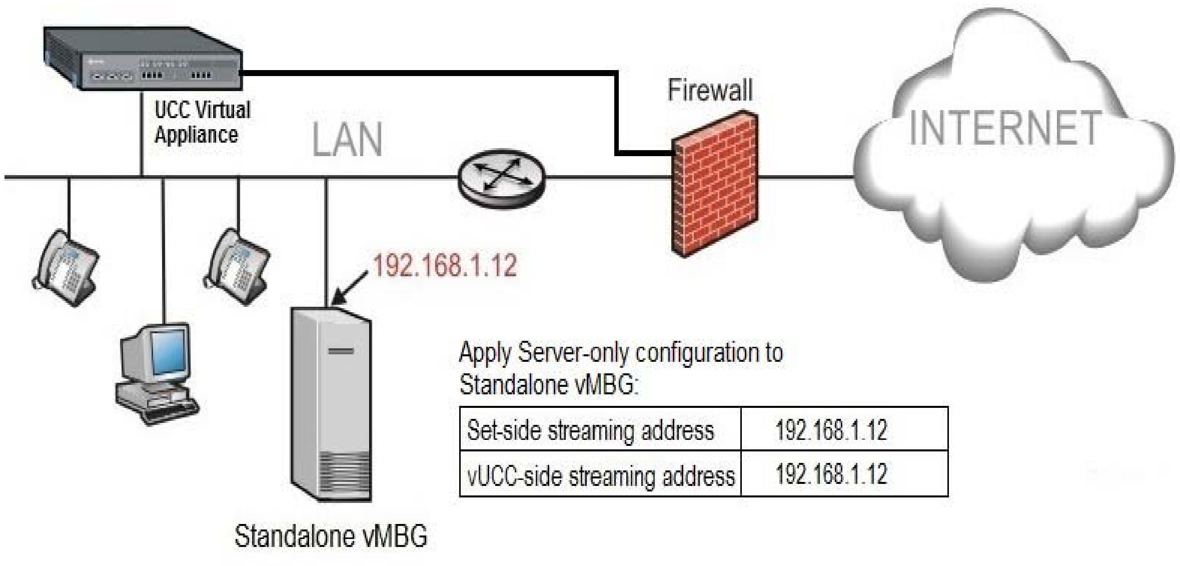
Deploy vMBG in Server-only Mode

1. Log into the MSL server console and select **Configure this server**.
2. In Local Network Parameters, enter the server's internal (LAN) IP address server or select the default. This address SHOULD be:

- dedicated to the MBG solution
- private
- reachable only from the internal network.

3. Log into the vMBG server manager.
4. Under **Applications**, click **Mitel Border Gateway**.
5. On the **Configuration** tab, click **Network Profiles**.
6. Select **Server-only configuration** on the network LAN.
7. Select **Apply LAN configuration**.

When configuration is complete, the system will use the LAN address of the server for both the set-side and ICP-side streaming addresses of the MBG. The following diagram provides an example of a "Server-only configuration on the network LAN":



Apply Server-only configuration to Standalone vMBG:

Set-side streaming address	192.168.1.12
vUCC-side streaming address	192.168.1.12

Figure 49: Standalone vMBG for Secure Call Recording

Configure Secure Recording Connector

Refer to the MBG online help for instructions on how to configure SRC.

SIP Trunk Aggregation

If your hosted infrastructure has multiple vUCC systems, it is possible to reduce SIP trunking costs by purchasing the trunks in bulk and then aggregating (consolidating) the trunks on a separate standalone vMBG. The SIP trunks can then be distributed among the vUCC systems via the vMBG SIP Trunking web proxy services.

To support SIP trunk aggregation, the vMBG is deployed in Server-Gateway (Network Edge) mode. In this configuration mode, the server functions a firewall/Internet gateway with two Ethernet interfaces. One interface is connected to the external network (Internet) while the other is connected to the internal network. The firewall provided by the vMBG server is not configurable. All default data traffic initiated inside the network is allowed while data traffic initiated outside the network is denied.

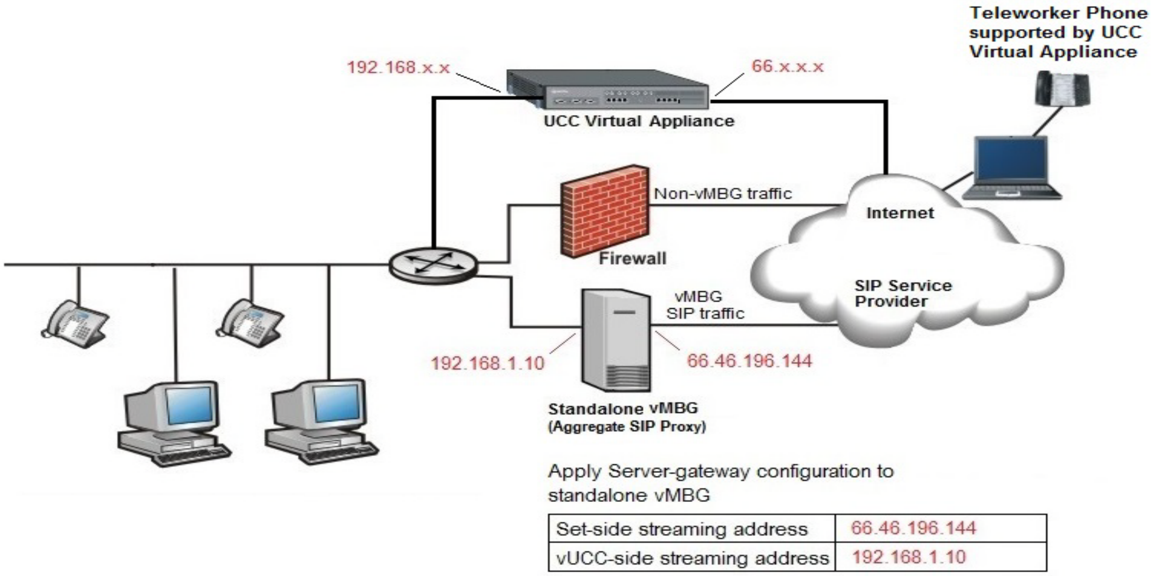
Deploy vMBG in Server-Gateway Mode

1. Access the MSL Server Console and select **Configure this server**.
2. In Local Network Parameters, enter the server's internal (LAN) IP address server or select the default.
3. In WAN Network Adapters, select the server's external (WAN) adapter.
4. The external (WAN) address MUST be:
   - dedicated to the MBG Solution
   - publicly routable
   - reachable from the Internet and the internal network (that is, the server should not reside behind a NAT device).
5. Access the vMBG server manager.
6. On the **Configuration** tab, click **Network Profiles**.
7. Select **Server-gateway configuration on the network edge**.
8. Select **Apply Server-Gateway configuration**.

When configuration is complete, the system programs the Real Time Protocol (RTP) streaming addresses as follows:

- ICP-side (vUCC-side) streaming address = LAN interface address
- Set-side streaming address = WAN interface address

Note: In the server-gateway configuration, the MBG server is the gateway for MBG traffic.



Apply Server-gateway configuration to standalone vMBG

Set-side streaming address	66.46.196.144
vUCC-side streaming address	192.168.1.10

Figure 50: Standalone vMBG for SIP Trunk Aggregation

Configure SIP Trunks

For Hosted UCaaS Provider deployments, a separate external standalone vMGB can be added to provide SIP trunking resources. The SIP trunking is consolidated on the standalone vMBG and provides the trunking capacity for multiple customers; all trunks come to one location and the incoming calls are routed to the appropriate MCD in each customer's UCC virtual appliance.

The IP addresses shown in are used as examples to illustrate the required configuration on the vMBG. In the following example, a SIP trunk is programmed for each customer.

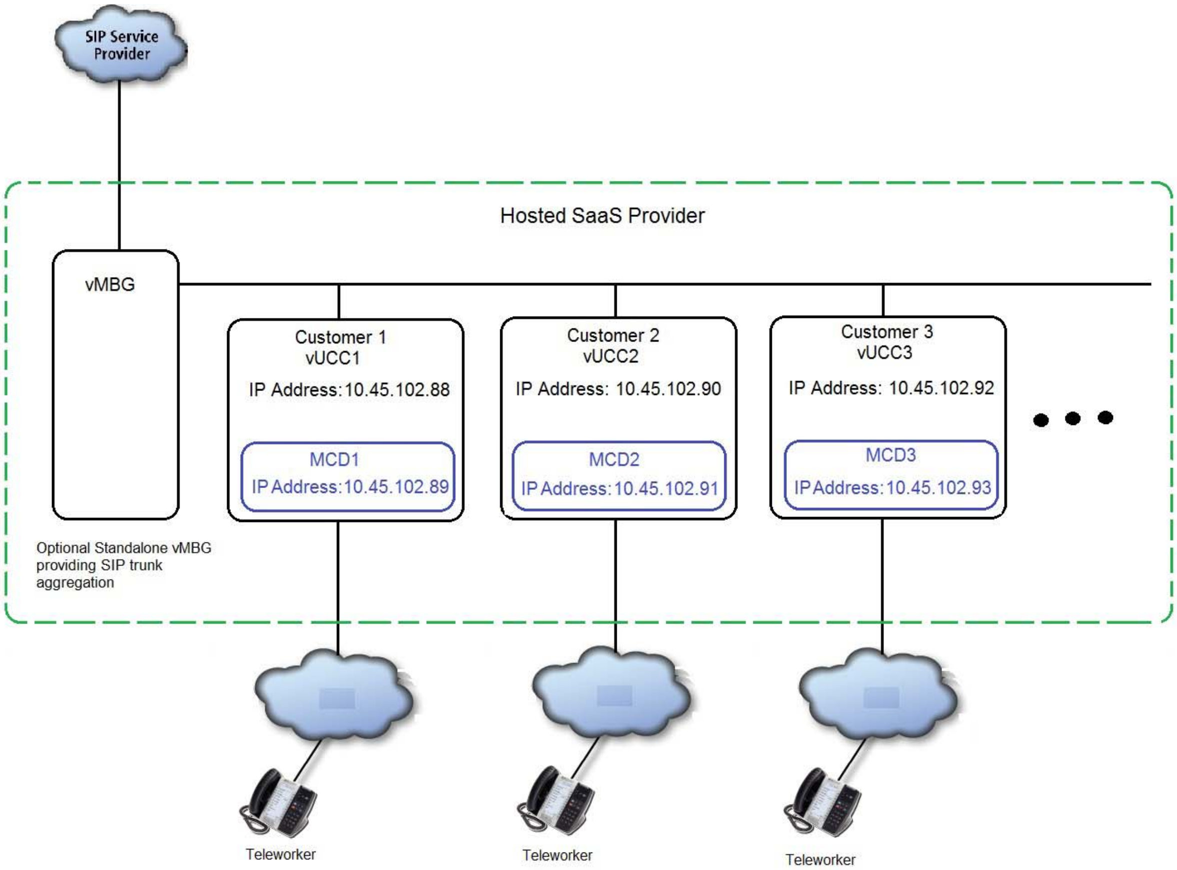
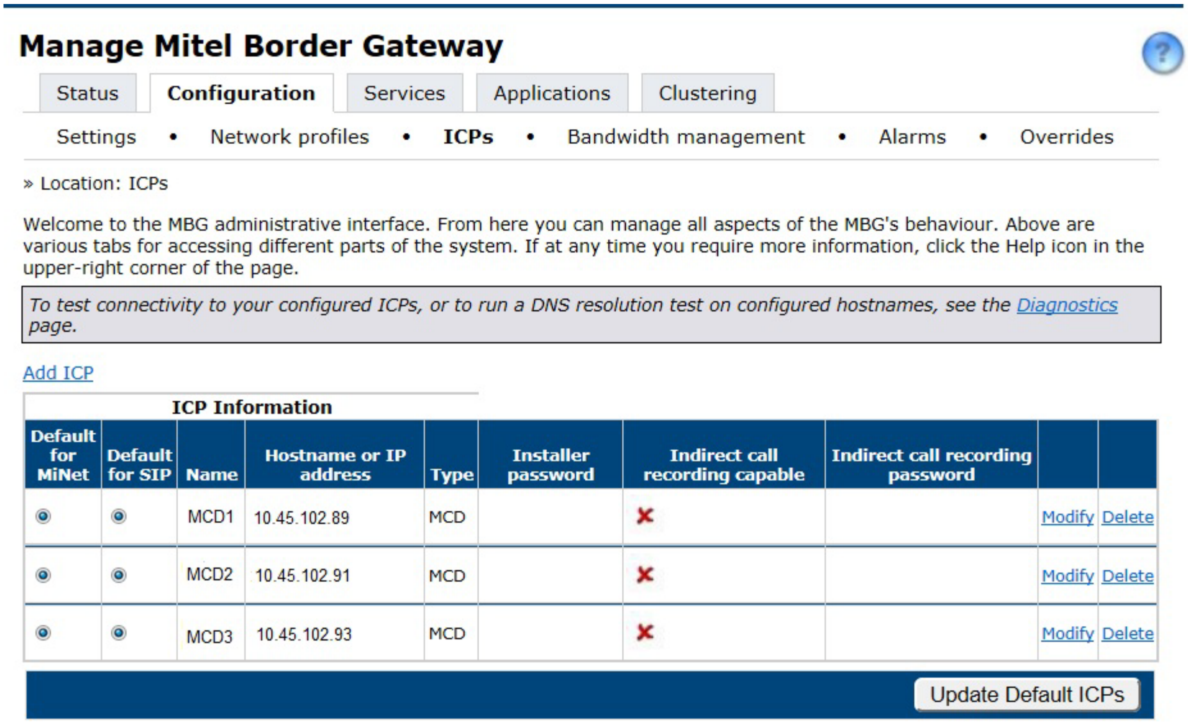


Figure 51: SIP Aggregate Trunking - Example IP Addresses

To configure SIP trunk aggregation:

1. Log into the standalone vMBG server manager.
2. Under **Applications**, click **Mitel Border Gateway**.
3. Program the vMCDs for each customer into the ICPs screen:
   - Click the **Configuration** tab.
   - Click the **ICPs** tab.
   - Click the Add ICP link to add the vMCDs into the screen. Refer to the online help for field descriptions and additional information. Figure 52 shows an example of the ICP Configuration screen.
   - Click **Save**.



Manage Mitel Border Gateway
Status
Configuration
Services
Applications
Clustering
Settings • Network profiles • ICPs • Bandwidth management • Alarms • Overrides

» Location: ICPs

Welcome to the MBG administrative interface. From here you can manage all aspects of the MBG's behaviour. Above are various tabs for accessing different parts of the system. If at any time you require more information, click the Help icon in the upper-right corner of the page.

To test connectivity to your configured ICPs, or to run a DNS resolution test on configured hostnames, see the Diagnostics page.

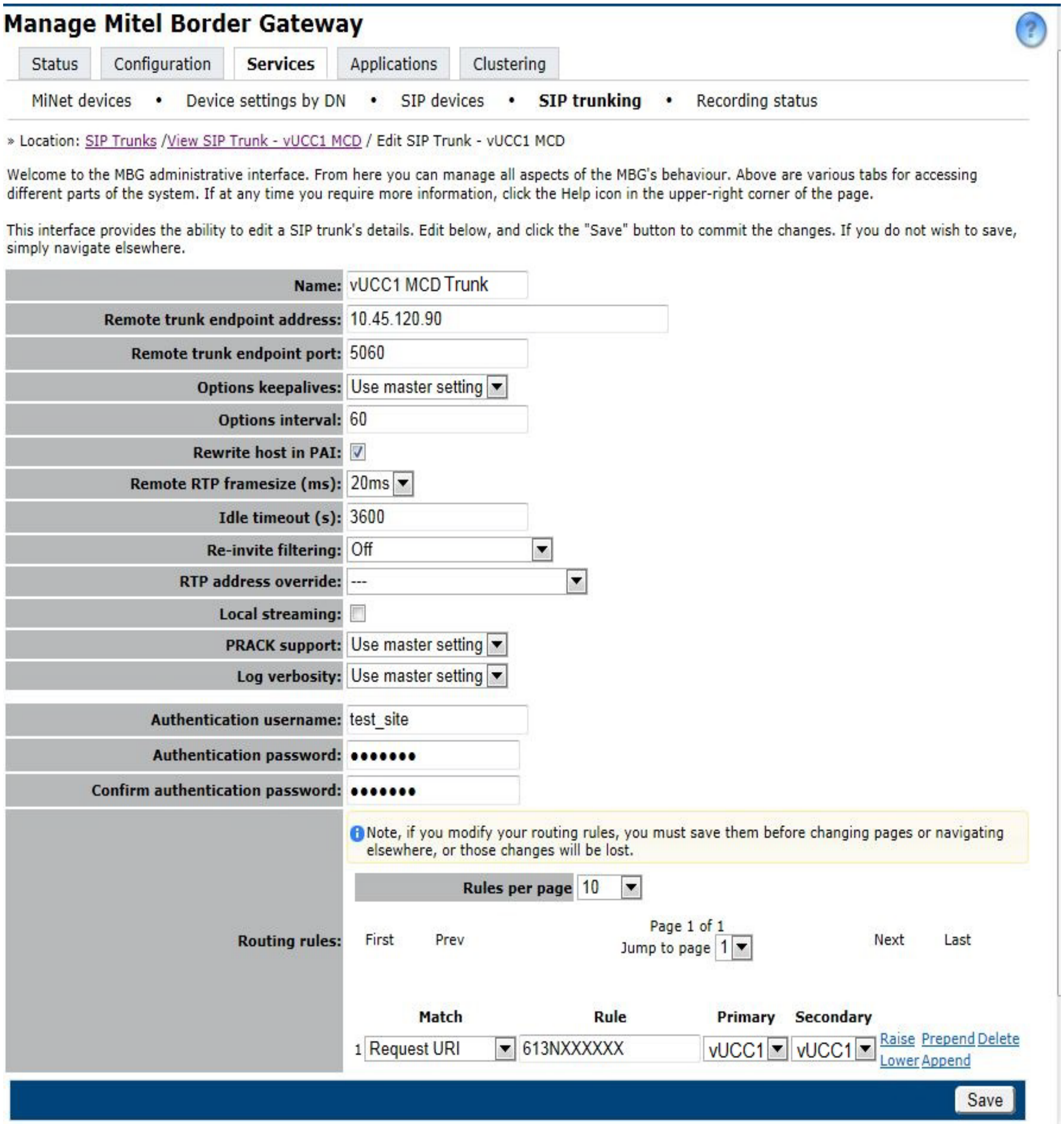
Add ICP

ICP Information

Default for MiNet	Default for SIP	Name	Hostname or IP address	Type	Installer password	Indirect call recording capable	Indirect call recording password		
◉	◉	MCD1	10.45.102.89	MCD		✗		Modify	Delete
◉	◉	MCD2	10.45.102.91	MCD		✗		Modify	Delete
◉	◉	MCD3	10.45.102.93	MCD		✗		Modify	Delete

Figure 52: ICP Configuration (Example)

4. Program SIP trunks to connect to the vUCC MCDs:
   - Click the **Configuration** tab.
   - Click the **Services** tab.
   - Click the Add a SIP trunk link to add a connection to a vUCC MCD. Refer to the online help for field descriptions and additional information. Note that you must enter the MCD IP address (not the vUCC IP address) in the "Remote trunk endpoint address" field.
   - Click **Save**.



Manage Mitel Border Gateway
Status
Configuration
Services
Applications
Clustering
MiNet devices • Device settings by DN • SIP devices • SIP trunking • Recording status

» Location: SIP Trunks /View SIP Trunk - vUCC1 MCD / Edit SIP Trunk - vUCC1 MCD

Welcome to the MBG administrative interface. From here you can manage all aspects of the MBG's behaviour. Above are various tabs for accessing different parts of the system. If at any time you require more information, click the Help icon in the upper-right corner of the page.

This interface provides the ability to edit a SIP trunk's details. Edit below, and click the "Save" button to commit the changes. If you do not wish to save, simply navigate elsewhere.

Name:	vUCC1 MCD Trunk
Remote trunk endpoint address:	10.45.120.90
Remote trunk endpoint port:	5060
Options keepalives:	Use master setting
Options interval:	60
Rewrite host in PAI:	☑
Remote RTP framesize (ms):	20ms
Idle timeout (s):	3600
Re-invite filtering:	Off
RTP address override:	---
Local streaming:	☐
PRACK support:	Use master setting
Log verbosity:	Use master setting
Authentication username:	test_site
Authentication password:	•••••••
Confirm authentication password:	•••••••

Routing rules:

Note, if you modify your routing rules, you must save them before changing pages or navigating elsewhere, or those changes will be lost.

Rules per page: 10

First Prev Page 1 of 1 Jump to page 1 Next Last

	Match	Rule	Primary	Secondary	
1	Request URI	613NXXXXXX	vUCC1	vUCC1	Raise Prepend Delete Lower Append

Figure 53: Adding a SIP Trunk

Provision Users

Depending on your site configuration, use one of the following methods to provision users on the vUCC system.

- ❒ **Import user data from a .csv file**: If a vUCC is replacing an existing PBX system, export a .csv file of the user data and then import the CSV file using the Bulk Provisioning Tool. During the import, you can apply roles and templates to provision the users with phone services and applications.
- ❒ **Sync user database with directory service**: If the site uses Active Directory and if the directory server contains an accurate, up-to-date list of users, synchronize the vUCC database with the Active Directory database.
- ❒ **Manually provision users**: If this is a new site without an existing user database, you can provision users manually from the Users and Services application.

Note: You can reduce the time spent provisioning by applying roles and templates. Roles and templates allow you to add phone services and applications to the users. Default roles and templates are available.

Import User Data From a CSV File

To import user data from a CSV file:

1. Export a CSV file of user data from the existing PBX system.
2. Log into the MAS server manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 121)
3. Under **Applications**, click **Users and Services**.
4. From the Users and Services application, define roles and user templates. See the Manage Roles and Templates book in the USP application online help for instructions. You have the option of using the default roles and templates provided by the system.

Note: The Message Waiting Indicator (MWI) is not automatically setup if a default UCC Template is used to provision a user. It is recommended that you create custom UCC templates based on the default UCC templates and modify them to use the Message Waiting method required by the customer site. Selectable Message Waiting methods for Message Waiting #1 and #2 include:

- DTMF to PBX
- Pager
- Program RS232
- Centrex RS232
- HIS PMS
- Unified Integration
- Hitachi PMS
- Mitai Messaging

Mitai Messaging is recommended as the messaging option as other methods will consume additional Voicemail ports.

5. Import users using the Bulk User Provisioning Tool in the User and Services application.

Note: In MAS Release 5.0 and higher, the Bulk User Import Tool does not support importing MAC addresses from the CSV file.

6. Assign the UCC licenses to users through the Users and Services application. See Managing UCC licenses in the USP online help for instructions.

Sync User Database with Active Directory Service

To sync the user database with an Active Directory server:

1. Log into the MAS Server Manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 121)
2. Under **Applications**, click **Users and Services**.
3. From the Users and Services application, define roles and templates. See the Manage Roles and Templates book in the USP application online help for instructions. You have the option of using the default roles and templates provided by the system.
4. Sync the databases by performing an initial synchronization.
5. Resolve any detained or failed updates.

Provision Users Manually

To provision users manually:

1. Log into the MAS Server Manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 121)
2. Under **Applications**, click **Users and Services**.

3. From the Users and Services application, create the users and assign services. See the Manual Provisioning topic in the USP application online help for instructions.

Perform Backups

After you complete initial vUCC configuration, perform the following backups:

- Backup the vUCC database (see “Server Manager Backup” on page 115)
- Backup the UCC virtual appliance using VMware tools (see page 118)
- Backup the optional vMBG. Refer to the vMBG server manager online help for instructions.

Chapter 6

Maintain

Maintenance Overview

Regular maintenance tasks include:

- □ "Performing Upgrades" on page 113
- □ "Performing Backups" on page 115
- □ "Common System Administration Tasks" on page 120

Performing Upgrades

An upgrade is when you move a vUCC system software up to a new release:

- A full upgrade installs a new release of software (for example, from vUCC Release 5.0.x to vUCC Release 6.0.x).
- A service pack upgrade installs new version of software within the same release (for example, from vUCC 5.0.2 to vUCC 5.0.3 or from vUCC 5.0.3 to vUCC 5.1.1.

Note: There are no upgrade paths from existing Mitel products (for example MAS, vMAS, MCD, or vMCD) to vUCC.

Prerequisites

- ❐ There is a connection available to the AMC.
- ❐ The new vUCC must be deployed on the same network as the current vUCC. You must configure the new vUCC with a temporary IP address to allow the backup to be restored from the current vUCC system.
- ❐ All administrative applications on vUCC are closed.
- ❐ The system is NOT processing calls. (Upgrading should be done outside of business hours.)
- ❐ Ensure that the virtual appliance has the required resources.

Upgrade

The upgrade procedure is very similar to the install procedure. You simply deploy the new OVA file and then run the Initial Configuration Wizard. From the wizard, restore the system database from a backup file on a network share. The system will be taken out of service during the restore process.

Note: All other upgrade methods, such as upgrading vUCC from the MAS admin console or from the Server Manager **Blades** panel, are not supported

1. Download the vUCC OVA file from Mitel Online to a network drive or vSphere Client PC (see page 57 for instructions).

2. Log into the MAS Server Manager. Under **Administration**, click **Backup**. Back up the vUCC database to a network drive.
3. Shut down the current (Release 5.0.x) vUCC.

Note: If you are deploying with new IP Addresses, you don't need to shut down the current vUCC until just before you start the restore.

4. Deploy the new vUCC vApp (OVA file) on the host system (see page 58 for instructions).
5. Right-click on the newly created vUCC (for example: vUCC 5.52.3.0 build) and select **Open Console**. The vUCC console opens within the vSphere Client.
6. Power on the vUCC by clicking the green button in the toolbar.
7. After you power on the vUCC VM, the Application Properties screen is displayed. In the Applications Properties screen:
   - Set the Country field. You can leave the Timezone blank. It will be restored from your database backup.
   - Leave the Hostname, Domain Name, and ARID fields blank. This information will also be restored from your database backup.
   - If you are restoring the database from a Network Share, you must enter the LAN IP Address and Netmask, a WAN IP Address and Netmask, and a Gateway IP Address.
OR
If you are restoring from the current vUCC, enter a new, temporary IP address in the LAN IP Address field. This address must available on the local LAN and be different than the one used by the current virtual appliance. The temporary IP address will be replaced by the original address during the restore.
   - Click **Next**.
8. Log into the server manager interface using the administrator password that you entered in the Applications Properties screen. See “Logging into the Server Manager (Administrator Portal)” on page 121 for instructions.
9. If you are using a temporary IP address, ensure that the current vUCC virtual appliance is shut down before you proceed with the restore.
10. Launch the Initial Configuration Wizard.
    - Click Next to display the **Configurations Options** page.
    - Click **Restore the configuration data from backup file**.
    - Navigate to the backup file.
    - Click **Next**.
11. After the restore has finished, click **Next** and the vUCC system reboots.
12. Synchronize the UCA server with MCA software versions (required to support video):
    - In MAS server manager, under **Applications**, click **Unified Communications Server**
    - Click **Configure Mitel UC Server**.
    - Click the **Collaboration** tab.
    - Click the Local MCA Server link.
    - Click **Sync Now**. The MCA Server and Client software versions are updated.

Upgrading Applications Suite Licenses

To purchase and activate additional UCC licenses:

1. Contact Mitel Customer Services (or your Service Provider) and place your order.
2. Obtain your Application Record ID from Mitel Customer Services.
3. In your AMC account, access the appropriate Application Record and assign the upgrade products from your license account to the Application Record. Assign any MCD User and Device licenses to the MCD ICP Application Record. The AMC upgrades your licenses on its hourly synchronization.
4. Access the server manager. See “Logging into the Server Manager (Administrator Portal)” on page 121.
5. Under **ServiceLink**, click **Status**.
6. Click the **Sync** button to download your AMC license upgrades. UCC licenses are applied automatically during the synchronization.

Performing Backups

There are two methods that you can use to back up system data (including all server configuration data, application configuration data, user settings, messages, and greetings):

- **Server Manager "Backup"**: allows you to perform backups of the vUCC database (includes the application databases and the MCD system database) to a local desktop computer or schedule backups to a network file server.
- **VMware Tools**: allow you to back up the vUCC OVA file (see “vUCC Backups using VMware Tools” on page 118).

Notes:

1. You can use different filenames for database backup files, but the filename must not contain spaces and the file extension must be TGZ. For example: "backup_file_Jan23.tgz"
2. If vUCC is deployed in LAN only mode with Teleworker running remotely on an vMBG in the DMZ, you should back up both the vUCC database and the vMBG database at the same time.

Server Manager Backup

Backup to Desktop

Use this procedure to save your system backup to a file or device on your desktop computer or maintenance PC.

A **Backup to desktop** operation saves all of the data to a single, large compressed file and is therefore limited by the maximum file size of the client operating system. For example, if you are backing up data to a Windows client that uses the FAT file system (the default for many versions of Windows), you are limited to a maximum file size of 2 GB. Other file systems may have a larger limit. If the backup file exceeds the maximum file size of the client operating system, it cannot be properly restored.

1. Log into the Administrator portal (server manager). See page 121 for instructions.
2. Under **Administration**, click **Backup**.
3. Select the **Backup to desktop** option.
4. Click **Perform**. MSL prepares the system for backup. The "Backup to desktop - Operation status report" screen is displayed with the estimated backup size.
5. Ensure that your browser and target file system support downloads of this size, and click **Begin Download**.
6. When prompted to Open or Save, click **Save**.
7. In the file download screen that appears:
   - Name the file and then select the location where the file will be saved. Note that the filename of the backup must not contain any spaces; otherwise, you will receive an error when you attempt to restore it.
   - Click **Save**.
   - In the Download Complete Window, click **Close**.
   - After saving, you can copy the backup file to a CD/DVD or USB storage device, if required.

Schedule Backups to Network File Server

Use this option to

- perform immediate system backups to a Network File Server
- schedule daily, weekly, or monthly system backups to a Network File Server.

Note: You can only have one backup scheduled on the server. To cancel an existing backup schedule, select **Disabled** and then click **Update**.

Before you can perform network backups, you must create a shared folder on the Network File Server that allows network users to write to the folder. For example, to create a shared folder on a PC running Windows 7:

1. Right-click on the desktop and select **New** and then select **Folder**.
2. Name the folder, for example: "vUCC Backups".
3. Right-click on the folder and select **Properties**.
4. Click the **Sharing** tab.
5. Click **Share**.
6. Select "Everyone" and click **Add**.
7. Set the Permission level to Read/Write.

8. Click **Share**.
9. Click **Done**.

Next, specify the Network File Server and shared folder in the MAS server manager interface:

1. Log into the MAS server manager.
2. Under **Administration**, click **Backup**.
3. From the **Select an action** list, click **Configure network backup**.
4. Click **Perform**.
5. Identify the server where the backup file will be stored.
   - Enter the **IP address** of the file server where the backup will be stored.
   - Enter the **Sharename** of the shared folder where the backup file will be stored. (For example, "vUCC Backups".) You must set the permissions of the shared folder to allow network users to write files to the folder.
   - Enter an **Optional Sub Directory** for the backup file, if desired. The specified directory must exist in the share folder. The field accepts multi-level directories; for example "vUCC/Sept/backups". If you leave this field blank, the system stores the file in the root directory of the specified network share.
   - Enter the **Username** to use when connecting to the backup server.
   - Enter the **Domain or Workgroup Name** of the server. (For example, mitel.com.)
   - Enter the **Password** to use when connecting to the backup server.
   - (Optional) Select the **Maximum number of backup files to keep** (1-999) on the server. When the number of stored files reaches this maximum count, the oldest version is deleted.
   - Click **Update**.

To perform an immediate backup

1. Click **Backup Now**.

To schedule backups to a network file server:

1. Under **Administration**, click **Backup**.
2. From the **Select an action** list, click **Configure network backup**.
3. Click **Perform**.
4. Select the frequency with which you want to perform backups. Backup file names will include timestamps, for example: mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz).
   - To disable regularly scheduled backups, click **Disabled**.
   - For Daily backups, select a time of day (hour, minute, AM/PM).
   - For Weekly backups, select a time of day, and day of the week.
   - For Monthly backups, select a time of day, and day of month.
5. Click **Save**.

vUCC Backups using VMware Tools

You can use the following VMware tools to create vUCC backups to recover the system from database corruption or disaster situations:

- Export of vUCC OVA file from vSphere Client
- VMware Data Recovery
- vStorage APIs for Data Protection (VADP).

Note: "VMware Data Recovery" and "vStorage APIs for Data Protection" are optional tools. vUCC does not support VMware Site Recovery Manager (SRM).

Note: Snapshots are not supported for vUCC (regardless of whether the vUCC virtual appliance is powered on or off). vUCC system performance is degraded if snapshots are present on the platform.

Exporting an OVF Template

The vSphere Client allows you to export an OVF template of the vUCC virtual appliance. An OVF template is essentially a copy of the virtual appliance in OVA file format. In the event of database corruption, you can deploy the exported OVF template file to the VMware vSphere platform to restore the vUCC virtual appliance.

1. Shut down the vUCC virtual server from the vSphere Client:
   - Right-click on the vUCC instance.
   - Select **Shutdown Guest**. The normal shut down sequence appears on the server manager console.
2. From the vSphere Client select **File > Export > Export OVF Template**:

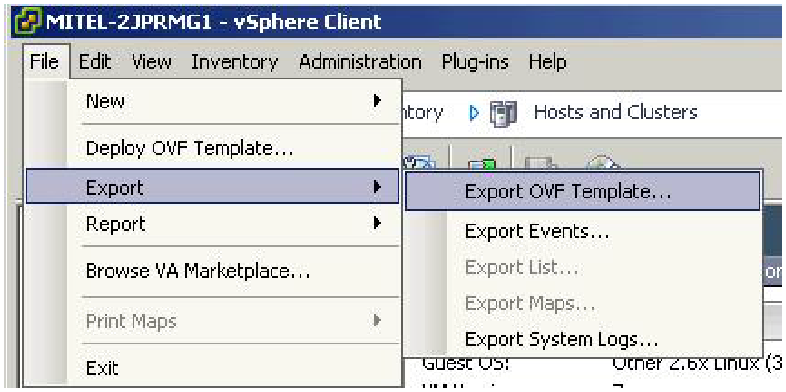
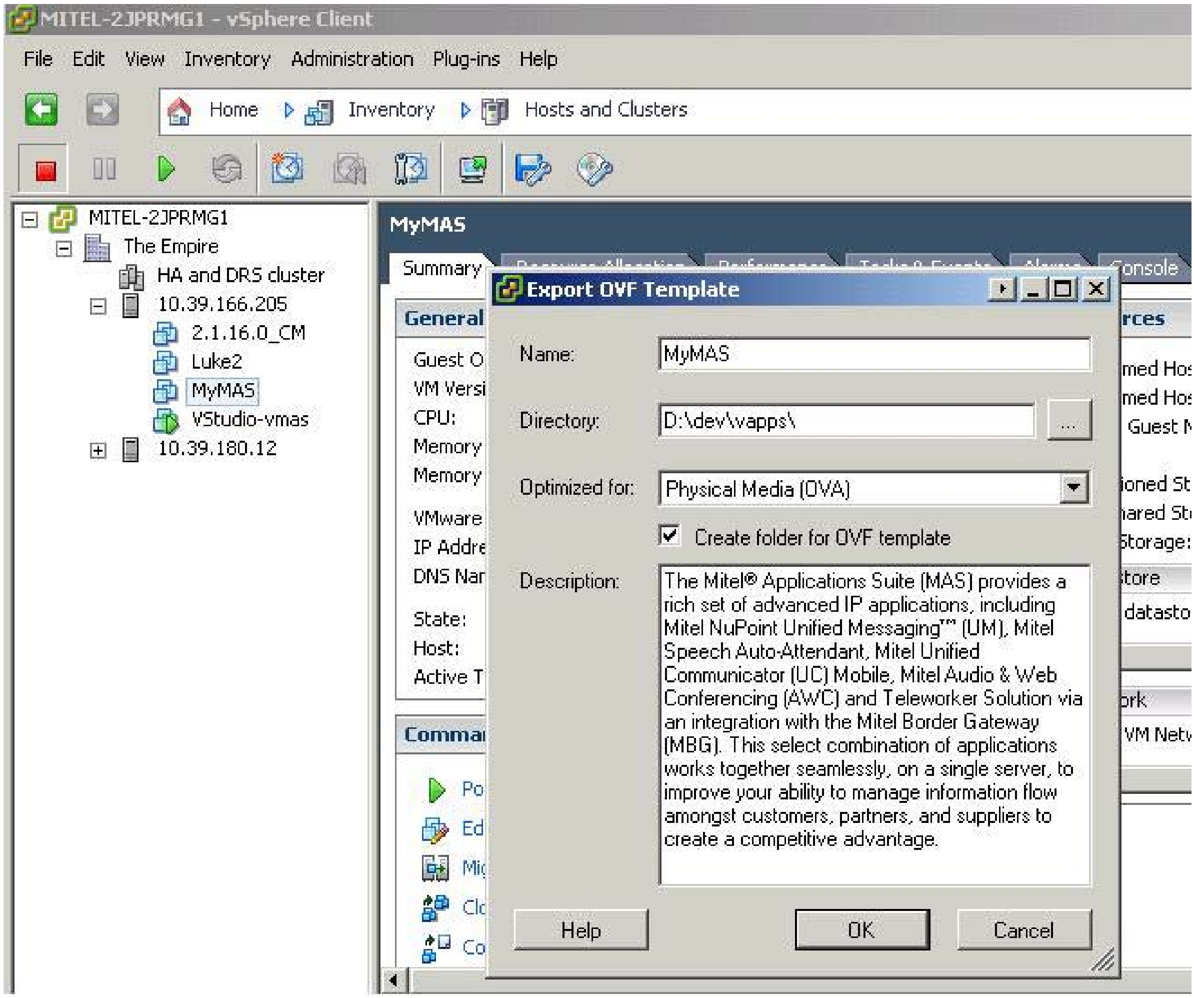


Figure 54: Exporting OVF Template

3. Enter the Name of the OVF Template file and specify the directory where you want the file to be saved.
4. Select either Optimized for Physical Media (OVA) or Web
   - **Physical Media (OVA)**: export consists of a single OVA file (recommended).
   - **Web**: export consists of multiple files.
5. Select the **Create folder for OVF template** check box.



Export OVF Template

Name: MyMAS

Directory: D:\dev\vapps\

Optimized for: Physical Media (OVA)

☑ Create folder for OVF template

Description: The Mitel® Applications Suite (MAS) provides a rich set of advanced IP applications, including Mitel NuPoint Unified Messaging™ (UM), Mitel Speech Auto-Attendant, Mitel Unified Communicator (UC) Mobile, Mitel Audio & Web Conferencing (AWC) and Teleworker Solution via an integration with the Mitel Border Gateway (MBG). This select combination of applications works together seamlessly, on a single server, to improve your ability to manage information flow amongst customers, partners, and suppliers to create a competitive advantage.

Figure 55: Export OVA Template: Set Parameters

6. Click **Ok**. A progress bar is displayed. A "Completed successfully" dialog box appears when the export is done.

7. Restart the vUCC virtual server from the vSphere Client:
   - Right-click on the vUCC instance.
   - Select **Restart Guest**. The normal startup sequence appears on the server manager console.

Common System Administration Tasks

Shutting Down vUCC

You can power off, power on, restart, and suspend the virtual appliance from the vSphere Client. The basic vSphere Client power operations for a virtual appliance are listed in Table 14.

Table 14: Virtual Appliance Power States

vSphere Client Operation	Description
Shutdown Guest	Performs a graceful shut down of the vUCC operating system.
Power Off Guest	Performs a hard reset, similar to disconnecting the power source. Use the **Shutdown** option instead of the **Power Off** option to shut down a vUCC system.
Suspend Guest	Pauses the virtual appliance activity. All operations are stopped until you issue the **Resume** operation. This feature is typically used to free up computing resources on a short-term basis without shutting down the virtual appliance. **WARNING:Do NOT suspend the vUCC. It results in a loss of communication services and could cause database corruption.**
Resume Guest	Resumes virtual appliance operation from a suspended state.
Restart Guest	Restarts the virtual appliance guest operating system and application gracefully. It is recommended that you perform the **Reboot** operation from the **Reboot or Reconfigure** screen of the MAS server manager to perform a system reboot.
Power On Guest	The Power On starts a virtual application. To minimize downtime of Mitel vApps, set the "Virtual Machine Startup and Shutdown" setting to allow virtual appliances to start and stop automatically with the system on a single server configuration. If several Mitel vApps are configure to run on the same server, you may need to adjust the startup order based on the vApp startup dependencies. Refer to the *Virtual Appliance Deployment Solutions Guide* for information regarding start-up order.

Note: You can specify the type of power operation that occurs when you click the power buttons on the vSphere console toolbar. Assign the **Shutdown** operation to the **Power Off** (red square) button to initiate an orderly shutdown of virtual appliances.

Scheduling a vUCC power state change

You can use the vSphere Client scheduled task wizard to schedule power state changes for the vUCC. For example, you could schedule a reboot of the vUCC to occur at a specific time each day. You must ensure that the scheduled power state change does not conflict with a vUCC scheduled activity (for example, scheduled database backup to a network file server).

Shutting Down vUCC

Shut down vUCC using the **Shutdown Guest** operation from the vSphere Client. This operation performs a graceful shutdown of the guest MSL operating system. In normal circumstances, do not use the **Power Off** operation since this performs a hard reset (similar to disconnecting the power source).

To shut down the vUCC virtual server from the vSphere Client:

1. Right-click the vUCC instance.
2. Select **Shutdown Guest**. The normal shut down sequence appears on the server manager console.

To restart the vUCC virtual server from the vSphere Client:

1. Right-click the vUCC instance.
2. Select **Restart Guest**. The normal startup sequence appears on the server manager console.

Logging into the Server Manager (Administrator Portal)

The vUCC server manager is a web-based administrator portal that provides a central location for configuring the virtual appliance and system settings. This administrator portal web interface provides access to the

- Server Manager - allows you to configure and maintain the virtual appliance
- Application Web Pages - allow you to configure and administer the installed applications (for example NuPoint Unified Messenger).

Web browser access to vUCC administration and end-user interfaces is provided through

- Internet Explorer 8.0, 9.0, or 10.0 (Note that Internet Explorer 7.0 is not supported)
- Google® Chrome™ 21 or higher
- Mozilla® FireFox® 14 or higher

To log into server manager:

1. On a PC on the same subnet as the vUCC server, open a browser and enter the following URL in the address bar:
   https://<*IP Address of the vUCC*>/server-manager

Note: If your client PC is on a different subnet than the vUCC, you must add your local network in Server Manager Local Networks Page.

2. Enter User Name (default is "admin") and the system Password that you created during installation, and then click **Login**. The administrator portal opens.
3. Do one of the following:
   - In the left-hand menu, under **Applications**, click an application name to open the interface of that application.
   - Click the **Help** link in the administrator portal for detailed server administration instructions.
4. By default, MAS is configured to send a Welcome E-mail to new users. The e-mail contains:

- a link to the My Unified Communications web portal, and
- the user's login ID, password, and passcode

See Configure Service Information Email in the *MAS Administrator online help* for the Service Information (Welcome) E-mail configuration options. In order for the system to list the Speech Auto Attendant pilot/access number in the Service Information E-mail, you must enter the pilot number into the Network Element screen of MAS.

If you choose to disable the Service Information E-mail functionality, you will need to advise users of the URL for the My Unified Communications portal:
https://<*IP Address of the vUCC*>/portal

5. Proceed to "Installing a Web Certificate" on page 123.

Logging into the Mitel Communications Director (MCD) Tools

The MCD includes a number of Embedded System Management (ESM) programming tools:

- **System Administration Tool** that provides a Web-based interface that trained technicians use to program the system.
- **Group Administration Tool** that provides a Web-based interface to enable administrators to make changes to user information.
- **Desktop Tool** that provides a Web-based interface to enable display IP telephone users to program feature keys on their phone.

Obtain MCD System IP Address

1. Log into the Server Manager (see page 121).
2. Under **Applications**, click **Mitel Communications Director**.
3. Record the MCD System IP Address.

Logging into the Tools

To log into one of the ESM tools:

1. Launch a browser and enter the URL of the MCD system:
   https://<System IP Address>
2. To log into the ESM tools screen:
   - In the **Login ID** field enter "admin".
   - In the Password field, enter the vUCC Administrator password that you configured during the Initial Configuration Wizard.
   - Select **Remember Login ID** if you want to save the Login ID on your computer.
   - Click **Log In**.

Note: The Administration password that you configured in the Initial Configuration Wizard is applied to the MAS server manager, MAS server console, and MCD Embedded System Management tools. However, if you later change the password from a MAS administration interface, the change is not applied to the MCD administration tools. Likewise, if you change the password from the MCD system administration tool, the change is not applied to the MAS administrator interfaces. This is because the MAS and MCD admin accounts are separate and independent.

Note: When logging into the MCD administration tools on the vUCC, you must enter "admin" as the username (not "system" which is the default username for standalone MCD systems).

3. Click the desired Tool (Desktop, Group Administration, or System Administration).
4. You might be prompted to install some XML Components when you log into the System Administration Tool for the first time. At the following prompt, “Do you wish to install or upgrade the required XML components?”, click “Install Now”. The install takes less than 30 seconds and you do not need to restart your computer.

Note: The system will allow up to five concurrent System Administration Tool or Group Administration Tool sessions (or any combination of the two) provided that the initial login browser is closed plus ten concurrent Desktop Tool sessions.

Note: The System Administration Tool will temporarily lock you out for 15 minutes after three consecutive attempts to log in have failed.

Installing a Web Certificate

When users connect to their My Unified Communications portal for the first time, they may get a warning message stating that there is a problem with the website’s security certificate or that your browser has blocked the content. This message appears because the application web server is not recognized as a trusted site. Users can safely select the option to continue to the application web server site.

To prevent these security warnings from appearing

- install the Mitel Root CA certificate locally on each user’s client PC, or
- purchase and install a Secure Sockets Layer (SSL) certificate from a third-party Certificate Authority (CA).

For instructions on how to install the Mitel Root CA certificate (security certificate), see the *Install Mitel Root Certificate* topic in the My Unified Communications portal online help.

For instructions on how to install a third-party SSL certificate, refer to the Manage Web Server Certificate topic in the Server Manager online help for details.

- To prevent the Security Alert warning from appearing on client stations on the local network, purchase a Secure Sockets Layer (SSL) certificate for the vUCC virtual appliance and then import it onto the vUCC virtual appliance.

- To prevent the Security Alert warning from appearing on remote client stations, purchase a Secure Sockets Layer (SSL) certificate for the MBG Web Proxy server and then import it onto the MBG Web Proxy server.

Allow Local Network Access

If the users are deployed on a different subnet than the vUCC virtual appliance, it is necessary to grant them local network access. First, you must configure them as a trusted Local Network and then grant them express permission.

To configure Local Networks:

1. Log into the MAS server manager (see page 121).
2. Navigate to **Local Networks** in the **Security** section and then click **Add**.
3. Enter the **IP Address** of the network to which you are granting access. (For example, 168.195.52.0).
4. Enter the **Subnet** mask to apply to the network address. (For example, if your network IP address is 168.195.52.0 and you want to allow access to all network IP addresses in the range from 1 to 255, enter 255.255.255.0. This allows IP addresses 168.195.52.**1** through 168.195.52.**255** to access your virtual appliance).
5. Enter the **Router address**. (IP address of the router on your local network).
6. Click **Save**.
7. Repeat steps 1 through 5 to configure additional trusted networks.

To grant secure shell access to the Local Network you have created:

1. Log into the MAS server manager (see page 121).
2. Navigate to **Remote Access** under the **Security** section.
3. In the **Secure Shell Access** field, select one of the following:
   - **No Access**: select this option to restrict access to your own local network
   - **Allow access only from local networks**: select this option to allow access to selected local networks. This is the recommended setting.
   - **Allow Public access (entire Internet)**: select this option to allow access to the entire Internet. This setting is NOT recommended.
4. In the **Allow administrative command line access over secure shell** field, do one of the following:
   - Select **Yes** to allow users to connect to the virtual appliance and log in as root.
   - Select **No** to restrict users from logging in as root.
5. In the **Allow secure shell access using standard passwords** field, do one of the following:
   - Select **Yes** to allow users to connect to your virtual appliance using a standard password.
   - Select **No** to restrict virtual appliance access to users with RSA Authentication.

6. Click **Save**.

Changing the System Language

During the initial deployment of a new system, you set the system language. End-users can also set the language of their My Unified Communications interface from their portal login screen and set the prompt language from their Settings screen.

To change the system's end-user language to one of the other supported languages (such as North American English, British English, Canadian French, European French, Dutch, Latin American Spanish, or German):

1. Log into the MAS server manager (see page 121).
2. Under **Configuration**, click **Application Suite Language**.
3. Select the desired language from the Language drop-down box.
4. Click **Save**.

Note: For details regarding language support, see Configure Applications Suite Language Settings in the Server Manager online help.

Chapter 7

Troubleshoot

Viewing or Collecting Log Files

To assist in troubleshooting, you can either view or download the log files generated by the services running on MAS.

To view/download the log files:

1. Under **Administration**, click View **log files**.
2. Under View Log Files, choose a log view. Most system services write their logs to the messages file.
3. Enter a **Filter Pattern** to view online the lines of the log that contain that text. This option applies only to viewed files. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.

   A regular expression (abbreviated as regexp, regex, or regxp) is a string that describes or matches a set of strings, such as particular characters, words, or patterns of characters, according to certain syntax rules. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification.
4. Specify a **Highlight Pattern** to mark in bold the specified text in any logs that the text appears. This option applies only to viewed files. Check the Regular expression box if you want to apply the text filter in the format of a regular expression.
5. From **Operation**, select **View log file** or **Download**.
6. Click **Next**. If you selected **View log file**, the log files are displayed.

Note: The system automatically updates the list every 5 seconds with any new logs.

Database Restore or Recovery

This section provides procedures for

- vUCC database restore
- vUCC system disaster recovery.

Conditions and Constraints

The following conditions and constraints apply to database restores:

- Do not attempt to restore a database that has been taken from an individual application (for example, a NP-UM database) within MAS to a vUCC deployment.
- All application data programmed in the vUCC database is overwritten by the backup data during the restore operation. The data in the backup is not merged with the existing database.
- You cannot restore a vUCC OVA file from a newer vSphere platform to a platform with an older version of vSphere. For example, you cannot restore a vUCC OVA file that was exported from a vSphere 5.1 platform to a vSphere 5.0 platform.

Restoring a Database Backup

To restore a vUCC system database:

1. Log into the server manager interface using the administrator password that you entered in the Applications Properties screen. See "Logging into the Server Manager (Administrator Portal)" on page 121 for instructions.
2. Launch the Mitel Integration Wizard.
   - Select **Upgrade**.
   - Navigate to the backup file.
   - Click **Restore**.
3. After the restore is finished, the vUCC system software upgrade procedure is complete.
4. If Teleworker is running remotely on a vMBG server in the DMZ, you must also restore the vMBG server with the current database; otherwise, the databases will be out of synch.

vUCC System Disaster Recovery

You can recover a vUCC system on the same virtual appliance by deploying the latest vUCC OVF file and then restoring your vUCC database backup.

Note: VMware SRM cannot be used for vUCC disaster recovery.

1. Download the vUCC OVA file from Mitel Online to a network drive or vSphere Client PC (see page 57 for instructions).
2. Shut down the current vUCC.
3. Deploy the new vUCC (OVA file) on the host system (see page 58 for instructions).
4. Right-click on the newly created vUCC (for example: vUCC 5.2.3.0 build) and select **Open Console**. The vUCC console opens within the vSphere Client.
5. Power on the vUCC by clicking the green button in the tool bar.
6. After you power on the vUCC VM, the Application Properties screen is displayed.
   - Complete the fields in the Application Properties screen with the information for the existing vUCC VM. Note that if you enter different IP addresses, they will be overwritten buy the addresses from the backup file when you perform the restore.
   - Click **Next**.
7. Log into the server manager interface using the administrator password that you entered in the Applications Properties screen. See "Logging into the Server Manager (Administrator Portal)" on page 121 for instructions.
8. Launch the Initial Configuration Wizard.
   - Select **Upgrade**.
   - Navigate to the backup file.
9. Click **Restore**.

Troubleshooting Chart

Note: Refer to the Virtual Appliance Quick Reference Guide for a list of the top five problems encountered while deploying Mitel virtual appliances, as reported by Support. This guide is available at http://edocs.mitel.com/TechDocs/Solutions-Guides/vQuickRef.pdf

Symptom	Possible Cause	Corrective Action
When you attempt to deploy the vUCC VA, an error message appears indicating that the OVF properties are not supported.	You are attempting to deploy the vUCC from the vSphere Client directly to an ESXi host.	Install vSphere vCenter prior to the initial deployment of vUCC.
In the VMware deployment wizard, the IP Address fields in the Properties screen are truncated.	If your PC screen resolution is set above 100%, for example 125%, some IP Address fields in the wizard may be truncated.	Ensure that your PC display resolution is set to 100%.
Unable to access MAS server manager interface after deployment.	An invalid LAN IP address was entered in the vUCC Properties screen during OVF deployment.	Enter a valid LAN IP or WAN IP address through the MAS server console interface: 1. Right-click on the newly created vUCC (for example: vUCC 5.1.3.0 build) and select **Open Console**. The vMAS virtual appliance console opens within the vSphere Client. 2. Power on the VM by clicking the green button in the toolbar. 3. Click the **Console** tab. The MSL Server Console boots up and the server console login prompt appears. 4. Place the cursor in the console screen and enter the vUCC administration login and password. If at any time you need the cursor available for other desktop activities, press the CTRL + ALT keys. 5. Use the Server Console menu to correct the IP address(es)
	An valid LAN IP address was entered in the vUCC Properties screen during OVF deployment, but this IP address is not on the same subnet as the vUCC.	
During the Initial Configuration Wizard, you receive an insufficient license error on the Initial Configuration screen.	The licensing key is missing the minimum required number of licenses to support deployment.	In the AMC, add the specified licenses to the vUCC Base ARID, vUCC ULM ARID, or both as indicated in the warning message
Cannot power up vUCC.	You have cloned a vUCC and are attempting to power it up.	Cloning of an vUCC is not supported. You can only clone vUCC templates.

Symptom	Possible Cause	Corrective Action
After you deploy the vUCC and complete the Initial Configuration Wizard, the UCA clients cannot connect to vUCC via the WAN IP.	The UCA Advanced Connector is not configured with the vUCC LAN IP Address.	1. Log into the MAS server manager. 2. Under **Applications**, click **Mitel Border Gateway**. 3. Click **Applications**. 4. Click **UC Advanced**. 5. Click **Edit**. 6. Check the **UC Advanced connector enabled** box. 7. Enter the vUCC LAN IP Address in the following three fields: • UC Advanced hostname or server IP address • Nupoint Voicemail hostname or server IP address • Collaboration server hostname or server IP address.
vUCC system performance is slow.	VMware resources are inadequate.	1. Log into the MAS server manager. 2. Under **Administration**, click M**itel Virtualization**. 3. Run the Mitel Virtualization Diagnostics Tool. 4. See the *Virtual Appliance Deployment Solutions Guide* This guide lists the resource requirements for all Mitel virtual solutions.
	You have taken snapshots of vUCC. System performance is degraded if snapshots are present on the platform	Delete all vUCC snapshots from system.
After importing (restoring) an vUCC OVF template backup file, system performance and voice quality is poor.	Network adapter type is set incorrectly. After a importing an OVF template file, the network adapter type is reset to default. The network adapter must be reset to type VMXNET3.	Set the network adapter to type VMXNET3: 1. In the vSphere Client, click the vUCC App properties **Hardware** tab. 2. Select Network adapter 1 from the Hardware list. 3. Click **Remove**. 4. Click **Add**. 5. From the "Adapter type" drop-down menu, select MXNET3. 6. Click **Next** and then click **OK**.

Symptom	Possible Cause	Corrective Action
Voice quality issues	VMware resources are inadequate.	1. Log into the MAS server manager. 2. Under **Administration**, click M**itel Virtualization**. 3. Run the Mitel Virtualization Diagnostics Tool. 4. See the *Virtual Appliance Deployment Solutions Guide* This guide lists the resource requirements for all Mitel virtual solutions.
	vUCC is installed in the vSphere environment using **Thin** provisioning. Thin provisioning can cause voice quality issues due to disk sharing.	Reinstall vUCC and select Thick provisioning during the install wizard.
The Table of Contents or help topics in an application online help system are not present or not functioning correctly in Internet Explorer 10.0.	Help compatibility issues with Internet Explorer 10.0	Put the browser in compatibility mode by clicking the Compatibility View icon located in the browser address bar on the right side.

Appendix A

System Defaults

Introduction

This appendix identifies the following system defaults:

- Defaults applied from the Application Configuration page to the OVF property configuration file during initial configuration
- Default settings applied to the vMCD, vMAS, and vMBG applications by the Initial Configuration Wizard
- Default MCD Class of Service (COS) settings applied to new users that are created using single-point of provisioning from Active Directory or MAS, and
- Default UCC Roles and Templates that you can use to assign UCC licenses to users.

Application Configuration Page Defaults

The settings that you enter in the Application Configuration screen define the vUCC OVA properties are applied to the OVA.

Table 15: Application Configuration Page Defaults

Configuration Item	Description	Default
Time zone Setting	Time zone setting for the vUCC.	No default
Country	Country in which vUCC is being deployed.	Matches the time zone default setting
Admin password	Initial administrator password for the MAS server manager after the VA is deployed. The initial configuration wizard requires you to change the administrator password. If you leave the password field blank, MSL will not boot.	No default
Host name	Host name used by the vUCC. This field can be left blank for template creation.	vUCC
Domain Name	Domain name for this host. This field can be left blank for template creation.	mycompany.local.
UCC License Key	Record ID for licensing the system. This field can be left blank for template creation.	Blank
DNS Server IP	DNS Server IP Address(es)	No default
LAN IP Address	IP address for the local (LAN) interface. The selected IP address must belong to the local (LAN) interface. This address can be left blank for template creation, but must be set in the VM "Edit Settings" > Option > vApp Options > Properties dialog box before you power on the VM.	No default
LAN Netmask	Netmask of the LAN	No default

Table 15: Application Configuration Page Defaults

Configuration Item	Description	Default
WAN IP Address	IP address for the external (WAN) interface. The IP address selected must belong to the external (WAN) interface. This IP address can be left blank for template creation, but must be set in the VM "Edit Settings" > Option > vApp Options >Properties dialog box before you power on the VM.	No default
WAN Netmask	Netmask of the WAN	No default
WAN Gateway Address	WAN Gateway IP Address	No default

Initial Configuration Wizard Defaults

To simplify initial configuration, the wizard applies default settings to the vUCC system. Default settings are applied to the vMAS, vMCD and vMBG applications.

Standard Default Settings

Refer to the following online help file for the standard default settings that are applied to the vMCD platform and vMAS applications:

MCD and MAS default settings

vUCC-Specific Default Settings

Table 16 summarizes the default settings that are applied specifically to vUCC deployments.

Table 16: vUCC Application-Specific Defaults

Application	Configuration Item	Default
MCD	System Administration Tool Login and Password	Defaults to MAS server manager Username and Password.
MCD	Administrator email address and SMTP email	Defaults to settings in MAS server manager under Configuration > E-mail settings.
MCD	Licenses and Options	Refer MCD defaults (go to link above) with the following additional defaults: • No Extended Agent Skill Groups • Maximum Elements per Cluster = 30 • Maximum Configurable IP Users and Devices = 700 • No Extended Hunt Groups.

Table 16: vUCC Application-Specific Defaults

Application	Configuration Item	Default
MCD	Class of Service (COS), Feature Access Codes (FAC), Speed Calls, Station Message Detail Recording (SMDR) Options	See Standard Defaults
MCD	Class of Restriction (COR)	When you create a user from the MAS USP application, the user is created with COR 2.
MCD	Domain Name, Primary and Secondary DNS servers	Defaults to the settings in MAS server manager under Configuration > Domain
MCD	Date and time zone	Defaults to the settings in the MAS server manager under Configuration > Date and Time.
MCD	SIP Trunks	SIP peer profile defaults are provided for common SIP Service Provider on a per-country basis. The SIP Network Element name defaults to the SIP Service Provider Name. The number of SIP trunk defaults to 1. For North America, you are prompted for a local number (main business number) and the number of digits dialed for that local number (7 or 10). This local number is typically registered with the Service Provider. You are also prompted for username and password to access the SIP Service Provider.
MCD	SIP Trunk Proxy	Defaulted if MBG SIP Proxy is onboard the vUCC system, configurable if MBG SIP proxy is on an external MBG. SIP Network Element name is defaulted. You are prompted for external MBG SIP proxy FQDN or IP address.
MCD	Automatic Route Selection	See Standard Defaults
MCD	Voicemail Hunt Group	Defaults to hunt group pilot number 7000 with 4 ports starting at 7001. Message waiting indicator set to HCI reroute. HCI hunt group defaulted to 7400.
MCD	Call Services Emergency ID (CESID)	Defaults to main business number.
MCD	MCA Hunt Groups	Defaults to hunt group pilot number 7850 with 3 ports starting at 7851.
MAS	Application Suite Language setting	Language set based on country selection.
MAS - NPM	Voice mail message storage per user	200 voice mail messages per user (LCOS 1).
MAS - NPM	Limits COS and Feature COS settings	Refer to NuPoint Messaging documentation for the LCOS and FCOS default settings. For LCOS settings, see LCOS settings For FCOS settings, see: FCOS settings

Table 16: vUCC Application-Specific Defaults

Application	Configuration Item	Default
MAS-NPM	NuPoint Administrator Mailbox	By default, only generic non-customer-specific greetings are supported.
MCA	MCD COS options for MCA ports	See Standard Defaults
MCA	Administrator email settings	Defaults to settings in MAS server manager under Configuration > E-mail settings.
UCA	Database management mode	The "first-run" wizard puts the UCA server in integrated mode using the default MSL domain name and time zone. The language defaults to the MAS application suite language
MBG	SIP Connector	SIP Connector is provisioned if internal SIP proxy is used.

Route and Class of Restriction Defaults

The Initial Configuration Wizard configures the system with the following default call types:

- Local
- Long Distance
- Overseas
- Emergency
- Mobile
- Toll Free
- Premium

Each call type is assigned a default route, Class of Restriction (COR) group number, and digit modification plan. The administrator provisions each user with a COR group number through the MCD System Administration tool (see “Assign Classes of Restriction” on page 98). The COR group number determines the type of calls that the user is allowed to make. By default, users are assigned COR group 2, which allows them to make Local and Long Distance calls, but restricts them from making Overseas calls.

Table 17: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Local	1	1	4, 5, 8	1-3, 6, 9-75	1	0
Long Distance	2	2	1, 4, 5, 7, 8, 10-75	2-3, 6, 9	1	0
Overseas	3	3	1, 2, 4-8, 10-75	3, 9	1	0
Emergency	4	4		1, 2-75	0	0
Mobile Calls	6	6	1, 2, 4, 5, 7, 8, 10-75	3, 6, 9	0	0

Table 17: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Emergency	7	4		1, 2-75	1	0
Toll Free	8	8	4, 5	1-3, 6-75	1	0
Premium	9	9	1-8, 10-75	9	1	0

Compression and Bandwidth Management

By default, compression is applied between SIP trunks and non-SIP endpoints while bandwidth management is not applied.

Time Zone

Time-zone does not allow for out-of-zone set location.

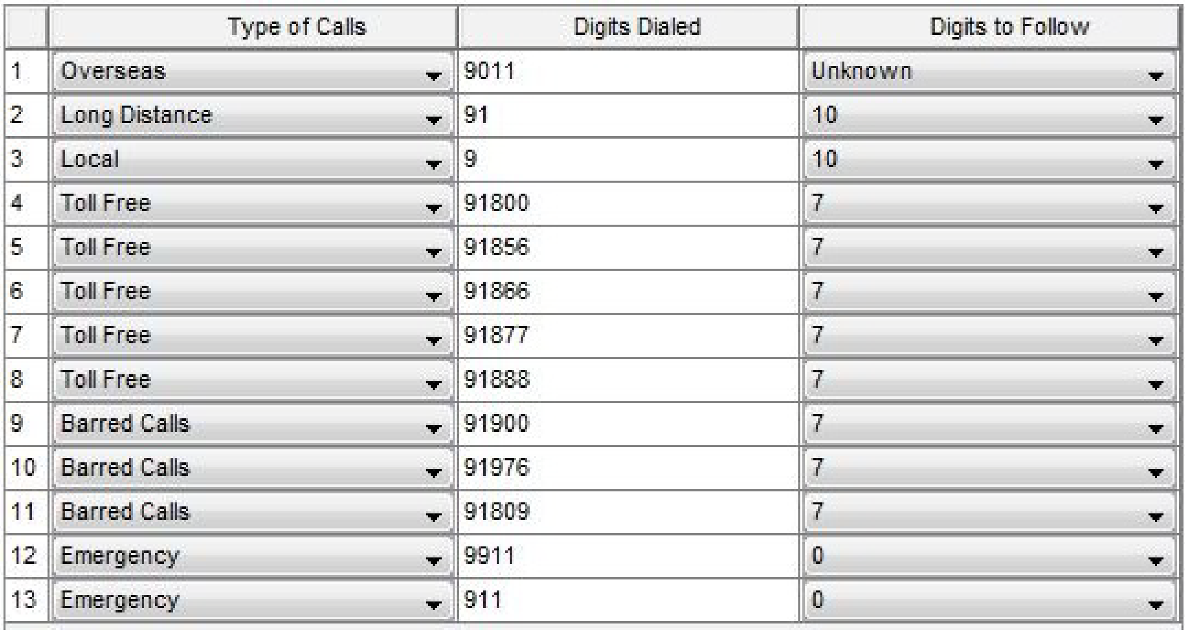
Country Specific Defaults

The following sections list defaults specific to each country.

North America

Table 18: Local Attributes for North America

Parameter	Description	Country Setting
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	Format consists of an area code, followed by a city code and a local number. For example: 613 592 2122
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	9
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	1
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	011
Emergency Calls	The digits that a user dials to place an emergency call	911



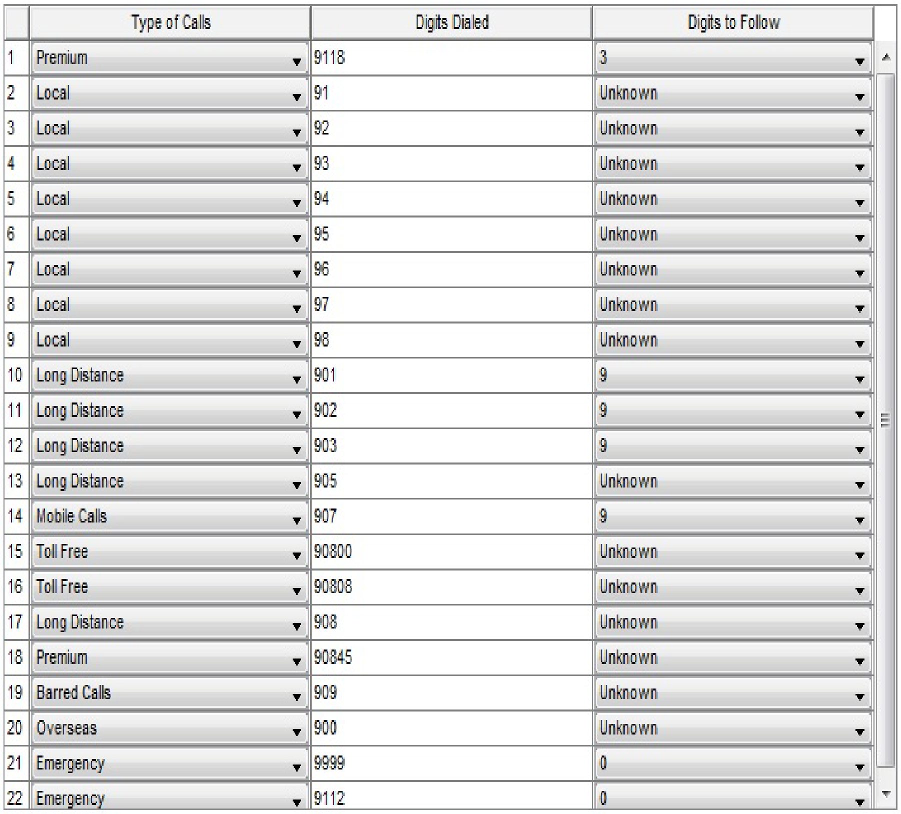
	Type of Calls	Digits Dialed	Digits to Follow
1	Overseas	9011	Unknown
2	Long Distance	91	10
3	Local	9	10
4	Toll Free	91800	7
5	Toll Free	91856	7
6	Toll Free	91866	7
7	Toll Free	91877	7
8	Toll Free	91888	7
9	Barred Calls	91900	7
10	Barred Calls	91976	7
11	Barred Calls	91809	7
12	Emergency	9911	0
13	Emergency	911	0

Figure 56: ARS Rules for North America

United Kingdom

Table 19: Local Attributes for United Kingdom

Parameter	Description	Country Setting
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	Regional or mobile code followed by the number: 01xxx yyyyyy 02xxx yyyyyy 07xxx yyyyyy (mobile) For example: 01291 430000
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	9
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	9 followed by the national code. For example: 901xxx yyyyyy 902xxx yyyyyy
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	9 followed by the country code For example: 9001xxx yyyyyy
Emergency Calls	The digits that a user dials to place an emergency call	999, 112



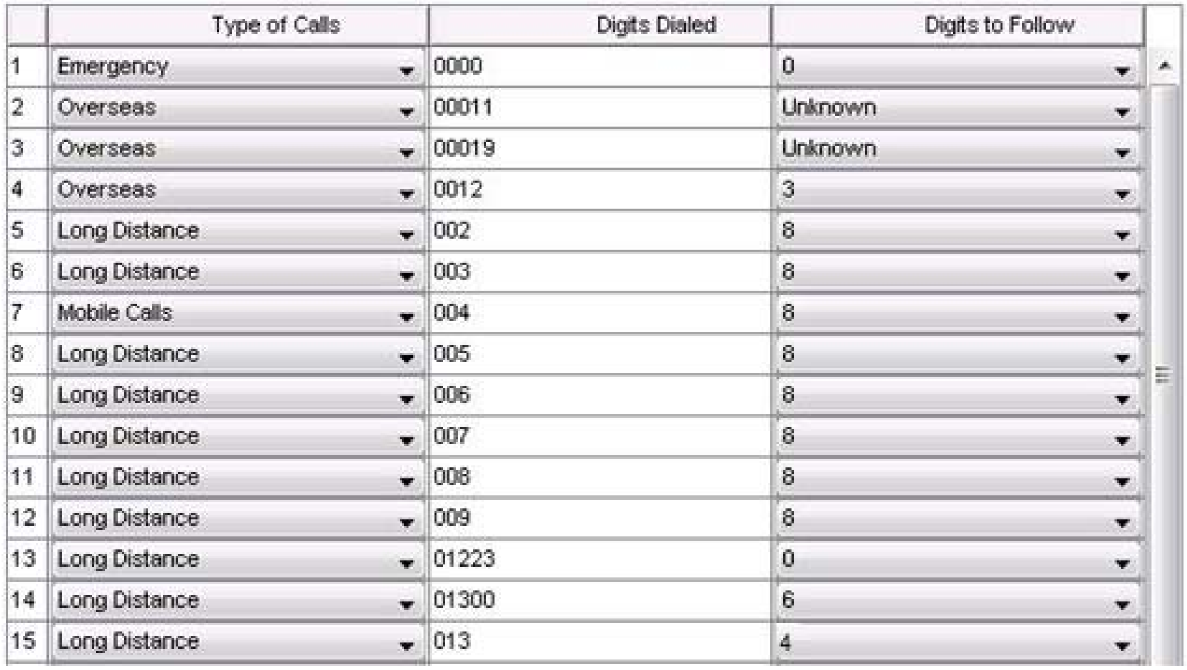
	Type of Calls	Digits Dialed	Digits to Follow
1	Premium	9118	3
2	Local	91	Unknown
3	Local	92	Unknown
4	Local	93	Unknown
5	Local	94	Unknown
6	Local	95	Unknown
7	Local	96	Unknown
8	Local	97	Unknown
9	Local	98	Unknown
10	Long Distance	901	9
11	Long Distance	902	9
12	Long Distance	903	9
13	Long Distance	905	Unknown
14	Mobile Calls	907	9
15	Toll Free	90800	Unknown
16	Toll Free	90808	Unknown
17	Long Distance	908	Unknown
18	Premium	90845	Unknown
19	Barred Calls	909	Unknown
20	Overseas	900	Unknown
21	Emergency	9999	0
22	Emergency	9112	0

Figure 57: ARS Rules for United Kingdom

Australia

Table 20: Local Attributes for Australia

Parameter	Description	Country Setting
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	End-user numbers are 10 digits long, conventionally written in the form **(0x) xxxx xxxx** for geographic and **04xx xxx xxx** for mobile numbers. If the number is written where it may be viewed by an international audience (for example, on an email signature or website) then the number is often written as **+61 x xxxx xxxx** or **+61 4xx xxx xxx** respectively (the initial **0** is not used for calls from overseas).
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	0
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	0
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	0011
Emergency Numbers	The digits that a user dials to place an emergency call	000, 106



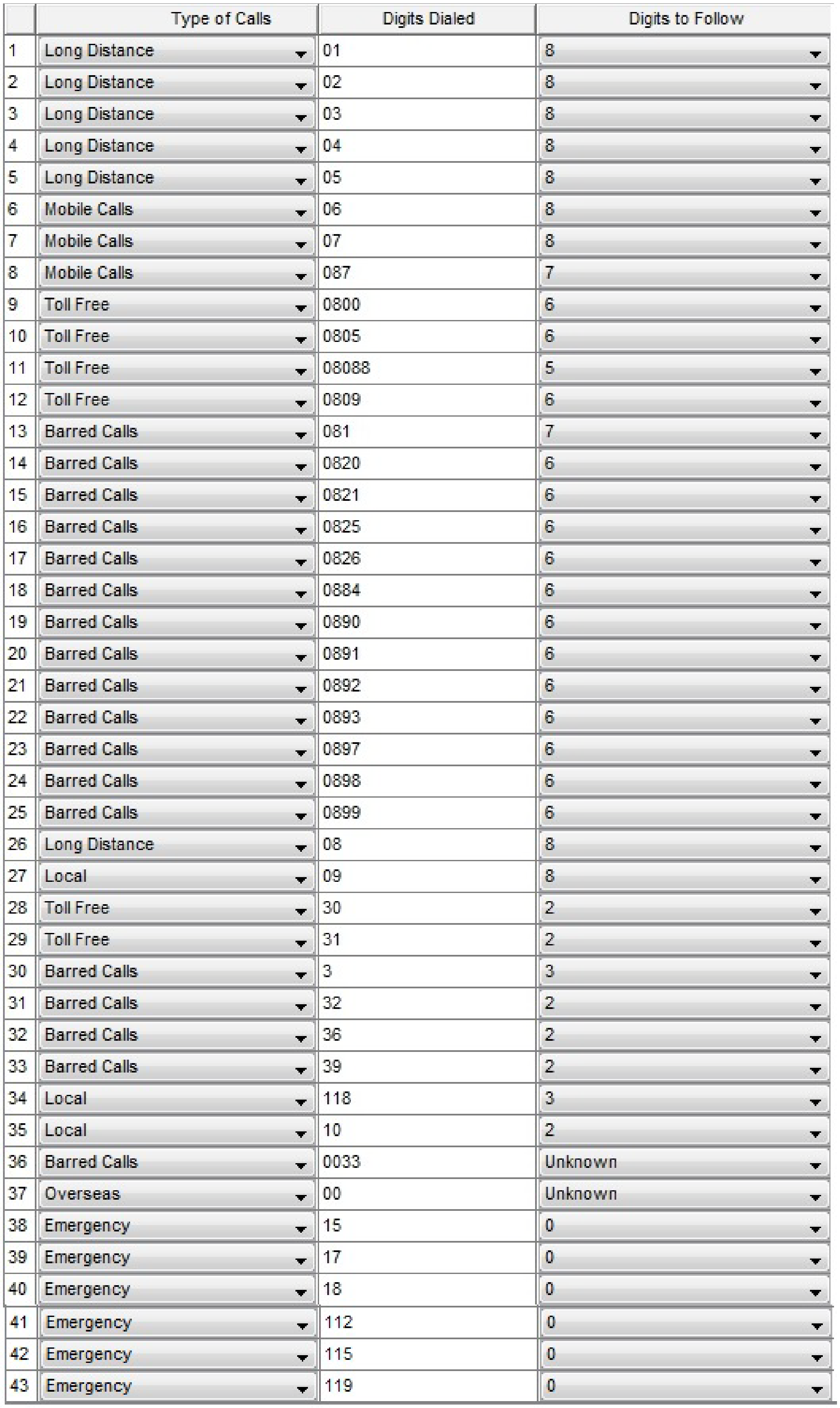
	Type of Calls	Digits Dialed	Digits to Follow
1	Emergency	0000	0
2	Overseas	00011	Unknown
3	Overseas	00019	Unknown
4	Overseas	0012	3
5	Long Distance	002	8
6	Long Distance	003	8
7	Mobile Calls	004	8
8	Long Distance	005	8
9	Long Distance	006	8
10	Long Distance	007	8
11	Long Distance	008	8
12	Long Distance	009	8
13	Long Distance	01223	0
14	Long Distance	01300	6
15	Long Distance	013	4

Figure 58: ARS Rules for Australia

France

Table 21: Local Attributes for France

Parameter	Description	Country Setting
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	01 xx xx xx xx The numbering plan uses a ten-digit closed numbering scheme, where the first two digits denote the area: 01 Ile-de-france 02 Northwest France 03 Northeast France 04 Southeast France 05 Southwest France 06 and 07 Mobile phone services 08 Freephone 09 Non-geographic number
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	None
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	None
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	00
Emergency Numbers	The digits that a user dials to place an emergency call.	15, 17, 18, 112, 115, 119



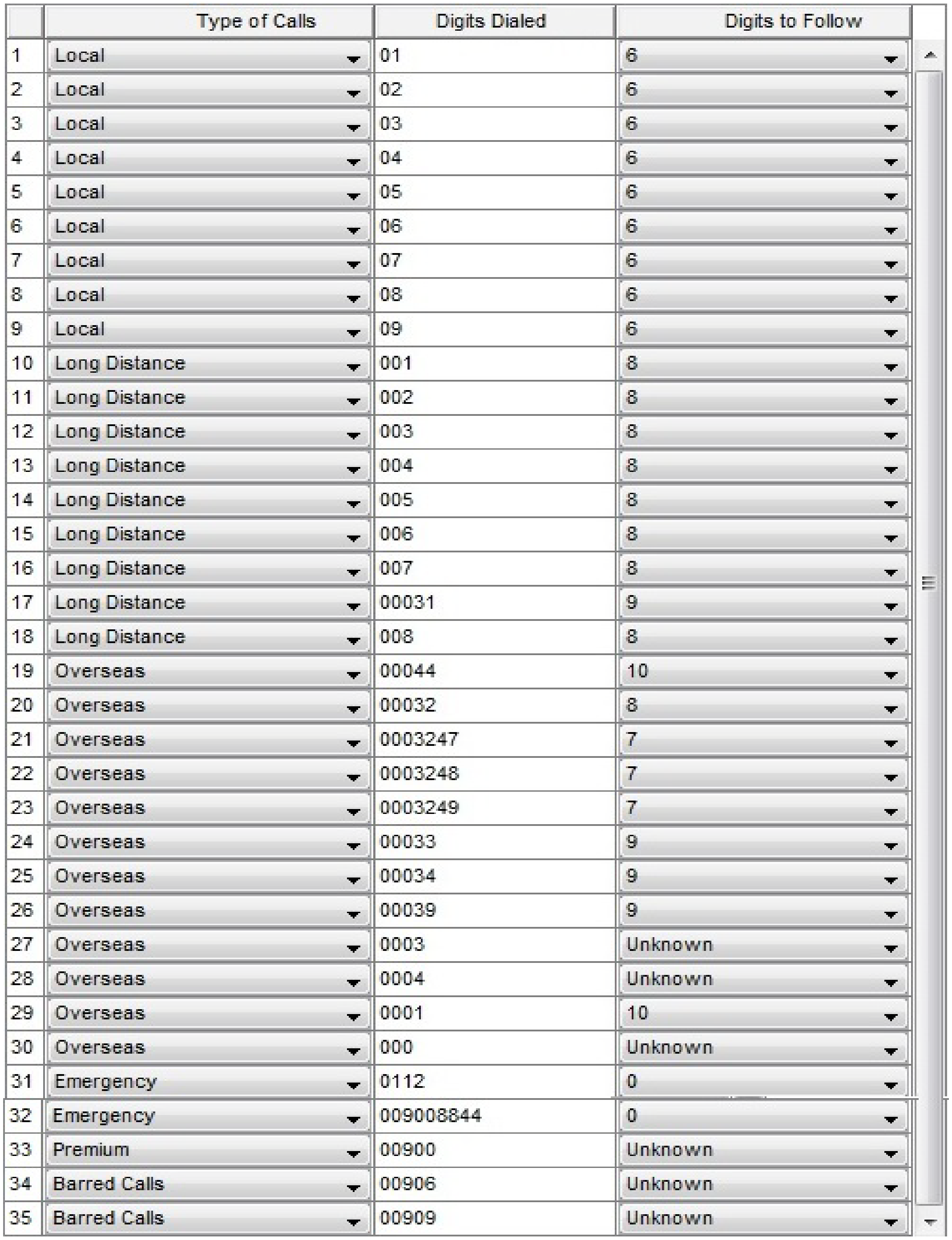
	Type of Calls	Digits Dialed	Digits to Follow
1	Long Distance	01	8
2	Long Distance	02	8
3	Long Distance	03	8
4	Long Distance	04	8
5	Long Distance	05	8
6	Mobile Calls	06	8
7	Mobile Calls	07	8
8	Mobile Calls	087	7
9	Toll Free	0800	6
10	Toll Free	0805	6
11	Toll Free	08088	5
12	Toll Free	0809	6
13	Barred Calls	081	7
14	Barred Calls	0820	6
15	Barred Calls	0821	6
16	Barred Calls	0825	6
17	Barred Calls	0826	6
18	Barred Calls	0884	6
19	Barred Calls	0890	6
20	Barred Calls	0891	6
21	Barred Calls	0892	6
22	Barred Calls	0893	6
23	Barred Calls	0897	6
24	Barred Calls	0898	6
25	Barred Calls	0899	6
26	Long Distance	08	8
27	Local	09	8
28	Toll Free	30	2
29	Toll Free	31	2
30	Barred Calls	3	3
31	Barred Calls	32	2
32	Barred Calls	36	2
33	Barred Calls	39	2
34	Local	118	3
35	Local	10	2
36	Barred Calls	0033	Unknown
37	Overseas	00	Unknown
38	Emergency	15	0
39	Emergency	17	0
40	Emergency	18	0
41	Emergency	112	0
42	Emergency	115	0
43	Emergency	119	0

Figure 59: ARS Rules for France

Netherlands

Table 22: Local Attributes for Netherlands

Parameter	Description	Country Setting
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	Geographical telephone numbers are sequences of 9 digits (0-9) and consist of an area code of two or three digits and a subscriber number of seven or six digits, respectively. When dialed within the country, the number must be prefixed with the trunk access code 0, identifying a destination telephone line in the Dutch telephone network. Non-geographical numbers have no fixed length, but also required the dialing of a trunk access code (0). They are used for mobile telephone networks and other designated service types, such as toll-free dialing, Internet access, voice over IP, restricted audiences, and information resources.
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	0
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	0
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	000 (followed by country code)
Emergency Numbers	The digits that a user dials to place an emergency call	112 is emergency Police emergency is 09008844



	Type of Calls	Digits Dialed	Digits to Follow
1	Local	01	6
2	Local	02	6
3	Local	03	6
4	Local	04	6
5	Local	05	6
6	Local	06	6
7	Local	07	6
8	Local	08	6
9	Local	09	6
10	Long Distance	001	8
11	Long Distance	002	8
12	Long Distance	003	8
13	Long Distance	004	8
14	Long Distance	005	8
15	Long Distance	006	8
16	Long Distance	007	8
17	Long Distance	00031	9
18	Long Distance	008	8
19	Overseas	00044	10
20	Overseas	00032	8
21	Overseas	0003247	7
22	Overseas	0003248	7
23	Overseas	0003249	7
24	Overseas	00033	9
25	Overseas	00034	9
26	Overseas	00039	9
27	Overseas	0003	Unknown
28	Overseas	0004	Unknown
29	Overseas	0001	10
30	Overseas	000	Unknown
31	Emergency	0112	0
32	Emergency	009008844	0
33	Premium	00900	Unknown
34	Barred Calls	00906	Unknown
35	Barred Calls	00909	Unknown

Figure 60: ARS Rules for Netherlands

MAS Single Point of Provisioning Defaults

When you create a new user using single-point provisioning, MAS applies a default COS option to the user based on the services that you apply to that user. This COS option corresponds to a COS option on the MCD system. The following tables list the COS settings that the Initial Configuration Wizard applies to the MCD system and the MAS application services (where applicable).

If you manually configure the MCD system and MAS applications, then you must program these Class of Service Option settings into the MCD system through the System Administration Tool. The corresponding COS option number must also be programmed into the Network Elements screen of the Users and Services application. If you choose to manually program these COSs, it is recommended that you use the default COS numbers.

For simplicity, only the settings that have been changed from their default Class of Service settings are listed. Therefore, to manually create a required COS, select the COS number and then apply the settings specified below. On an existing MCD system, if a COS number (for example COS 11) is already in use, you will need to modify your COS programming to free up the required COS. Note that you can use the **Copy** button in the Class of Service Assignment form to copy existing settings to a different COS number. You can also use the Copy button to copy the default settings from a blank COS to one of the required COS numbers if the COS has been modified.

COS Settings for MAS Users

The configuration wizard automatically creates COS 1, 3, and 4 with the required settings for standard users.

Default Standard User COSs

Option	User COSs	
	Standard User (COS 1)	**VM User with RAC (COS 3)**
ACD Silent Monitor Accept	Yes	Yes
ACD Silent Monitor Allowed	Yes	Yes
ACD Silent Monitor Notification	Yes	Yes
Group Presence Control	No	No
Group Presence Third-Party Control	No	No
SMDR External and Internal	Yes	Yes
Work Timer	20 s	20 s

The wizard creates COS 11,13, and 14 with the required settings for Hot Desk users.

Default Hot Desk User COSs

Option	Hot Desk User COSs (Default)	
	User (COS 11)	**VM User with RAC (COS 13)**
ACD Silent Monitor Accept	Yes	Yes
ACD Silent Monitor Allowed	Yes	Yes
ACD Silent Monitor Notification	Yes	Yes
Group Presence Control	No	No
Group Presence Third-Party Control	No	No
Hot Desk External User Answer Confirmation	No	Yes
Hot Desk External User Permanent Login	Yes	Yes
Hot Desk Login Accept	Yes	Yes
Hot Desk Remote Logout Enabled	Yes	Yes
SMDR External and Internal	Yes	Yes
Work Timer	20 s	20 s

COS for Application Ports

The wizard creates COS 82, 83, 84, and 85 for the NuPoint Unified Messaging application and the Speech Auto Attendant application with the required settings for the ports:

Default NuPoint Unified Messaging Ports COSs

Option	NP Ports COS (Default)	NP RAC Ports COS (Default)	NP MWI Ports COS (Default)	Speech AA Ports COS (Default)
	(COS 82)	(COS 83)	(COS 84)	(COS 85)
Calling Party Name Substitution	No	No	No	Yes
COV/ONS/E&M Voice Mail Port	Yes	Yes	Yes	No
Dialled Night Service	No	No	No	Yes
Display Dialed Digits during Outgoing Calls	No	No	No	Yes
Do Not Disturb Permanent	No	No	Yes	No
HCI/CTI/TAPI Call Control Allowed	Yes	Yes	Yes	Yes
HCI/CTI/TAPI Monitor Allowed	Yes	Yes	Yes	Yes
Public Network Access via DPNSS	Yes	Yes	No	Yes

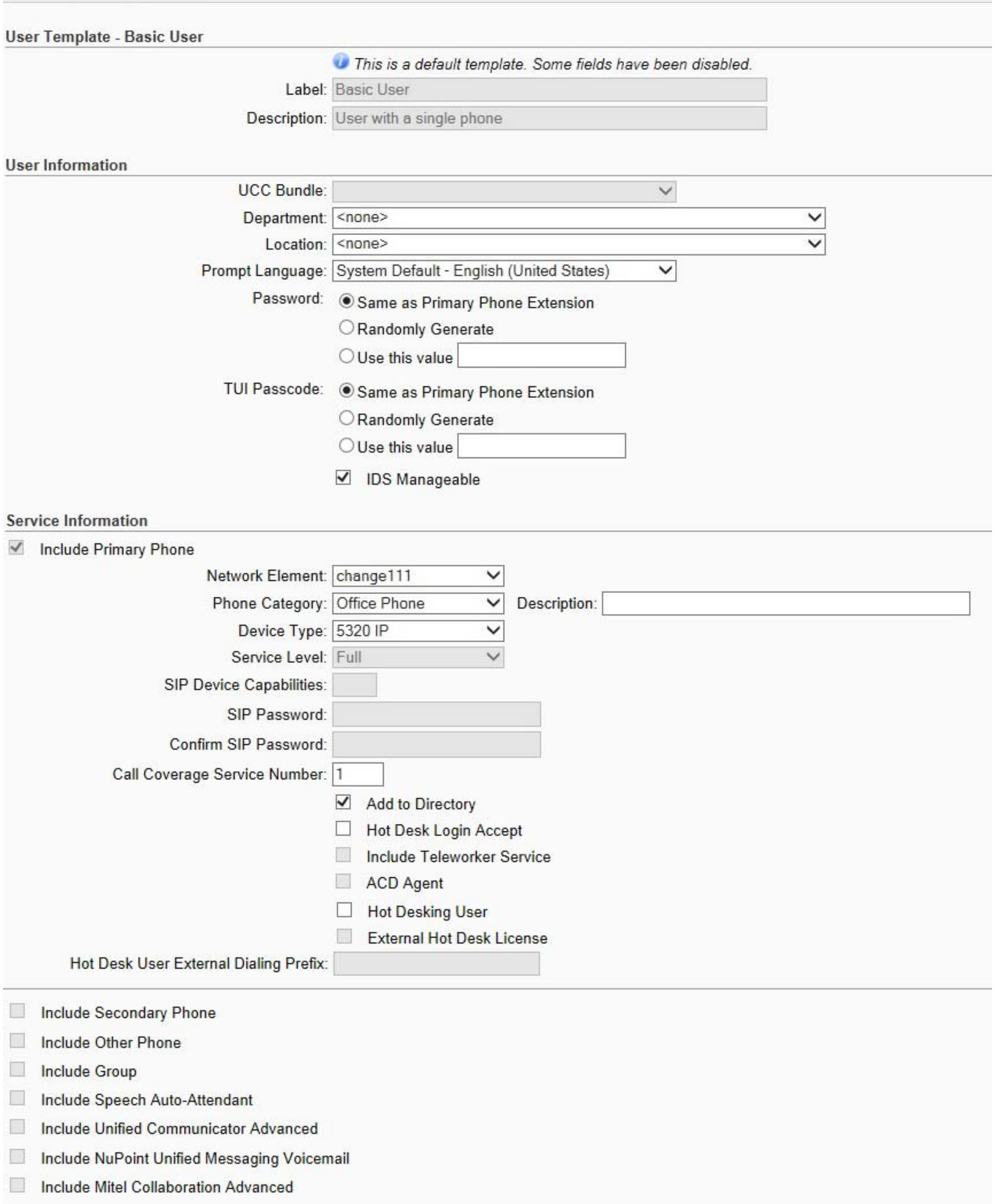
The wizard creates COS 86 with the required settings for the Mitel Collaboration Advanced ports:

Default MCA Ports COS

Option	MCA Ports COS (Default)
	(COS 86)
Suppress Simulated CCM after ISDN Progress	Yes

Basic Role and Default Template

Use the basic user default template "User with a Single Phone" to configure a MCD user with a single full service phone including the basic (free of charge) UCA client. This template is not associated with a UCC licensing bundle, so basic users require "a la carte" MCD user licenses.



User Template - Basic User

This is a default template. Some fields have been disabled.

Label: Basic User

Description: User with a single phone

User Information

UCC Bundle:

Department: <none>

Location: <none>

Prompt Language: System Default - English (United States)

Password: ● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

TUI Passcode: ● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

☑ IDS Manageable

Service Information

☑ Include Primary Phone

Network Element: change111

Phone Category: Office Phone Description:

Device Type: 5320 IP

Service Level: Full

SIP Device Capabilities:

SIP Password:

Confirm SIP Password:

Call Coverage Service Number: 1

☑ Add to Directory
□ Hot Desk Login Accept
□ Include Teleworker Service
□ ACD Agent
□ Hot Desking User
□ External Hot Desk License

Hot Desk User External Dialing Prefix:

□ Include Secondary Phone
□ Include Other Phone
□ Include Group
□ Include Speech Auto-Attendant
□ Include Unified Communicator Advanced
□ Include NuPoint Unified Messaging Voicemail
□ Include Mitel Collaboration Advanced

Figure 61: Basic Default Template

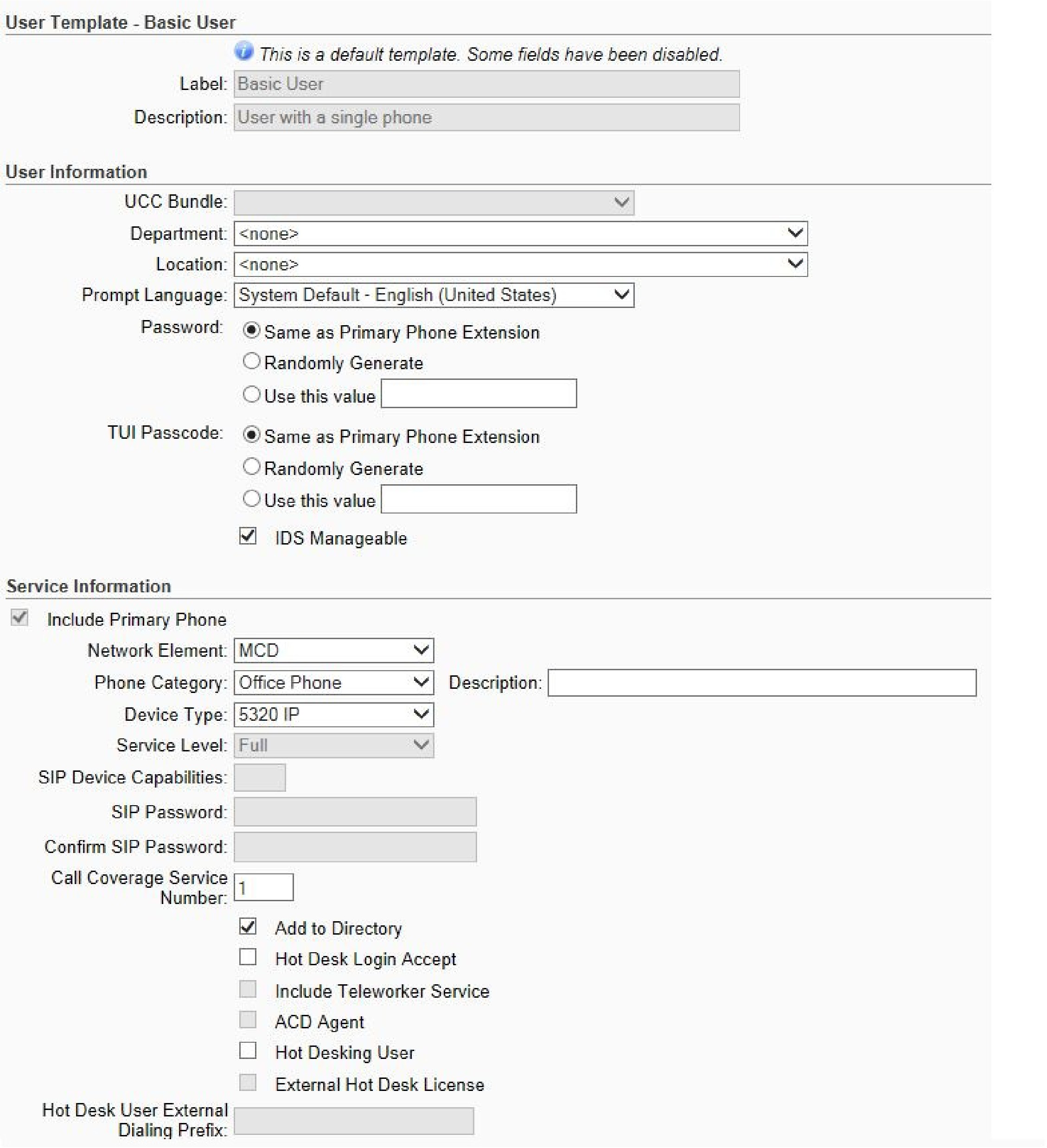
UCC Default Roles and Templates

Default Roles

There are three default UCC business roles. Each role is associated with a default template:

- Default UCC Entry User for Business Role
- Default UCC Standard User for Business Role
- Default UCC Premium User for Business Role

Entry User for Business Template



User Template - Basic User

This is a default template. Some fields have been disabled.

Label: Basic User

Description: User with a single phone

User Information

UCC Bundle:

Department: <none>

Location: <none>

Prompt Language: System Default - English (United States)

Password: ● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

TUI Passcode: ● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

☑ IDS Manageable

Service Information

☑ Include Primary Phone

Network Element: MCD

Phone Category: Office Phone Description:

Device Type: 5320 IP

Service Level: Full

SIP Device Capabilities:

SIP Password:

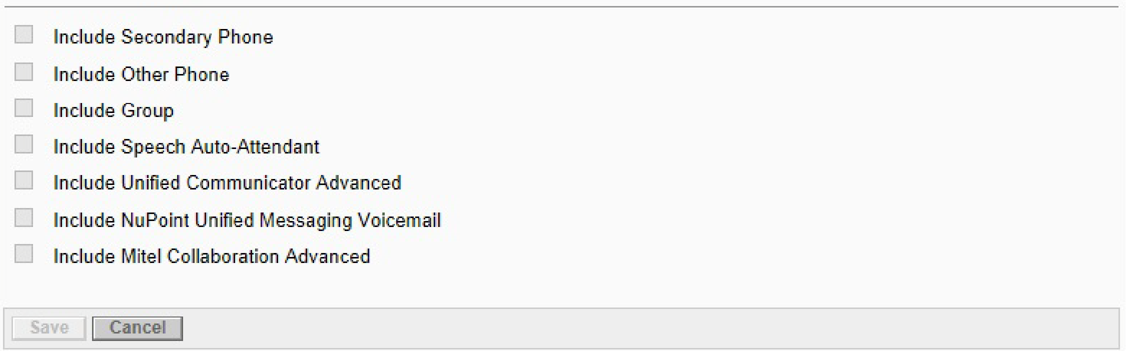
Confirm SIP Password:

Call Coverage Service Number: 1

☑ Add to Directory
□ Hot Desk Login Accept
□ Include Teleworker Service
□ ACD Agent
□ Hot Desking User
□ External Hot Desk License

Hot Desk User External Dialing Prefix:

Figure 62: Entry User for Business Template (Page 1 of 2)



□ Include Secondary Phone

□ Include Other Phone

□ Include Group

□ Include Speech Auto-Attendant

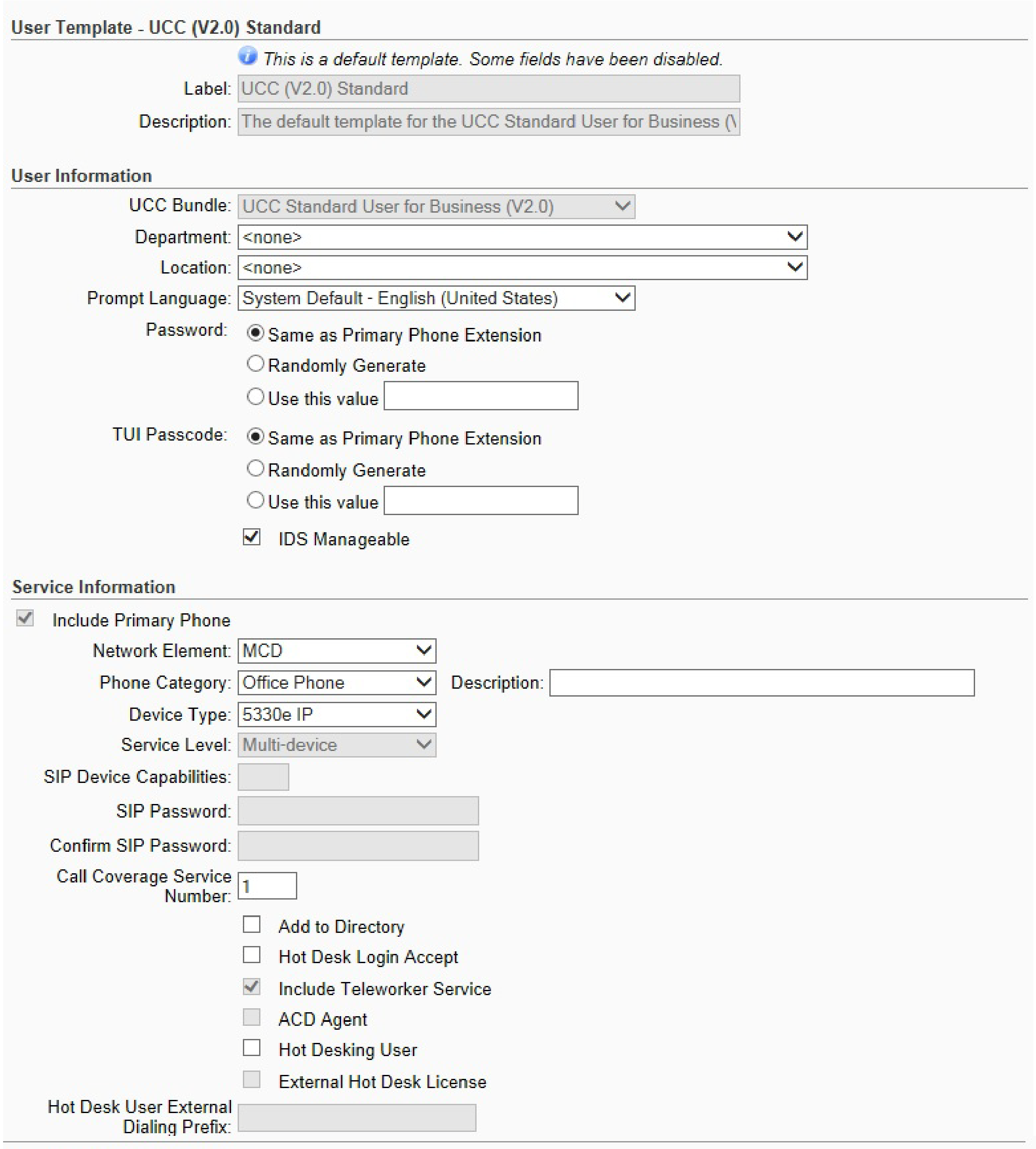
□ Include Unified Communicator Advanced

□ Include NuPoint Unified Messaging Voicemail

□ Include Mitel Collaboration Advanced

Figure 63: Entry User for Business Template (Page 2 of 2)

Standard Level for Business Template



User Template - UCC (V2.0) Standard

This is a default template. Some fields have been disabled.

Label: UCC (V2.0) Standard

Description: The default template for the UCC Standard User for Business (\

User Information

UCC Bundle: UCC Standard User for Business (V2.0)

Department: <none>

Location: <none>

Prompt Language: System Default - English (United States)

Password:
● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

TUI Passcode:
● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

☑ IDS Manageable

Service Information

☑ Include Primary Phone

Network Element: MCD

Phone Category: Office Phone

Description:

Device Type: 5330e IP

Service Level: Multi-device

SIP Device Capabilities:

SIP Password:

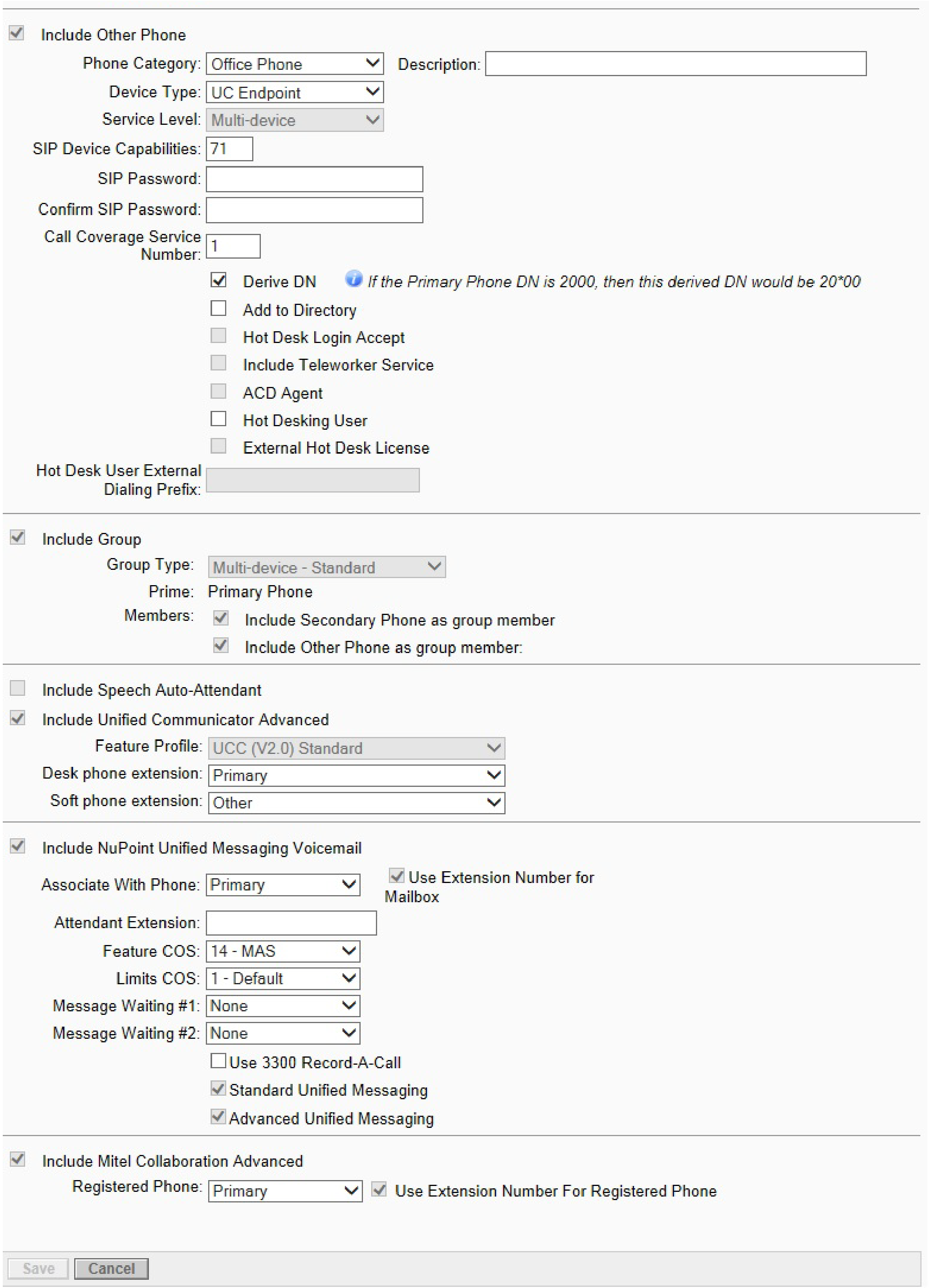
Confirm SIP Password:

Call Coverage Service Number: 1

☐ Add to Directory
☐ Hot Desk Login Accept
☑ Include Teleworker Service
☐ ACD Agent
☐ Hot Desking User
☐ External Hot Desk License

Hot Desk User External Dialing Prefix:

Figure 64: Standard User for Business Template (Page 1 of 2)



☑ Include Other Phone

Phone Category: Office Phone Description:

Device Type: UC Endpoint

Service Level: Multi-device

SIP Device Capabilities: 71

SIP Password:

Confirm SIP Password:

Call Coverage Service Number: 1

☑ Derive DN *If the Primary Phone DN is 2000, then this derived DN would be 20*00*

□ Add to Directory

□ Hot Desk Login Accept

□ Include Teleworker Service

□ ACD Agent

□ Hot Desking User

□ External Hot Desk License

Hot Desk User External Dialing Prefix:

☑ Include Group

Group Type: Multi-device - Standard

Prime: Primary Phone

Members: ☑ Include Secondary Phone as group member

☑ Include Other Phone as group member:

□ Include Speech Auto-Attendant

☑ Include Unified Communicator Advanced

Feature Profile: UCC (V2.0) Standard

Desk phone extension: Primary

Soft phone extension: Other

☑ Include NuPoint Unified Messaging Voicemail

Associate With Phone: Primary ☑ Use Extension Number for Mailbox

Attendant Extension:

Feature COS: 14 - MAS

Limits COS: 1 - Default

Message Waiting #1: None

Message Waiting #2: None

□ Use 3300 Record-A-Call

☑ Standard Unified Messaging

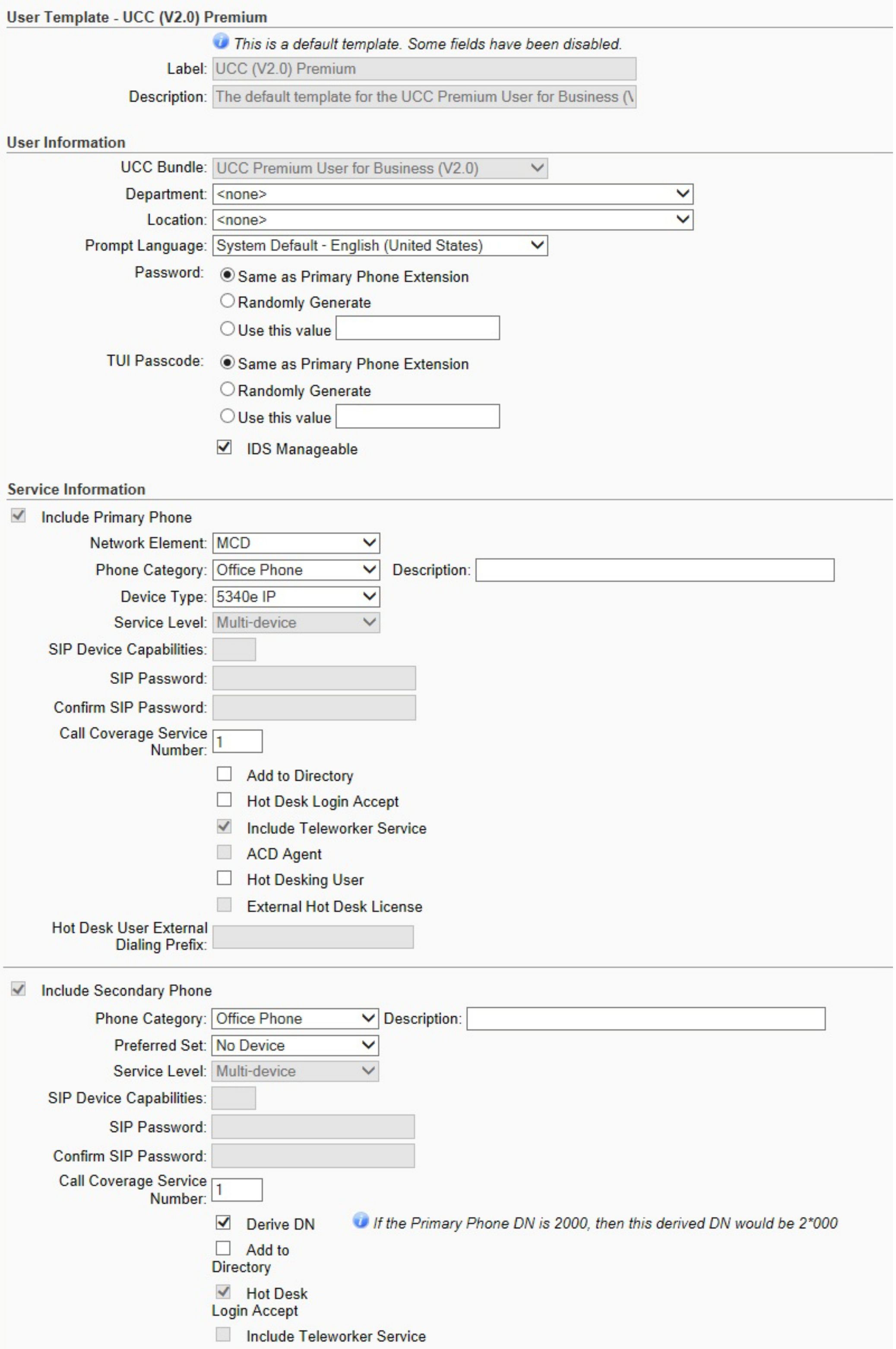
☑ Advanced Unified Messaging

☑ Include Mitel Collaboration Advanced

Registered Phone: Primary ☑ Use Extension Number For Registered Phone

Figure 65: Standard User for Business Template (Page 2 of 2)

Premium User for Business Template



User Template - UCC (V2.0) Premium

This is a default template. Some fields have been disabled.

Label: UCC (V2.0) Premium

Description: The default template for the UCC Premium User for Business (\

User Information

UCC Bundle: UCC Premium User for Business (V2.0)

Department: <none>

Location: <none>

Prompt Language: System Default - English (United States)

Password: ● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

TUI Passcode: ● Same as Primary Phone Extension
○ Randomly Generate
○ Use this value

☑ IDS Manageable

Service Information

☑ Include Primary Phone

Network Element: MCD

Phone Category: Office Phone Description:

Device Type: 5340e IP

Service Level: Multi-device

SIP Device Capabilities:

SIP Password:

Confirm SIP Password:

Call Coverage Service Number: 1

☐ Add to Directory
☐ Hot Desk Login Accept
☑ Include Teleworker Service
☐ ACD Agent
☐ Hot Desking User
☐ External Hot Desk License

Hot Desk User External Dialing Prefix:

☑ Include Secondary Phone

Phone Category: Office Phone Description:

Preferred Set: No Device

Service Level: Multi-device

SIP Device Capabilities:

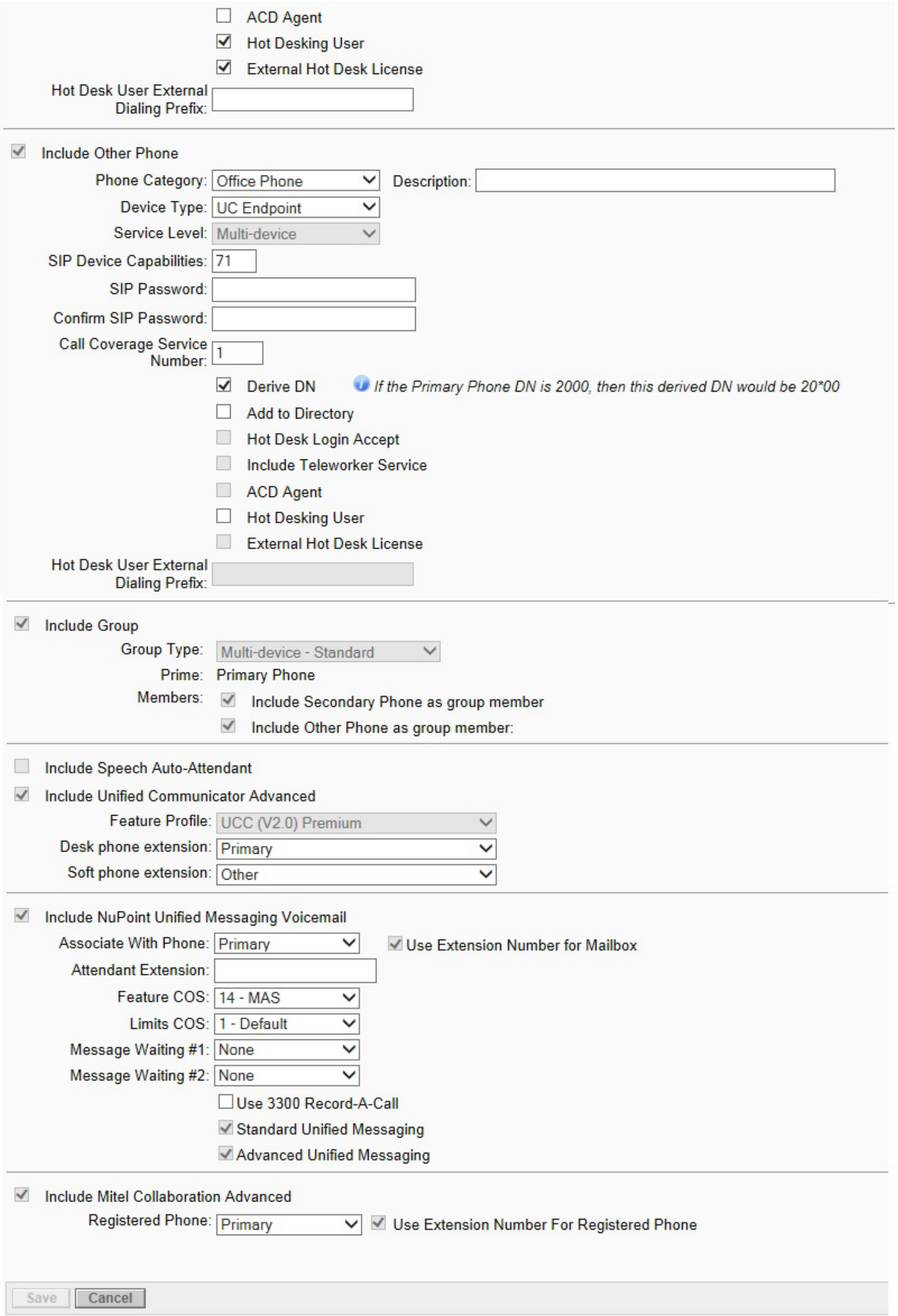
SIP Password:

Confirm SIP Password:

Call Coverage Service Number: 1

☑ Derive DN *If the Primary Phone DN is 2000, then this derived DN would be 2*000*
☐ Add to Directory
☑ Hot Desk Login Accept
☐ Include Teleworker Service

Figure 66: Premium User for Business Template (Page 1 of 2)



☐ ACD Agent
☑ Hot Desking User
☑ External Hot Desk License
Hot Desk User External Dialing Prefix:

☑ Include Other Phone
Phone Category: Office Phone — Description:
Device Type: UC Endpoint
Service Level: Multi-device
SIP Device Capabilities: 71
SIP Password:
Confirm SIP Password:
Call Coverage Service Number: 1
☑ Derive DN — *If the Primary Phone DN is 2000, then this derived DN would be 20*00*
☐ Add to Directory
☐ Hot Desk Login Accept
☐ Include Teleworker Service
☐ ACD Agent
☐ Hot Desking User
☐ External Hot Desk License
Hot Desk User External Dialing Prefix:

☑ Include Group
Group Type: Multi-device - Standard
Prime: Primary Phone
Members: ☑ Include Secondary Phone as group member
☑ Include Other Phone as group member:

☐ Include Speech Auto-Attendant
☑ Include Unified Communicator Advanced
Feature Profile: UCC (V2.0) Premium
Desk phone extension: Primary
Soft phone extension: Other

☑ Include NuPoint Unified Messaging Voicemail
Associate With Phone: Primary — ☑ Use Extension Number for Mailbox
Attendant Extension:
Feature COS: 14 - MAS
Limits COS: 1 - Default
Message Waiting #1: None
Message Waiting #2: None
☐ Use 3300 Record-A-Call
☑ Standard Unified Messaging
☑ Advanced Unified Messaging

☑ Include Mitel Collaboration Advanced
Registered Phone: Primary — ☑ Use Extension Number For Registered Phone

Figure 67: Premium User for Business Template (Page 2 of 2)

Appendix B

VMware Support for vUCC

vCenter Management Support for vUCC

The following vSphere features are supported by vCenter Management for vUCC deployments.

vSphere 5.0 or 5.1 Feature	vUCC Support	Comments
Virtual Appliance Management		
vApp Deployment (Import)	Yes	Use the Export function to create a backup of the vUCC deployment. In the event of database corruption, you can then use the Import function to recover the system.
Export OVA	Yes	
Shutdown	Yes	Use Shutdown to perform a graceful shutdown of vUCC.
Power On	Yes	Use the Power On option to start vUCC. On a single server configuration, set the “Virtual Machine Startup and Shutdown” settings to allow virtual appliances to start and stop automatically with the system and minimize downtime.
Power Off	No	Use Shutdown instead of Power off.
Suspend/Resume	No	Do not use. Suspending vUCC will result in a loss of phone service and could cause database corruption.
Reset/Restart	Yes	Use this command to shutdown the guest operating system and application and then restart them.
Cold Migration	Yes	Migration is the process of moving a virtual appliance from one host or storage location to another. With vCenter, you have the following migration options. • Moving a powered-off virtual appliance to a new host. Optionally, the user can relocate configuration and disk files to a new storage locations. Cold migration can be used to migrate virtual appliances from one datacenter to another. • Moving a suspended virtual appliance to a new host. Optionally, the user can relocate configuration and disk files to a new storage locations. The user can also migrate suspended virtual appliances from one datacenter to another.
Migration while suspended	No	
Snapshot (Powered Off)	No	Snapshots are not supported for vUCC.
Snapshot (Powered On)	No	
Snapshot (Suspended)	No	
Cloning	No	A clone is a copy of an existing virtual appliance. When the cloning operation is complete, the clone is separate virtual appliance. Cloning is not supported for configured vUCC OVA files.
		Page 1 of 4

vSphere 5.0 or 5.1 Feature	vUCC Support	Comments
Health Monitoring	Yes	The vSphere Client provides extensive monitoring and reporting tools to help you diagnose potential resource allocation problems. These tools interact with the hypervisor (ESX/ESXi).
Performance Reports	Yes	
Virtual Machine Advanced Management	vUCC 5.0 has not been qualified against vSphere 5.0/5.1 vCenter Advanced Management features such as SRM	
vMotion	Yes	vMotion provides live migration of virtual appliances from one physical host to another with zero downtime. While a vMotion migration is in progress, vUCC users may experience voice quality degradation. See also “vMotion Support” on page 164.
Storage vMotion	Yes	This feature allows you to move the virtual disks or configuration file of a powered-on virtual appliance to a new datastore. Migration with Storage vMotion allows the user to move a virtual appliance’s storage without any interruption in the availability of the virtual appliance.
High Availability	Yes	High Availability (HA) provides easy-to-use, cost effective high availability for all applications running in virtual appliances. In the event of server failure, affected virtual appliances are automatically restarted on other host appliances in the cluster that have spare capacity. HA minimizes downtime and IT service disruption while eliminating the need for dedicated standby hardware and installation of additional software. VMware HA provides uniform high availability across the entire virtualized IT environment without the cost and complexity of failover solutions tied to either operating systems or specific applications. Note that vUCC requires a fair amount of CPU and memory reservation and it will not restart on a server unless the appropriate resources are available.
Fault Tolerance	No	Fault Tolerance cannot be used with vUCC.
Distributed Resource Scheduler (DRS)	Yes	Distributed Resource Scheduler is a VMware service that supports resource management within clusters. Distributed Resource Scheduler works with vMotion to provide automated resource optimization and virtual appliance placement and migration, to help align available resources with pre-defined business priorities while maximizing hardware utilization.
		Page 2 of 4

vSphere 5.0 or 5.1 Feature	vUCC Support	Comments
Distributed Power Management (DPM)	Yes	VMware Distributed Power Management (DPM) continuously optimizes power consumption in the datacenter. When virtual appliances in a DRS cluster need fewer resources, such as during nights and weekends, DPM consolidates workloads onto fewer servers and powers off the rest to reduce power consumption. When virtual appliance resource requirements increase (such as when users log into applications in to morning), DPM brings powered-down hosts back online to ensure service levels are met.
Update Manager and O/S Patching	No	Update Manager compares the operating systems and applications running in the Virtual Infrastructure deployment against a set of standard updates and patches. Updates specified by the user can be applied to operating systems and applications on scanned ESX Server hosts and virtual appliances. This functionality is not supported for vUCC.
VMware Consolidated Backup	No	VMware Consolidated Backup cannot be used with vUCC.
VMware vStorage APIs	Yes	The "vStorage APIs for Data Protection" feature enables backup software to protect system, application, and user data in their virtual appliances in a simple and scalable way. These APIs enable backup software to: • Perform full, differential, and incremental image backup and restore of virtual appliances. • Perform file-level backup of virtual appliances using supported Windows and Linux operating systems.
Data Recovery	Yes	Data recovery is a backup and recover product for VMware vSphere that provides quick, easy, and complete data protection for virtual appliances. Note that vUCC only supports the VMware Data Recovery operation during off-hours or during a maintenance window where disk I/O activities are limited. Degradation in voice quality occurs during the VMware Data Recovery operation.
Hot Add	No	VMware Hot Add allows CPU and memory to be added to virtual appliances when needed without disruption or downtime.
		Page 3 of 4

vSphere 5.0 or 5.1 Feature	vUCC Support	Comments
VMsafe	No	VMware VMsafe™ is a security technology for virtualized environments that can help to protect your virtual infrastructure in ways previously not possible with physical appliances. VMsafe provides a unique capability for virtualized environments through an application program interface (API)-sharing program that enables select partners to develop security products for VMware environments. The result is an open approach to security that provides customers with the most secure platform on which they can virtualize their business-critical applications.
Site Recovery Manager	No	VMware vCenter Site Recovery Manager provides business continuity and disaster recovery protection for virtual environments. Protection can extend from individual replicated datastores to an entire virtual site.
		Page 4 of 4

VMware View Support

The following MAS Release 5.0 or later application desktop user interfaces are supported in a VMware View virtual desktop environment with the specified conditions and limitations:

- **My Unified Communications Portal**
  - Web portal is fully supported in VMware View Release 4.6 or later.
- **Unified Communicator Advanced Desktop Client**
  - Desktop client in deskphone mode is fully supported in VMware View Release 4.6 or later.
  - Desktop client in softphone mode is supported in VMware View Release 5.0 or later. The softphone media connection must be redirected from the central server to the USB port on the user’s thin client. A Personal Computer-over-Internet Protocol (PCoIP) display protocol connection is required to support this connection. Softphone mode is not supported in VMware View Local Mode. Remote Desktop Protocol (RDP) is not supported.
  - Video is not currently supported.
  - Assign users with dedicated VMware View desktops. Floating desktops are not recommended because users must re-enter their credentials (for example, UCA server address, user identification, and password) every time they want to open a UCA desktop client.
- **Unified Communicator Advanced Web Client**
  - Web client is fully supported in VMware View Release 4.6 or later.
- **Mitel Collaboration Advanced Client**
  - Collaboration client for desktop collaboration and application sharing is fully supported in VMware View Release 4.6 or later.

  - Video collaboration and recorded conference playback are currently not supported.
- **Contact Center Solutions Agent and Supervisor Desktops**
  - CSM Release 6.0 or later required.
  - Agent and Supervisor Desktops fully supported on VMware View Release 4.6 or later
  - Softphone is currently not supported.

Note: Refer to the VMware View Support Solutions Guide on the Mitel Customer Documentation web site for more information.

vMotion Support

- Mitel tested vMotion in a configuration with a single SAN storage within a single data center.
- For vMotion operation beyond the Mitel tested configuration, please contact Mitel Profession Services to assess whether the non-Mitel test configuration can be supported.
- Refer to the Virtual Appliance Deployment Solutions Guide at http://edocs.mitel.com/TechDocs/Solutions-Guides/BP-Virtualization.pdf for more information.

Global Headquarters	U.S.	EMEA	CALA	Asia Pacific
Tel: +1(613) 592-2122	Tel: +1(480) 961-9000	Tel: +44(0)1291-430000	Tel: +1(613) 592-2122	Tel: +61(0) 2 9023 9500
Fax: +1(613) 592-4784	Fax: +1(480) 961-1370	Fax: +44(0)1291-430400	Fax: +1(613) 592-7825	Fax: +61(0) 2 9023 9501

www.mitel.com

For more information on our worldwide office locations, visit our website at www.mitel.com/offices

THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Mitel to be accurate as of the date of its publication, is subject to change without notice. Mitel assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

M MITEL (design) is a registered trademark of Mitel Networks Corporation. All other products and services are the registered trademarks of their respective holders.

© Copyright 2010, Mitel Networks Corporation. All Rights Reserved.