MiCollab

Client Engineering Guidelines

Release 9.7

March 2023

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

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

Contents

MiCollab Client Overview $\qquad$ 1

This chapter contains the following sections:

- Prerequisites
- About the MiCollab Client documentation set
- What's New in this Release

MiCollab Client is a product that converges the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration to simplify and enhance communications.

These guidelines are provided to assist System Administrators in deploying MiCollab Client. The MiCollab Client product consists of MiCollab Client Service and MiCollab Clients.

The MiCollab Client Service runs on the Mitel Standard Linux (MSL) Operating System, which can be installed on different hardware platforms.

The MiCollab Client interfaces consist of the following:

- MiCollab for PC Client
- MiCollab MAC Desktop Client
- MiCollab for Mobile Client

  - Android
  - iPhone
- MiCollab Web Client
- Legacy MiVoice for Skype for Business Plugin
- MiCollab for Microsoft Client

> **ⓘ Note**:
>
> The MiCollab for Mobile Softphone is designed for use on mobile phones. Although it can be installed on tablet devices, the user interface is currently not designed for use on tablets. These devices will be supported in an upcoming release.

> 🛈 **Note**:
>
> If you are licensed to use the Presence on Mitel Sets feature and your desk phone is a 5320, 5330, 5340, or 5360 IP phone, you can display MiCollab Client or IM client presence information on your phone for corporate or personal contacts when you assign the contact to a Private Speed Call or Speed Call button.

> 🛈 **Note**:
>
> InAttend Users can view presence information for contacts associated with MiCollab Client. This feature is limited to users on MiVoice MX-ONE and MiVoice 5000 communication platforms only. Telephony Presence is not supported.

This document describes the MiCollab Client Server configuration requirements in order to assist in sales and support of this product. This information is intended for Training, Sales, and Product support staff and complements other sales material and product documentation.

1.1   Prerequisites

As the scope of these Engineering Guidelines is to cover the MiCollab Client Service application which runs on the Mitel Standard Linux Server (MSL), the reader should first refer to the *MSL Installation and Administration Guide* and the *MSL Qualified Hardware List* available at Mitel Document Center.

When configuring and deploying MiCollab Client on a server co-resident with MiCollab (formerly MAS), the reader should refer to the *MiCollab Installation and Maintenance Guide and the MiCollab Engineering Guidelines*, available at Mitel Document Center.

Table 1: Compatibility Table

Product	Version supported
Call Control Servers	
MiVoice Business	9.0SP3 or higher

Product	Version supported
MiVoice 5000	7.1SP2 or higher
MiVoice Office 400	6.1HF4
MiVoice Office 250	6.3SP5
MiVoice MX-ONE	6.3SP6 or higher
Browsers	
Apple Safari	13.1 or higher
Internet Explorer	11
Google Chrome[1]	90 or higher
Microsoft Edge	90 or higher
Mozilla Firefox	88 or higher
Operating Systems	
MAC OS X	10, 11, and 12
Windows	10 and 11
Windows Server 2012 Terminal Services	6.1

---

[1] MiCollab Web Client is supported on Chrome browser on Chromebook. It is only supported on Chrome OS versions that are still maintained by Google

Product	Version supported
Windows Terminal Services	Windows Server 2022 Remote Desktop Services
Microsoft .Net Framework	4.0, 4.5
Virtualization Software	
VMware vSphere	Refer to the *Virtual Solutions Deployment Guide*
Other	
Instant Messenger (optional)	Legacy MiVoice Skype for Business Plugin, Lync 2010, 2013
PIM (optional)	Act! 2008 & 2011 **Legacy MiCollab Desktop Client:** Outlook 2007, 2010 (32-bit & 64), 2013 (32-bit & 64), 2016 (32 and 64 bit) Google Calendar and contact integration
Calendar Integration	Calendar integration is supported for Google Calendar, Outlook, Lotus Notes, Office 365 or Exchange calendar.
Smart Tags	Microsoft Office 2007, 2010, 2013
MiCollab for Mobile & Devices	Google™ Android™ 8 or later iPhone iOS 13, 14, and 15
MiCollab UC-Client & Devices	Google™ Android™ 5.0 or later on Dalvik VM iPhone / iPad iOS 6.0, 7, 7.1, 8.0, 8.1, 8.2, 8.3, 9.1 or later

Product	Version supported
Federation[2]	Skype for Business, Lync 2010, and 2013 Lotus Notes Sametime 8.5, 9.0
Office 365	2019
Server-side Calendar Exchange Integration	Microsoft Exchange 2013 and 2013 SP1, 2016 and 2019
Thin Clients	• **Legacy MiCollab Desktop Client** [3] Citrix XenApp and XenDesktop 7.13, 7.14, 7.18, or 7.22 VMware View tm – 5.1, 6.2, or 7.4 Remote Desktop Services (RDS)(desktop and application mode) - Windows Server 2022

---

[2] Federation is supported only on Legacy MiCollab Desktop Clients. It is not supported for MiCollab deployments in MiCloud Flex on GCP environment.

[3] Citrix XenApp and XenDesktop 7.13, 7.14, 7.18, or 7.22 is required for the SIP softphone.

Product	Version supported
	• **MiCollab for PC Client / MiCollab Web Client[4] / MiCollab for Microsoft Client** Citrix XenApp and XenDesktop Citrix version 7.13, 7.14, 7.18, and 7.22 VMware View (desktop and application mode) 7.11 and 8 Remote Desktop Services (RDS) (desktop and application mode) – Windows Server 2022 • **Legacy MiVoice for Skype for Business Plugin** Citrix version 7.13, 7.14, or 7.18
Legacy MiVoice for Skype for Business Plugin Integration	Skype for Business 2016 and 2015, Lync versions 2010 and 2013
Virtualization	vSphere/vCloud 5.5, 6.0, 6.5, 6.7Hyper-V 2016

---

[4] Video functionality is not supported on MiCollab for PC Client and MiCollab Web Client on virtual environments. MiCollab Audio, Web and Video web sharing is supported on below mentioned virtual environments:

- Citrix XenApp and XenDesktop Client 7.13, 7.14, 7.18, and 7.22
- VMware View (Desktop and App) 7.4 and above

> **ⓘ Note**:
>
> Receiving Calls on MiCollab for Mobile Clients (Android and iPhone): If a MiCollab for Mobile Client softphone user receives an incoming PSTN call while on a PBX call, the PBX call is put on hold without warning.

1.2 About the MiCollab Client documentation set

For easy access to the various Mitel documentation suites, go to Mitel Document Center. A Mitel Online username and password is required to download technical and administrative documentation from the Mitel Document Center Web site. End-user documentation does not require a username and password.

The following documentation provides complete information about MiCollab Client and its services:

- The MiCollab Client Engineering Guidelines Release 8.1 (this document).
- The MiCollab Client Administrator Guide provides information about system requirements, installation, configuration, maintenance, and troubleshooting for the MiCollab Client Server.
- The MiCollab Client Server Administrator Interface Online Help is bundled with the MiCollab Client Server software blade and provides information about how to provision and manage MiCollab Client from the administrator UI.
- The MiCollab Client Quick Reference Guide provides basic end-user information for the MiCollab Client interfaces.
- The MiCollab Client Desktop Client Online Help is bundled with the MiCollab Client Desktop Client application and provides information about how to use the Desktop Client application on supported Windows platforms.
- MiCollab Vidyo Quick Reference Guide for Administrators provides configuration steps for MiCollab Vidyo integration.
- MiCollab Vidyo Quick Reference Guide for Users provides MiCollab Vidyo Desktop users with quick installation and usage information.
- MiCollab BluStar Features Quick Reference Guide provides an overview of supported features.
- MiCollab Client Features Quick Reference Guide provides an overview of supported features on the MiCollab Web, MiCollab for Mobile Client, and MiCollab Windows Desktop Client.
- MiCollab for Mobile end-user videos (mp4 format):

  - Dynamic status video:
  - MiCollab for Mobile wizard video:
- The MiVoice for Skype for Business Online Help is accessed via the "Help" functionality of the client.

1.3 What's New in this Release

For a list of new functionality, see MiCollab What's New Guide on the Mitel Customer Documentation site.

VMware View   2

MiCollab Client is supported in a virtualized environment.

> **ℹ Note**:
>
> VMware Horizon View is supported only on MiCollab Desktop Client (legacy Desktop Client). For more information about supported versions and features, refer to the *Virtual Deployment Solutions Guide*

The following are the supported VMware View configuration attributes:

- Linked-Clone virtual desktop pools
- Dedicated-Assignment desktop pools
- Floating-Assignment desktop pools
- Full VM desktop
- View Persona Management

> **ℹ Note**:
>
> Floating-Assignment desktop with View Persona Management is strongly recommended. However, there are situations where View Persona Management is not desirable, for example, where the administrator want all data to be wiped clean between sessions (e.g. kiosk, guest access).

With MiCollab Client Direct Media architecture, the real-time sensitive media path flows directly between any two endpoints. It does not need to be processed in the VDI background or traverse the WAN/Internet paths between the endpoints and the backend. This architecture prevents "tromboning" which has scalability issues resulting from a topology requiring extensive VDI backend use.

The basic system consists of:

- MiVoice Business
- A collection of View virtual desktops, managed by the View Connection Server
- VMware View Connection Server - this manages the View sessions

- A collection of physical endpoints (Thin Clients / PC's running View Client), used to present the virtual desktop to the end user
- VMware View Agent software
- VMware View Client software
- MiCollab Client Service
- MiCollab Client – in the View environment, this resides in the virtual desktop
- MiCollab Client plug-in – in the View environment, this contains the media portion of the MiCollab Client and handles the actual media streaming.

The following illustration shows a basic direct media architecture in an enterprise network

Figure 1: Direct Media Architecture
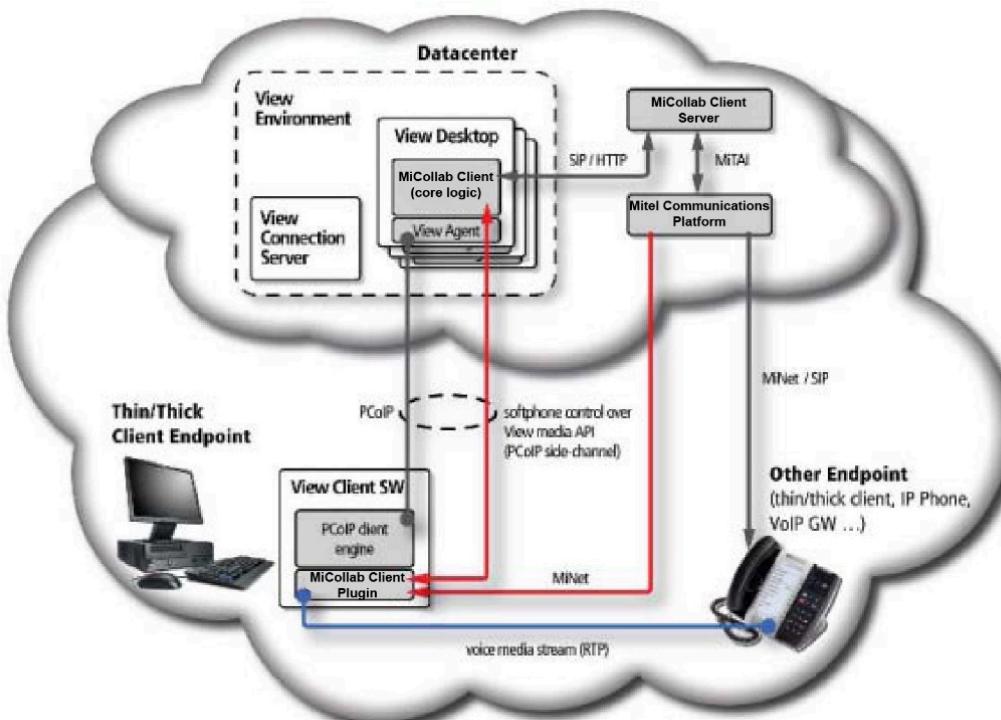
In a more complex scenario, the endpoints involved are not on the same network (behind different NATs). This configuration can handle calls between users in different remote offices each on their own network, between teleworker/home office users and others, between different customers of a hosting provider, or between remote endpoints and VoIP gateways (PSTN access, SIP service provider, and so on. Some endpoints may also reside inside the enterprise network.

Figure 2: Endpoints behind different NATs
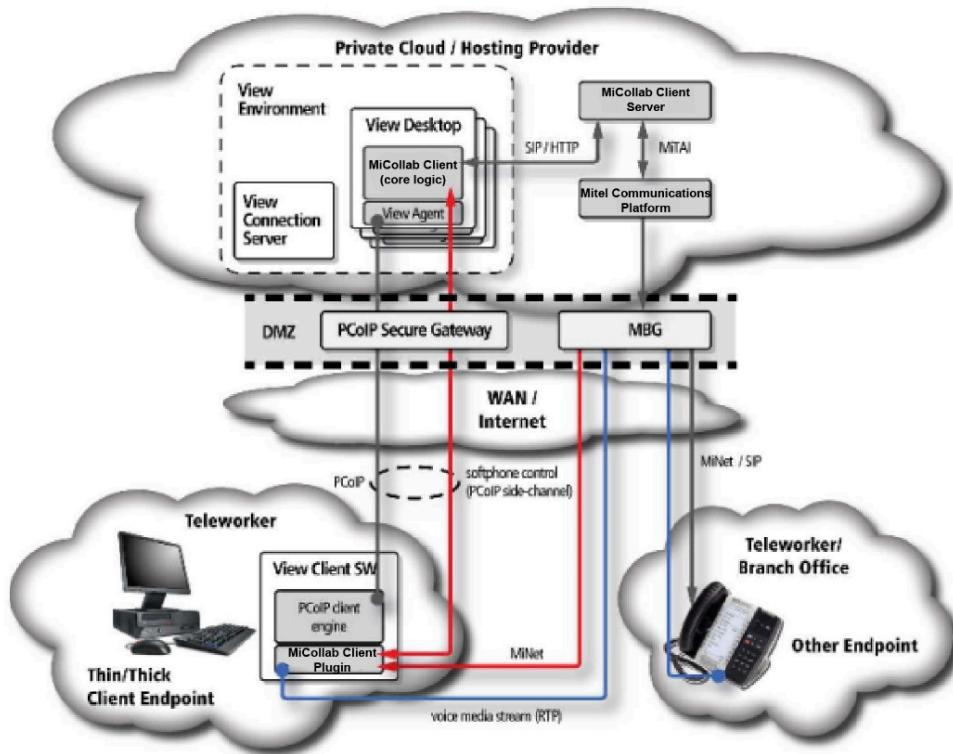
MiCollab Client multi-party conferencing

MiCollab Client multi-party conferencing support for is displayed in the following table.

Table 2: Multi-party conferencing

	MiCollab Desktop Client			MiCollab for Mobile	
Platform	3 PCC (CTI)	MiNET Softphone	SIPSoftphone	3 PCC (CTI)	Softphone
MiVoice Business	8-party	8-party	Yes	8-party	3-party
MiVoice Office 400	8-party	N/A	N/A	3-party	3-party
MiVoice MX-ONE	3-party	N/A	8-party	8-party	8-party (through PBX feature code)

Platform	MiCollab Desktop Client			MiCollab for Mobile	
	3 PCC (CTI)	MiNET Softphone	SIPSoftphone	3 PCC (CTI)	Softphone
MiVoice 5000	3-party	N/A	Yes	3-party	3-party

Deployment configurations 3

This chapter contains the following sections:

- MiCollab Client with MBG configurations
- MiCollab Client without MBG configurations

For deployment configurations where MiCollab Client is installed co-resident with other MiCollab applications, consult the *MiCollab Engineering Guidelines.*

Standalone MiCollab Client can be deployed in the following configurations:

- **MiCollab Client in LAN with MiCollab Border Gateway (MBG) Server in DMZ:** This configuration has MiCollab Client in MSL server located in the Local Area Network (LAN) and MiCollab Border Gateway (MBG) server in the Demilitarized Zone (DMZ). Two variants of this configuration are supported:

  - **MiCollab Client with Web Proxy:** Consists of MiCollab Client in an MSL server on the corporate LAN with Web Proxy in an MBG server in the DMZ. Remote Web browser users connect to the MiCollab Client Service through the Web Proxy. The MiCollab Mobile Client users connect to the MiCollab Client Service through Web Proxy when connecting from the cellular data network. In this configuration, there is no support for MiCollab Client Desktop Client in Teleworker mode.
  - **MiCollab Client with Teleworker and Web Proxy:** Consists of MiCollab Client on an MSL server on the corporate LAN with Teleworker and Web Proxy on an MBG server located in the DMZ. The Teleworker service in the MBG server is used to support the Teleworker users in the DMZ. The Web Proxy service is also installed in this configuration for remote access.
- **MiCollab Client in LAN with MBG Server in Network Edge:** This configuration has MiCollab Client in MSL server located in the Local Area Network (LAN) connected to a MBG server on the network edge (see Figure 2).
- **MiCollab Client in DMZ:** This configuration has MiCollab Client in MSL server located in the DMZ with necessary ports opened in the external firewall. There is no MBG server (no Teleworker or Web Proxy service) in this configuration.

> **ℹ Note**:
>
> When using MBG in the DMZ, any SIP ALG functionality in the external firewall must be turned off for MiCollab Client to work properly.

> ℹ **Note**:
>
> For Corporate BES users, the connection that MiCollab Client uses for real-time notifications uses https and may be denied by the BES. You can disable the real-time notification in the preferences screen.

3.1   MiCollab Client with MBG configurations

To support Teleworkers when MBG is in the network, use one of the following configurations:

- MiCollab Client Service in LAN with MBG and Web Proxy on a second MSL server in the DMZ
- MiCollab Client Service in LAN with MBG and Web Proxy on a second MSL server on the network edge
- MiCollab Client Service and MBG co-resident on a MAS server on the network edge in server-gateway mode (MAS configuration only)

Remote MiCollab Client Desktop Client and mobile client users use the Mitel Border Gateway (MBG) server to access the MiCollab Client Server and other integrated applications such as NuPoint UM voice mail and MiCollab Audio, Web and Video Conferencing (formerly MCA) when MiCollab Client is communicating with the MiVoice Business PBX.

Remote Web browser users and MiCollab Mobile Client clients connect to MiCollab Client in the LAN through the Web Proxy. Remote MiCollab Client Desktop Client users connect to MiCollab Client in the LAN through the Teleworker service in the MBG server.

An MBG server with Web Proxy installed in the Demilitarized Zone (DMZ) or on the network edge protects the MiCollab Client Service in the LAN from Internet exposure. These configurations provide a secure method for remote Web browser users and remote MiCollab Client Desktop Client users to connect with a MiCollab Client Service located on the corporate LAN. They also provide MiCollab Mobile Client clients (mobile devices with MiCollab Mobile Client application) access to MiCollab Client in the LAN.

When teleworker mode is enabled in the MiCollab Windows Desktop Client s and mobile clients, the SIP softphone and MiNET softphone route the signaling and media traffic through the MBG even when the clients are used in the internal network.

> ℹ️ **Note**:
>
> To receive real time notifications from the Office 365 Exchange server, a CA signed certificate must be installed on the MBG.

3.1.1   DMZ configurations

In a DMZ configuration, as shown in the following figure, the firewall is the gateway for all IP network traffic with the Internet.

Figure 3: MiCollab Client Service in LAN with MBG and web proxy in DMZ
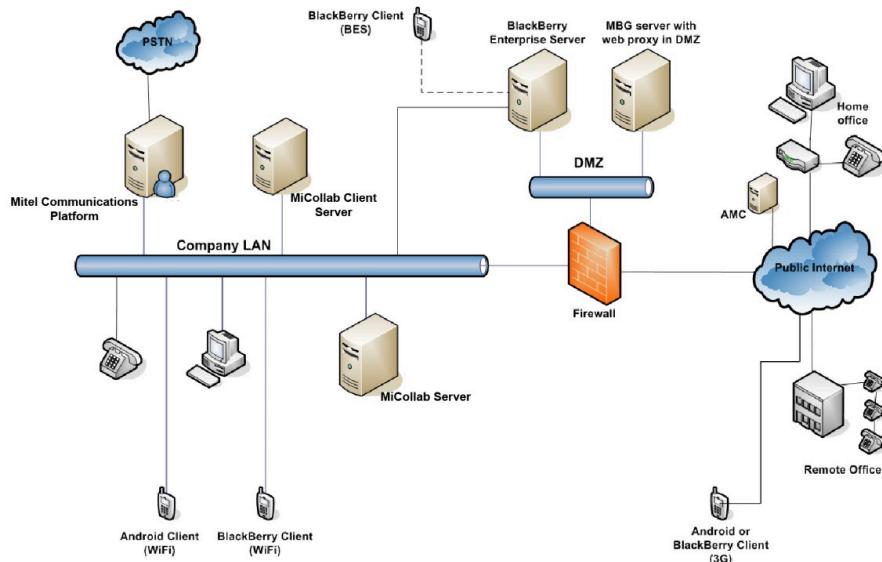
If the MBG is installed in a DMZ, the firewall facing the Internet must have ports specified in Table 1 opened for home office and remote office workers to access the MiCollab Client Service.

The ports listed with MBG <- Internet direction in "Compatibility Table" need to be open in the firewall facing the external network. Ports listed with MBG -> LAN direction needs to be opened in the firewall separating the DMZ and the LAN. The direction of the arrow indicates permission to initiate new traffic in that direction. These rules assume a stateful firewall that will permit return traffic on an existing established connection.

To support real-time notifications for MiCollab Mobile Clients, traffic from the Internet arriving at the firewall on port TCP 36008 must be port forwarded to TCP port 36008 on the MiCollab Client Service via a firewall rule. This rule is needed when running MBG version 7.0. If MBG is upgraded to version 7.1, this firewall rule is no longer needed.

Also refer to Ports needed by MiCollab Client Server on a Local Area Network (LAN) for a complete port usage diagram of MiCollab Client Service and different MiCollab Clients.

Table 3: Firewall ports to be opened when MBG is in DMZ

| Port range	Direction	Purpose
TCP 443	MBG -> LAN	For remote access of MiCollab NuPoint voice mail, MiCollab Client and MiCollab Audio, Web and Video Conferencing server.
TCP 36008	MBG <- Internet MBG -> LAN	For remote access to MiCollab Client Service for real-time notification support on MiCollab Mobile clients. (Does not traverse MBG in DMZ configuration when running MBG version 7.0).
TCP 6801,6802	MBG <- Internet	MiNET Call Control. Allow incoming and outgoing packets for TCP ports 6801 (MiNET-SSL) and 6802 (MiNET-Secure V1) between the server and the Internet. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNET), 6801 and 6802 between the server and the LAN and the server and the ICP(s). The LAN rule can be omitted if there are no IP sets on the LAN, but ensure that the ICP(s) can communicate with the server's public address.
TCP 6800,6801,6802	MBG -> ICPs	See note above for MiNET call control.
UDP 20000 – 31000	MBG ↔ Internet MBG ↔ LAN	For softphone RTP. These ports must be open in both directions from Internet to LAN.
SIP TCP 5060SIP TLS 5061	MBG ↔ Internet	Required for SIP softphone

> **ⓘ Note**:
>
> In the direction LAN **->** MBG WAN IP, allow NAT loopback (hairpinning) on ports TCP 443, UDP 20000 - 31000, and SIP TLS 5061.

Refer to the *MBG Engineering Guidelines* on the Mitel Document Center Web site for details about ports that need to be opened in the firewall for incoming traffic from Internet and outgoing traffic to LAN.

3.1.2   Network Edge configuration

In a Network Edge configuration, as shown in the following figure, the MBG server acts as a firewall/gateway for the MiCollab Client Service. Refer to Firewall ports to be opened when MBG is in DMZ above for ports to be opened in the firewall for this configuration and ignore the MBG -> LAN direction entries.

Figure 4: MiCollab Client Service in LAN with MBG and Web Proxy in network edge
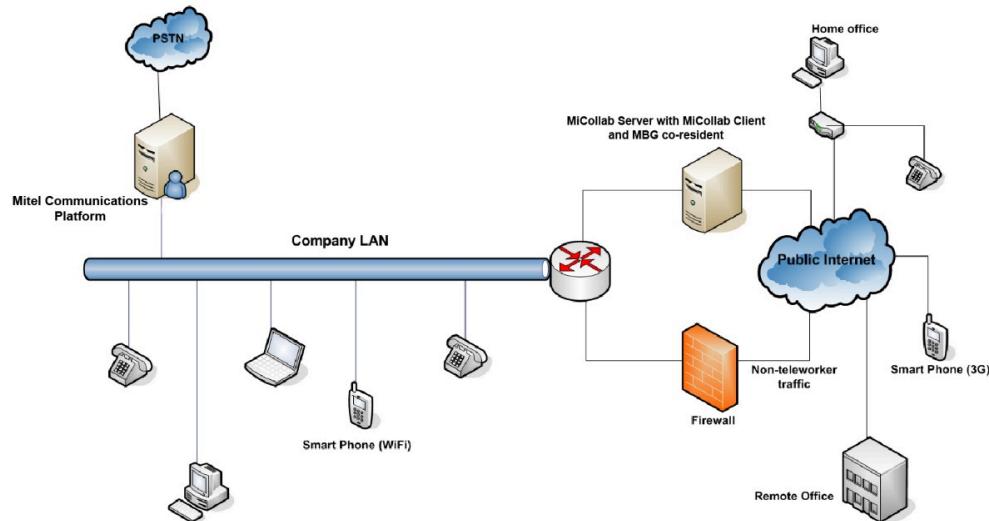
The MBG handles the routing of the external ports from external to the internal network. The MBG can be connected directly to the public Internet (See above figure) where port mapping is not needed on the firewall because the firewall is not used to pass MiCollab Client network traffic.

> ℹ️ **Note**:
>
> If a custom port forwarding rule was added for port 36008 in a MBG 7.0 environment, it should be removed once you upgrade to MBG 7.1 or higher. The port forwarding rule below is no longer necessary with MBG version 7.1 or higher.
>
> Background:
>
> The port forwarding rule was previously needed when using MBG version 7.0 to support real time notifications for MiCollab Mobile Clients. Traffic from the internet arriving at the MBG server on port TCP 36008 was forwarded to TCP port 36008 on the MiCollab Client Service through a port forwarding rule on the MBG server using the following parameters:

Table 4: Port forwarding configuration to support MiCollab Mobile Clients with MBG prior to release 7.1

| PORT FORWARDING PARAMETER	VALUE
Protocol	TCP
Source Port(s)	36008
Destination Host IP Address	IP Address of MiCollab Client Service
Destination Port(s)	36008
SNAT	checked

Refer to the MBG documentation on the Mitel Document Center Web site for MBG configuration details. Refer to the MiCollab documentation in the same location for Web Proxy configuration details.

3.1.3   Server/Gateway mode (when co-resident with MAS)

In a server/gateway mode, as in shown in the following figure, the MiCollab Client Service (as part of MiCollab) sits directly on both the Company LAN and the WAN.

Even though MiCollab Client is directly accessible on the network to teleworker users in this configuration, the MBG application must be configured to support RTP traffic used by remote soft phones.

Figure 5: MiCollab Client Service in Server/Gateway Mode as part of MAS
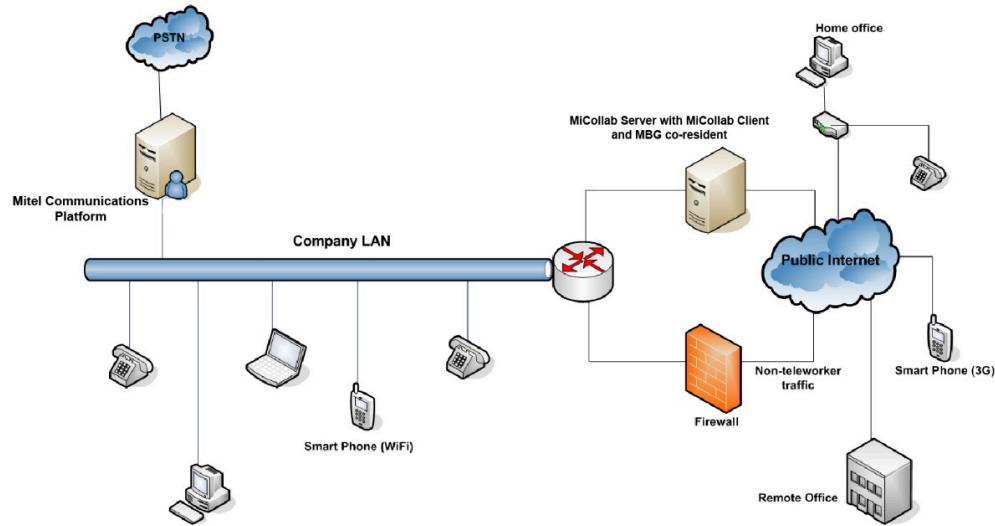
3.2   MiCollab Client without MBG configurations

Configurations that do not include the MBG are typically used with MiVoice Office 250 PBX. The following figure shows the configuration.

Figure 6: MiCollab Client Service in LAN or DMZ with no MBG
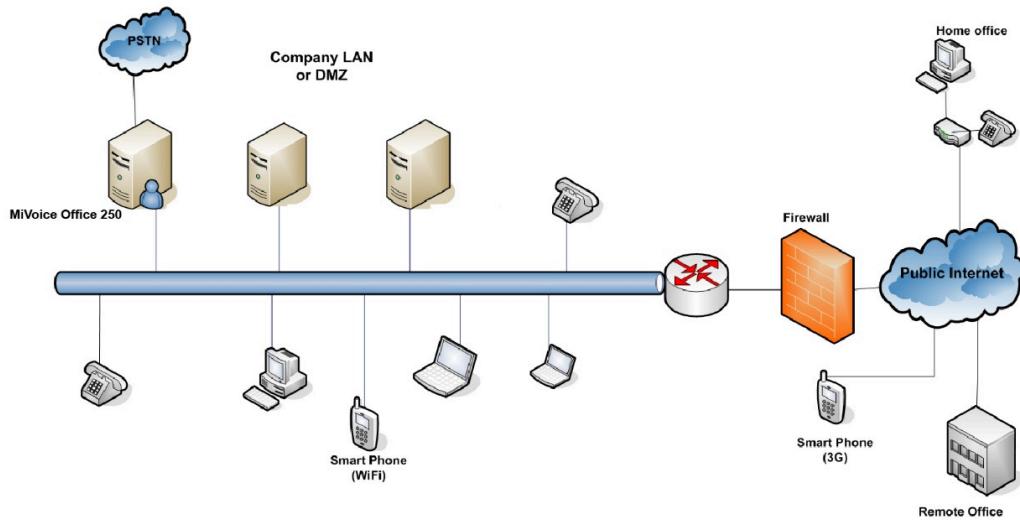
The following table lists the ports that need to be opened in the firewall for a configuration that does not include the MBG server. It also assumes that MiCollab Client Service and MiCollab Office 250 are in the DMZ and phones in the LAN when there is a DMZ setup. This table lists only ports needed for MiCollab Clients to work.

The ports listed with MiCollab Client <- Internet direction in the following table need to be opened in the firewall facing the external network. The direction of the arrow indicates permission to initiate new traffic in that direction. These rules assume a stateful firewall that permits return traffic on an existing established connection.

> **ℹ Note**:
>
> If the MiCollab Client internal and external hostname differ, mobile clients will not show images on the external network.

Table 5: Ports to be opened in firewall when there is no MBG in the network

Port range	Direction	Purpose
HTTPS 443	MiCollab Client <- Internet MiCollab Client -> Internet	For Web services access from MiCollab Client to MiCollab Client Service, MiCollab Audio, Web and Video access from the MiCollab Windows Desktop Client, NuPoint voicemail system access from the MiCollab Windows Desktop Client. For MiCollab Client Deployment and MiTeam solution.
TCP 36008	MiCollab Client <- Internet	For remote access to MiCollab Client Service for real-time notification support on MiCollab for Mobile clients.
TCP 6800,6801,6802	MiVoice Office 250 <- Internet	MiNET Call Control. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNET), 6801 (MiNET-SSL) and 6802 (MiNET-Secure V1) between the PBX and the Internet.

Port range	Direction	Purpose
UDP 6004-6261	MiVoice Office 250 <-->internet	For RTP traffic to MiVoice Office 250 Processor Module
UDP 6604-7039	MiVoice Office 250 <-->Internet	For RTP traffic to MiVoice Office 250 Processor Expansion Card
SIP UDP port 5060 SIP TLS port 5061	MiVoice Office 250 <--> Internet	Required for SIP softphone

The following figure shows the different ports MiCollab Client requires when all the other servers and clients shown in the figure are in the same LAN network. Use this as a reference to determine what ports to open in the firewall when there is one between the MiCollab Client Service and any of the other servers and clients shown.

Note:

SIP TCP port 5060 is used for MiCollab Business. SIP UDP port 5060 is used for MiCollab Office.

Note:

UDP audio port 50098 to 50508 is used for Legacy MiCollab Desktop Client. For MiCollab for PC Client, UDP audio port used is 55004 to 55024.

Figure 7: Ports needed by MiCollab Client Server on a Local Area Network (LAN)
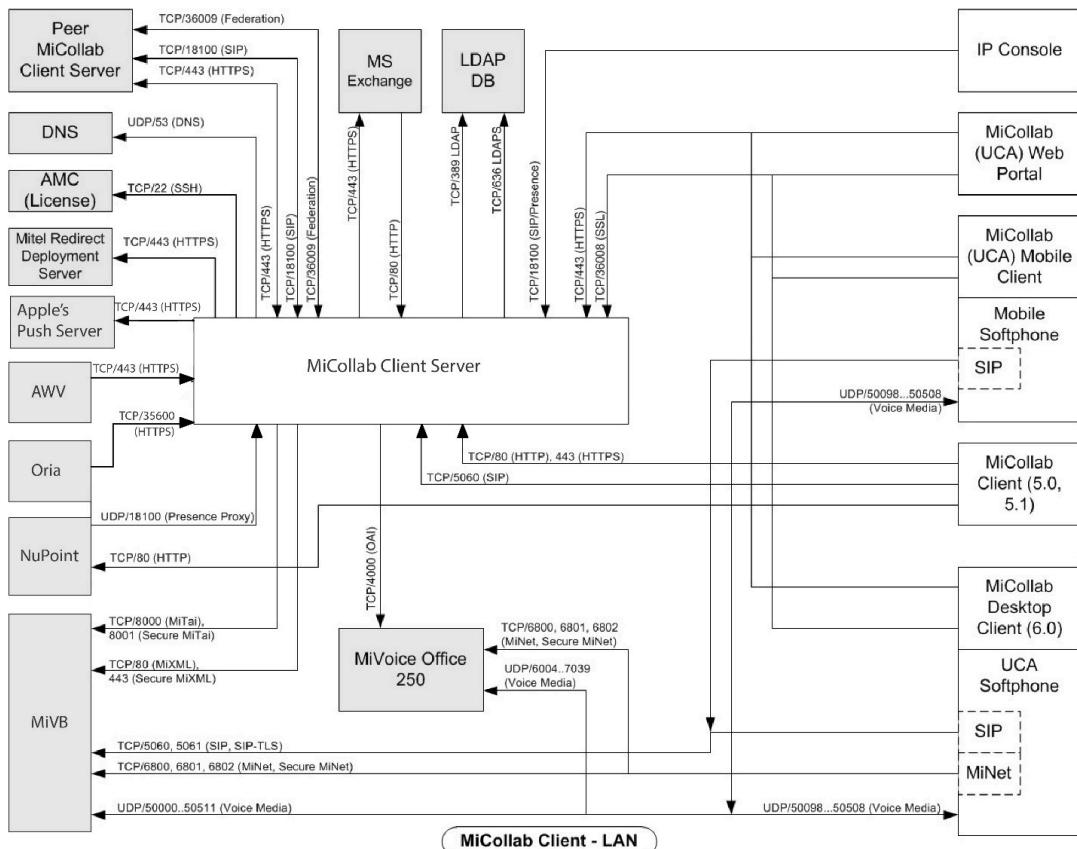
The following figure shows all the different ports MiCollab Client requires when all the other servers shown in the figure are in the same LAN network and the MiCollab Clients are connecting via the MBG. Use this as a reference to determine what ports to open in the firewall when there is one between the MiCollab Client Service and any of the other servers and clients shown.

> **ℹ Note**:
>
> UDP audio port 50098 to 50508 is used for Legacy MiCollab Desktop Client. For MiCollab for PC Client, UDP audio port used is 55004 to 55024.

Figure 8: Ports needed by MiCollab Client Service on a Local Area Network (LAN) where the MiCollab Clients are required to connect via the MiVoice Border Gateway (MBG)
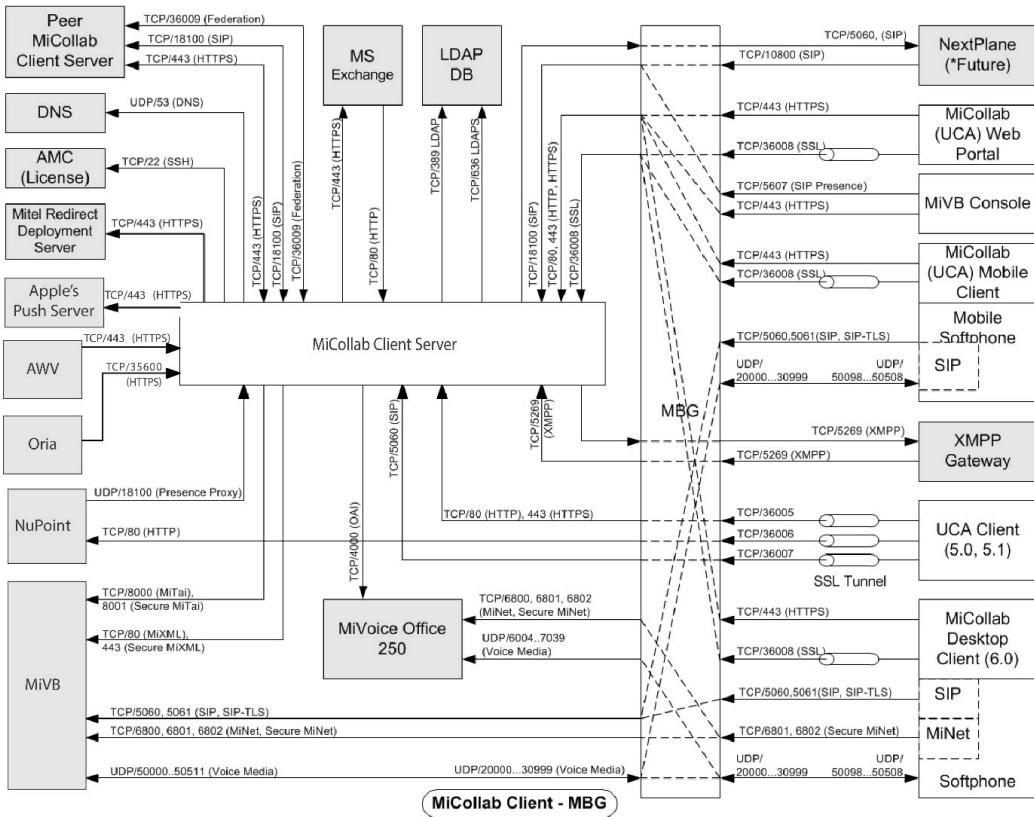
## 3.2.1   DNS Configuration with Web Proxy

MiCollab Client requires a split DNS setup. The MiCollab Client Service host name must be set up as shown in the example below.

A split DNS setup is one where a single domain is split into two zones: an internal zone and an external zone. Internal hosts are sent to an internal DNS server for name resolution and external hosts are sent to an external DNS server. The same DNS query produces different results depending on the source of the request.

The external DNS must be programmed to resolve requests for ucserver.example.com to the external IP address of the MBG server (IP3 in the following figure).

The internal DNS must be programmed to resolve requests for ucserver.example.com to the IP address of the MiCollab Client Service on the LAN (IP1 in in the following figure).

Figure 9: Split DNS setup
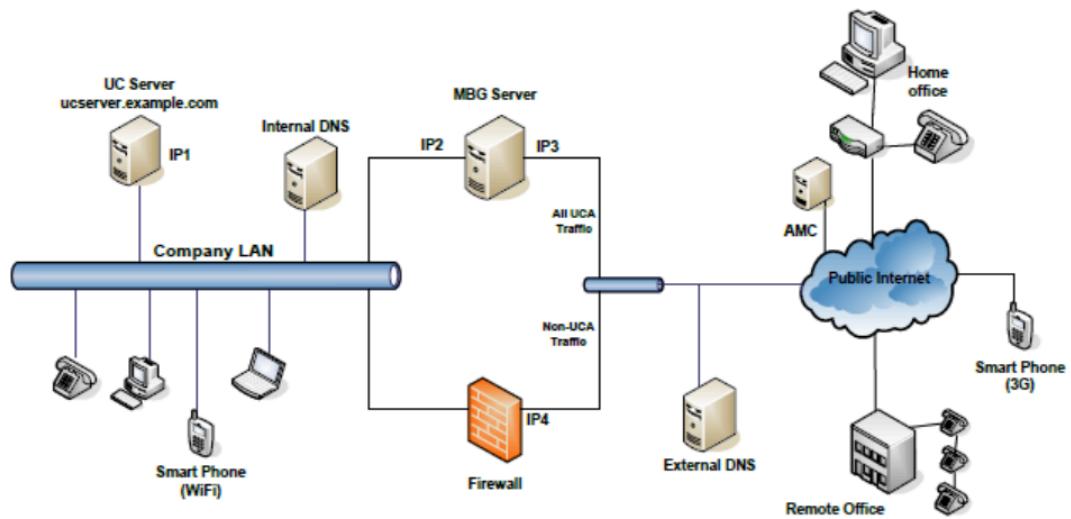
Note:

If the MBG is set up in the DMZ (instead of in the edge), then the external DNS must be programmed to resolve requests to ucserver.example.com to external interface of the firewall (IP4 in the above figure).

MiCollab Client Deployment configuration

4

This chapter contains the following sections:

The MiCollab server can be deployed in a variety of ways, depending on which services and applications you wish to provide, where your users are located, and whether you are using a physical or virtual system. When MiCollab is deployed with MiCollab Client Deployment, however, the following basic configuration scenarios are recommended:

MiCollab in LAN Mode Clustered with MBG(s) in the DMZ

MiCollab in LAN Mode Clustered with MBG(s) on the Network Edge

MiCollab with MBG on the Network Edge (Server Gateway Mode)

> ⓘ **Note**:
>
> A trusted third party SSL certificate is required for MiCollab Client Deployment. Install the certificate on the MBG in the DMZ and on the MiCollab on the LAN. See the appropriate configuration steps below.

Use these scenarios to obtain an overview of the conditions and settings that you need to employ. For detailed instructions, refer to the documents provided with MiCollab, MBG and MiCollab Client Deployment. For other deployment configuration examples, see the *MiCollab Engineering Guidelines.*

> ⓘ **Note**:
>
> The MBG Web Proxy is not supported directly on a MiCollab server in either LAN mode or Network Edge mode.

4.1 MiCollab in LAN Mode Clustered with MBG(s) in the DMZ

This solution consists of MiCollab on the corporate LAN and one or more MBGs providing Teleworker and Web Proxy services in the DMZ. The Teleworker service is employed on both the MiCollab and MBG systems while the Web Proxy Service is provided only by the MBGs. The Teleworker service in MiCollab is only used to remotely manage the Teleworker phones that are configured on the MBGs.

To support this configuration, install the MiCollab server with the MBG application in the LAN and install one or more standalone MBG servers in the DMZ. Then create a cluster that ties the MBGs together.

4.1.1 Conditions

The MiCollab server on the LAN must be configured in "Server-only on LAN" mode and the MBG(s) in the DMZ must be configured in "Server-only on DMZ" mode. (Note that MBG clustering is only supported for MiCollab systems that are configured in "Server-only on LAN" mode.)

The MBGs in the DMZ must be routable to the MiCollab server on the LAN.

All MBGs must have the same software version. This ensures support for the full range of MBG features and services.

The MBG on MiCollab and the MBG(s) in the DMZ must be added to a cluster. Clustering provides the following benefits:

- Allows data (including Teleworker services) to be managed from the MiCollab application.
- Enables license pooling. Note that, although licenses are pooled, it is recommended that you purchase all Teleworker service licenses for the MBG(s) located in the DMZ in order to avoid licensing issues.
- The MiCollab and MBG nodes must reside in separate logical zones. Use the default zone for the node located on the LAN and create a new zone for the nodes located in the DMZ.

MiCollab in LAN Mode Clustered with MBGs in the DMZ

See MiCollab Client Deployment help for more information.

To have Clients connect using DNS, set MBG's DNS to FQDN of the MBG configured in external DNS. This resolves both internal and external DNS to the public IP of the MBG Server.

> **ⓘ Note**:
>
> A proper configured NAT loopback (hairpinning) is required for the communication with the Public IP of the MBG.

4.2   MiCollab in LAN Mode Clustered with MBG(s) on the Network Edge

This solution consists of MiCollab on the corporate LAN and one or more MBGs providing Teleworker and Web Proxy services on the network edge. The Teleworker service is employed on both the MiCollab and MBG systems while the Web Proxy Service is provided only by the MBGs. The Teleworker service in MiCollab is only used to remotely manage the Teleworker phones that are configured on the MBGs.

To support this configuration, install the MiCollab server with the MBG application in the LAN and install one or more standalone MBG servers on the network edge. Then create a cluster that ties the MBGs together.

4.2.1   Conditions

The MiCollab server on the LAN must be configured in "Server-only on LAN" mode and the MBG(s) on the network edge must be configured in "Server-only on network edge" mode. (Note that MBG clustering is only supported for MiCollab systems that are configured in "Server-only on LAN" mode.)

The MBGs on the network edge must be routable to the MiCollab server on the LAN.

All MBGs must have the same software version. This ensures support for the full range of MBG features and services.

The MBG on MiCollab and the MBG(s) on the network edge must be added to a cluster. Clustering provides the following benefits:

• Allows data (including Teleworker services) to be managed from the MiCollab application.
• Enables license pooling. Note that, although licenses are pooled, it is recommended that you purchase all Teleworker service licenses for the MBG(s) located in the DMZ in order to avoid licensing issues.

The MiCollab and MBG nodes must reside in separate logical zones. Use the default zone for the node located on the LAN and create a new zone for the nodes located on the network edge.

See MiCollab Client Deployment help for more information.

4.3   MiCollab Server with MBG on the Network Edge (Server Gateway Mode)

Network Edge (Server-Gateway) mode can be used to deploy any of the MiCollab applications. In this configuration, MiCollab must have direct Internet access, which is required by the MBG Teleworker and MiCollab Client applications.

4.3.1   Conditions

The MiCollab server requires two Ethernet adaptors. One adapter is configured as "Local" for connection to the LAN, and the other is configured as "WAN" for connection to the Internet. The WAN network adapter requires a publicly routable IP address that is accessible to both the Internet and the LAN (in other words, the server should not reside behind a NAT device).

Preferably, MiCollab should be used in conjunction with the corporate firewall. The MiCollab system acts as a firewall/gateway for MiCollab applications while the corporate

firewall controls data traffic for the enterprise. If your voice/telephony network and your data network are separate, connect the MiCollab local network adapter to the voice/telephony network in order to support the MiCollab telephony applications.

Network Edge (Server-Gateway) mode involves a number of security considerations:

- Most application traffic is encrypted, because the system supports Secure Real-time Transport Protocol (SRTP) for SIP traffic on both the ICP side as well as the set side of the network edge. However, calls between SIP endpoints and some older Mitel MiNET devices may be unencrypted because the MiNET devices only support RTP. This issue does not arise when newer Mitel MiNET devices are in use.
- When using Teleworker in conjunction with LAN-facing applications, you must ensure that they review the configuration in relation to your corporate security policy. You may choose to deploy Teleworker on a separate server in a DMZ.

See MiCollab Client Deployment help for more information.

Server Gateway mode (iOS Client): For MiCollab Servers that are running in the Server Gateway mode, where they have a WAN and a LAN port, and a split DNS setup to point to both interfaces that will need to change. From MiCollab 8.0 onwards, MiCollab for Mobile Client for iOS must be configured to use the Teleworker Service through the WAN port. Therefore, while on the WiFi LAN, the application must use the WAN interface. For example, by re-deploying the iOS users with Teleworker setting on – targeted to the WAN IP of the teleworker.

Split DNS is not supported in this topology. The Client must use the IP address or a FQDN that resolves to the WAN port. It will also work for all other services except administration through Server Manager. You must point to the LAN port IP Address or FQDN to manage the server.

4.4   MiCollab Mobile Client for Smart Devices Configuration

MiCollab mobile clients (smart devices) make use of a web socket connection to the MiCollab Client Service to support real-time notifications of missed calls and other events. To enable this functionality, a persistent connection is made from the device via TCP port 36008 to the MiCollab Client Service.

If using an MBG server in server/gateway mode to proxy MiCollab Client traffic, a port forwarding entry should be configured on the MBG as specified in "Port forwarding configuration to support MiCollab Mobile Clients with MBG prior to release 7.1": Port forwarding configuration to support MiCollab Mobile Client. This is needed only if the MBG is running version 7.0. On upgrade to MBG version 7.1 or above, the port forwarding entry should be removed.

If an MBG is not being used, configure the firewall to forward traffic arriving on port 36008 to the MiCollab Client Service.

Figure 10: Configuring support for MiCollab Client
Smart Devices when using an MBG in the DMZ
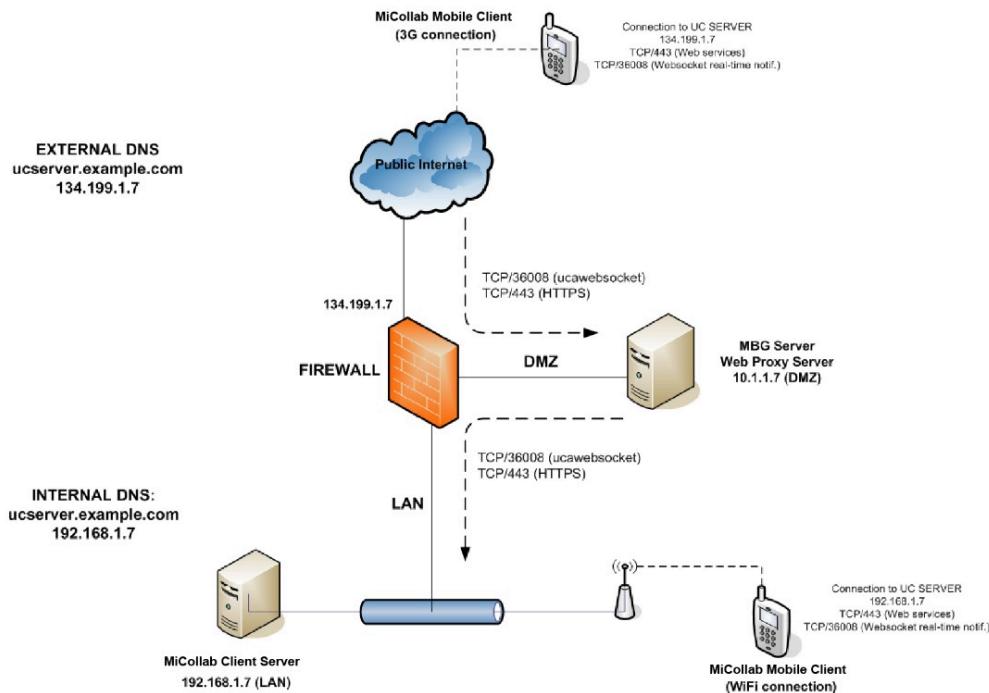
4.5   MiCollab Client Service Peering Configuration

MiCollab Client Service peering is used to connect MiCollab Client Services that are at different locations of a given company. It can also be used for scaling when multiple MiCollab Client Services are needed to support a large customer deployment.

Note the following for MiCollab Client Service peered configurations:

- There can be no MBG server between MiCollab Client Services that are peered.
- An MBG server is needed for each MiCollab Client Service for Teleworker support and remote access.
- If there are any firewalls between the server locations, the following ports must be opened on the firewalls in each direction:

  - TCP port 36009 (for web socket communication between peered MiCollab Client Services)
  - HTTPS port 443 (for web service access and MiTeam Cloud-based solution)
  - TCP port 18100 for SIP communications TCP port 18105 for SIP registrations
  - Refer to the *MiCollab Client Administrator Guide* for information regarding MiTeam Integration with peered configurations.

4.6   MiCollab Client Presence Federation configuration

MiCollab Client supports IM and presence federation with third party systems such as Lync and IBM Lotus Sametime. Federation between MiCollab Client and a Lync/Sametime server within the same company is supported. Federation is not supported across companies.

See "Compatibility Table" for supported third party systems.

An example of a federation configuration is shown in "Split DNS setup". TCP port 5269 for XMPP message communication must be opened in both directions on the firewall between the two servers.

Figure 11: MiCollab Client Service Setup for IM and presence federation with OCS
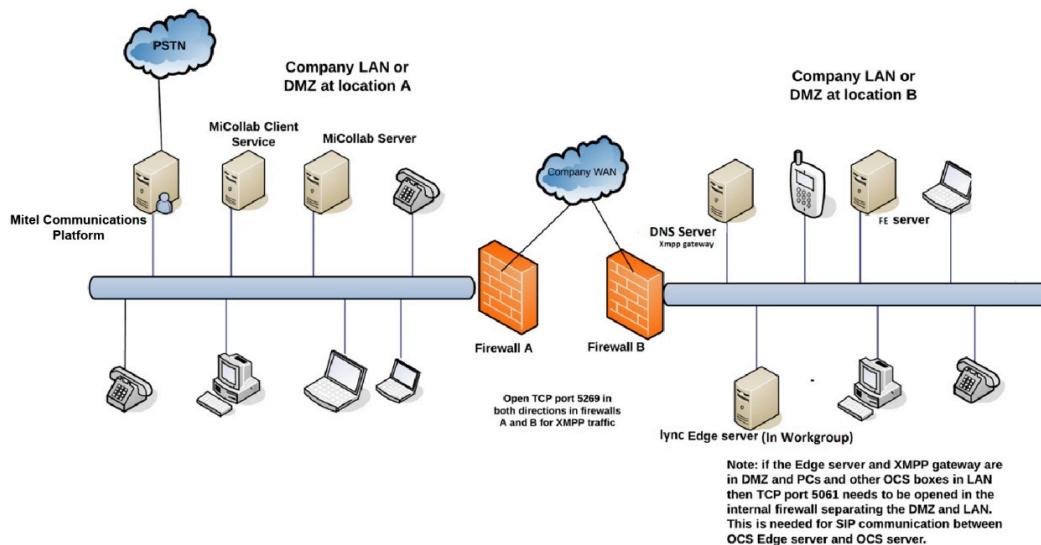
> **Note**:
>
> MBG 8.0 or higher is required to support federation with OCSLync, IBM Sametime when MBG is in the network between MiCollab Client Service and the federated Lync, Sametime.

4.7   Performance recommendations

The performance of the MiCollab Client Service is impacted by the following factors:

- The call traffic on the PBXs monitored by MiCollab Client Service.

- The corporate directory size (i.e. the number of accounts on the system).

- The client status change rate per second. This rate depends on the number of active Desktop Clients and MiCollab Mobile clients. The Desktop Client can trigger status changes based on calendar triggers and manual user changes. The mobile client can trigger status changes based on location changes and manual user changes.

- The number of subscriptions in the MiCollab Client Service for each connected client. This includes the desktop MiCollab client, web client and MiCollab Mobile clients.

- The visual voice mail traffic for the Desktop Client and mobile clients. Periodically, these clients do a voice mail message refresh. The refresh traffic depends on number of clients logged in to the system.

- Instant Messaging as determined by the number of simultaneous chat sessions opened.

- MiCollab Client Service peering: The impact of MiCollab Client Service peering on performance depends on the presence subscriptions for peered MiCollab Client contacts. Multiple users on MiCollab Client Service A subscribing to same user's presence on MiCollab Client Service B creates only one subscription on servers A and B. So the subscription overhead is minimized. The SIP Notify traffic has the most impact and this depends on call traffic and status change traffic on peered MiCollab Client Services.

- IM and Presence Federation. The impact of IM and Presence Federation on performance depends on the number of subscriptions to the federated contacts. The impact on performance depends only on status changes, as telephony presence is not federated.

For system recommendations, refer to "System recommendations".

4.8   Virtualization

MiCollab Client Service is provided in virtual appliance form for customers who have a VMware® environment in place. The virtual appliance includes Mitel Standard Linux® (MSL), MiCollab Client Service, and configuration requirements for the virtual machine.

Refer to the *Virtual Appliance Deployment Solutions Guide* for detailed virtualization information including version support and requirements.

Resource reservations are configured for the CPU and memory at OVA deployment time. The MiCollab Client Service virtual machine must have connectivity to Mitel's Application Management Center (AMC) for proper licensing operation. Running the MiCollab Client Service within a VMware environment requires a license that allows usage in a virtualized environment.

Refer to the VMware documentation supplied with the product and available on the *VMware Web site* for more information (http://www.vmware.com).

4.9 System capacities

The following tables provide the maximum system capacities validated by Mitel for MiCollab Client 7.1. Capacities vary based on factors listed in the Performance Recommendations section. These performance numbers are also applicable to MiVoice for Skype for Business.

Table 6: System recommendations

Capacity	Clients	CPUs	Memory	Disk Space
Up to 250 users	Up to 500 Clients	2 virtual CPUs	5 GB	40 GB
Up to 1500 users	Up to 3000 Clients	4 virtual CPUs	7 GB	40 GB
Up to 2500 users	Up to 5000 Clients	4 virtual CPUs	8 GB	40 GB
Up to 5000 users	Up to 10000 Clients	4 virtual CPUs	10 GB	40 GB

> **Note**:
>
> Physical server recommendations should meet or exceed virtual server recommendations.

> **Note**:
>
> Mitel supports any VMWare qualified server. Refer to the *Virtual Appliance Deployment Solutions Guide* for complete virtualization deployment information.

Table 7: MiCollab Client System Capacities: MiCollab Client Standalone

System Information	Single App	Single App
Physical/Virtual	Physical[5]	Virtual
LDAP Authentication	NO	NO
MiCollab Client peering	YES	YES
Number of MiCollab Client peers	8[6]	8
Number of users	5,000	5,000
Number of Clients per user	2	2
Total number of MiCollab Clients[7]	10,000	10,000
Average number of devices per user	2	2
Total Number of Devices[8]	10,000	10,000
Total Number of Corp Contacts	20,000	20,000
Number of MICD Instances	5	5

[5] Physical server recommendations should meet or exceed virtual server recommendations
[6] A total of eight MiCollab Client servers can be peered (i.e. a single MiCollab Client can peer with seven others)
[7] Supports Desktop, MiVoice for Skype for Business, Web, Android and iOS clients in any combination not exceeding the maximum number of clients.
[8] Supports Deskphone, Softphone (MiNET and SIP) and mobile devices in any combination not exceeding the maximum number of devices.

Number of Users Per Instance	1,000	1,000
Total Number of MiTAI Monitors	10,000	10,000
CPU	Mid Range	4 vCPU
Memory	Mid Range	10 GB
Processor Speed	Mid Range	2.1 GHz

Table 8: MiCollab Client System Capacities: MiCollab

	MiCollab Client on MiCollab	MiCollab Client on MiCollab	MiVoice for Skype for Business on MiCollab1
System information	**Single App**	**Single App**	**Single App**
Physical/Virtual	Physical	Virtual	Physical
LDAP Authentication	YES	YES	NO
MiCollab Client peering	YES	YES	NO
Number of MiCollab Client peers	8	8	0
Number of users	5,000	5,000	15,000
Number of Clients per user	2	2	1

System information	MiCollab Client on MiCollab	MiCollab Client on MiCollab	MiVoice for Skype for Business on MiCollab1
	Single App	Single App	Single App
Total number of MiCollab Clients[9]	20,000[10]	20,000	15,000
Average number of devices per user	2.75	2.75	1
Total number of devices[11]	13,750	13,750	15,000
Total number of corporate contacts	20,000	20,000	15,000
Number of MICD instances	5	5	15
Number of users per instance	1,000	1,000	1,000
Total number of MiTAI monitors	13,750	13,750	15,000
CPU	Mid Range	8 vCPU	Mid Range
Memory	Mid Range	16 GB	Mid Range

[9] Supports Desktop, MiVoice for Skype for Business, Web, Android and iOS clients in any combination not exceeding the maximum number of clients.
[10] MiVoice for Skype for Business supports 15,000 contacts.
[11] Supports Deskphone, Softphone (MiNET and SIP) and mobile devices in any combination not exceeding the maximum number of devices.

	MiCollab Client on MiCollab	MiCollab Client on MiCollab	MiVoice for Skype for Business on MiCollab1
System information	Single App	Single App	Single App
Processor speed	Mid Range	2.4 GHz	Mid Range

Table 9: MiCollab Client System Capacities: MiCollab

	MiCollab Client on MiCollab	MiCollab Client on MiCollab	MiCollab Client on MiCollab
Platform	MiVoice 5000	MiVoice MX-ONE	MiVoice Office 400
Physical/Virtual	Virtual	Virtual	Virtual
LDAP Authentication	YES	YES	YES
MiCollab Client peering	No	No	No
Number of MiCollab Client peers	0	0	0
Number of users	5,000	5,000	250
Number of Clients per user	2	2	2

Platform	MiCollab Client on MiCollab	MiCollab Client on MiCollab	MiCollab Client on MiCollab
	MiVoice 5000	MiVoice MX-ONE	MiVoice Office 400
Total number of MiCollab Clients[12]	10,000	10,000	500
Average number of devices per user	2	2	2
Total number of devices[13]	10,000	10,000	500
Total number of corporate contacts	5,000	5,000	5,000
Number of PBX instances	1	1	1
Number of users per instance	5,000	5,000	250
Total number of monitors	10,000	10,000	500
CPU	8 vCPU	8 vCPU	2 vCPU
Memory	16 GB	16 GB	5 GB

---

[12] Supports Desktop, MiVoice for Skype for Business, Web, Android and iOS clients in any combination not exceeding the maximum number of clients.

[13] Supports Deskphone, Softphone (MiNET and SIP) and mobile devices in any combination not exceeding the maximum number of devices.

	MiCollab Client on MiCollab	MiCollab Client on MiCollab	MiCollab Client on MiCollab
Platform	**MiVoice 5000**	**MiVoice MX-ONE**	**MiVoice Office 400**
Processor speed	2.4 GHz	2.4 GHz	2.4 GHz

4.10   Call history on MiCollab Client

The following table provides the maximum call history records stored on MiCollab Client and the server.

Table 10: MiCollab Client Call History

Call history	MiCollab Server[14]	MiCollab Client	
		MiCollab Next Generation Clients [15](MiCollab for PC, MAC, Mobile, and Web Client)	**Legacy MiCollab Desktop Client[16]**
Missed	50	50	1000
Received	50	50	
Dialed	50	50	

4.11   Remote Desktop Services (formerly Windows Terminal Services WTS)

MiCollab for PC Client is supported in a Windows Server Terminal Services or Remote Desktop Services (RDS) environment. MiCollab Client Softphone is supported on Windows Server Terminal Services or Remote Desktop Services (RDS) environments. Please reference "Compatibility Table" for compatible Windows Servers that Mitel recommends for MiCollab Client support.

Please follow Microsoft's recommendations when setting up a server to host Terminal Services. Mitel has performed some testing with a Terminal Server with the following configuration and limits:

Table 11: Windows Terminal Services or Remote Desktop Services Environments

Capacity	Limit
Maximum number of Terminal Services Connections	25
Softphone support	Yes

In order to support up to the stated limit of Terminal Server connections, Mitel recommends at a minimum the specifications below. Validation of this configuration was done with Microsoft Office and MiCollab Audio Web Video installed on the Terminal Server as well. The load applied by additional applications installed may vary and the Terminal Server administrator should follow Microsoft's recommendation for server specifications.

Terminal Server Specifications:

* CPU: Xeon x5650 2.67 GHz 6 cores (dual CPU)
* Memory: 6 GB
* OS: Windows 2016, 2019

4.12   Citrix

MiCollab Client and MiCollab with Skype for Business are compatible with Citrix Terminal services. MiCollab Client Softphone is supported on Citrix virtualized environments. Mitel has validated the following limits and requirements when deploying MiCollab Client or

MiCollab Client with Skype for Business. MiVoice for Skype for Business is supported on Citrix XenApp and Citrix XenDesktop version 7.13, 7.14, 7.18, or 7.22 virtualized environments.

Table 12: Citrix Environments

Capacity	Limit
Maximum number of MiCollab Clients per Citrix Server and master image	25
Softphone support	Yes

To support more than 25 clients per server or more than 25 Receivers, Mitel recommends deploying additional Citrix Servers (1 Citrix Server for every 25 MiCollab Client connections). Validation of this configuration was done by Mitel in a virtual environment. The physical server requirements would be equivalent and/or need to exceed the recommended specifications below. Also, additional load will be placed on the Citrix Server and image if other applications are being presented by the Citrix Server. Please follow Citrix's recommendations when deploying into a mixed environment.

Limitations (MiCollab for PC Client)

• MiTeam is not available (MiTeam is auto disabled when the Client is in a Citrix environment).
• MiCollab Client will not auto upgrade to a newer version.
• Video call is not supported.
• Users will not be able to share their desktop from the Client in XenApp.
• Users may experience slow response during large Group chats.

Specifications

• Citrix Master Image Server
• CPU Requirement: 8 vCPU (Validated with 2.67 GHz Processor)
• CPU Reservation: 12 GHz
• Memory Requirement: 16 GB RAM
• Operating System: Windows Server 2012 R2

4.13 VMware Horizon view

MiCollab Client and MiCollab with Skype for Business are compatible with VMware Horizon view services. MiCollab Client Softphone is supported on VMware virtualized environments. Mitel has validated the following limits and requirements when deploying MiCollab Client or MiCollab Client with Skype for Business. MiVoice for Skype for Business is supported on VMware Horizon view 7.4.

Table 13: VMware Environments

Capacity	Limit
Maximum number of MiCollab Clients per VMware Server and master image	25
Softphone support	Yes

To support more than 25 clients per server or more than 25 Receivers, Mitel recommends deploying additional VMware Servers (1 VMware Server for every 25 MiCollab Client connections). Validation of this configuration was done by Mitel in a virtual environment. The physical server requirements would be equivalent and/or need to exceed the recommended specifications below. Also, additional load will be placed on the VMware Server and image if other applications are being presented by the VMware Server. Please follow VMware's recommendations when deploying into a mixed environment.

Limitations (MiCollab for PC Client)

• MiTeam is not available (MiTeam is auto disabled when the Client is in a VMware environment).
• MiCollab Client will not auto upgrade to a newer version.
• Video call is not supported.
• Users will not be able to share their desktop from the Client in VMware Horizon view.
• Users may experience slow response during large Group chats.

Specifications

• VMware Master Image Server
• CPU Requirement: 8 vCPU (Validated with 2.67 GHz Processor)
• CPU Reservation: 12 GHz
• Memory Requirement: 16 GB RAM

- Operating System: Windows Server 2012 R2

4.13.1 Maximum number of users supported in virtualized environments

The following table lists the maximum number of users supported in virtualized environments.

Table 14: Maximum number of users supported in virtualized environments

Environment	Desktop mode	App mode
Citrix	25	25
VMware Horizon view	25	25
Microsoft Remote Desktop Services	25	25

4.14 MiCollab Client with Console option

The Console feature will support the following configuration:

- Up to 60 call per hour
- Up to 1500 contacts in searchable directory
- Up to 2 simultaneous calls
- Up to 25 active Consoles

For capacities beyond this, the 5550 IP Console or MiVoice Business Console is recommended.

The following information is the recommendations for using the MiCollab Client console to optimize usability and handling of call traffic.

General items for MiCollab Client Console

- MiCollab Client Console configuration will vary depending on the system type installed behind (MiVoice Business vs. MiVoice Office 250).
- It is ideal to use a Headset and enable the necessary headset mode options based on the type of headset and system installed on.

- Depending on the incoming call traffic, it is recommended to front line the external incoming call traffic to the Console by answering incoming calls first with Voice Mail Auto Attendant. Then via the Voice Mail have an option to dial the Attendant (Console) or time out to the Console.

MiVoice Business specific recommendations

- On the MiVoice Business it is recommended to program additional dedicated Multiline DN's on the keys of the console extension for call handling. Recommend adding multiple Multiline appearances for the Console extension. Avoid programming the Console extension DN on the Keys for multiline appearances. Use unique DN's for each additional Multiline key appearance on the extension used for the Console.
- Use a Hunt group on the MiVoice Business to focus the incoming calls where the Console additional Multiline DN's are part of the hunt group.

MiVoice Office 250 specific recommendations

- Recommend programming the extension number of the console in a hunt group and focus the incoming call traffic at the hunt group.
- Recommend on the MiVoice Office 250 Key programming to configure multiple Call Keys and at least 1 Intercom button. This is not necessary for using the Console but will help the console user if they need to use the telephone associated with the console where this will provide visibility of the calls on the telephone.

4.14.1 MiCollab Client with 5550 IP Console or MiVoice Business Console

> **ⓘ Note**:
>
> Please refer to "Compatibility Table" for a compatibility reference of MiCollab Client with the 5550 IP Console and the MiVoice Business Console.

The 5550 IP Console Release or MiVoice Business Console Release support the following configuration when deployed in a solution with the MiCollab Client.

Table 15: MiCollab Client with 5550 IP Console or MiVoice Business Console

Capacity	Limit
Number of MiCollab Client Peered Servers	8

Capacity	Limit
Number of MiCollab Client Contacts	20, 000
Maximum number of MiVoice Business Consoles	5

Each MiVoice Business Console has a limit of the following parameters:

Capacity	Limit
Maximum number of calls processed per hour per console	360
Maximum number of MiVoice Business Consoles handling calls	5
Average number of status changes per day per contact	5

Please refer to the MiVoice Business documentation for the MiVoice Business console hardware requirements.

4.15   MiCollab Client Quality of Service

The following sections provide Quality of Service guidelines for MiCollab Desktop and Mobile Clients.

- MiCollab Client Bandwidth Usage
- QoS and network traffic prioritization
- Wi-Fi network qualification
- MiTAI Monitor usage

4.15.1   MiCollab Client Bandwidth Usage

This section covers the bandwidth usage for the desktop and mobile clients. The usage depends on the number of calls placed or received by the client, the number of status

changes invoked by the client, and number of users for whom client is receiving real time status updates.

The numbers that are provided in this section should be used as reference to come up with overall bandwidth usage for a particular site based on usage patterns expected. When the client is in Teleworker mode, the numbers apply to the network between the internal interface of the MBG and MiCollab Client Service.

When the clients log in for the first time, there will be sudden increase in traffic because the clients fetch all the corporate directory entries and their corresponding pictures. The increase in traffic depends on the corporate directory size. To fetch 10 corporate contacts takes about 2500 bytes. The SIP subscribes from the client add very little overhead compared to the SIP Notify traffic and can be ignored. Starting from MiCollab Client 5.1 version, all the MiCollab Client clients use web socket protocol for chat feature and presence notifications. The message size in web socket protocol for presence notifications and for chat exchanges is significantly less when compared to SIP protocol.

- MiCollab Clients

All the MiCollab Clients have the following usage pattern (The telephony events apply to desktop client only):

- Receives web socket notification for every status change update for each user that the client has subscribed to. This adds up to 500 bytes on average per status update per user.
- The desktop client receives WebSocket notifications for telephony events when the client makes or receives calls. This is about 1000 bytes per telephony event received. The client receives 4 telephony events for calls originated from client and receives 3 telephony events for calls received.
- Client uses HTTP protocol for Web services to set user status. Each Web service handshake to set the status takes about 3000 bytes. A typical Desktop Client user does about 5-6 status changes per day. This is assuming one status change on login in the morning and status change on logout with 3-4 meetings in a day.
- Client uses CSTA Web services for third party call control to make calls, answers calls, hang up calls, and other call control functions. Each Web service handshake for CSTA uses about 1500 bytes.
- The visual voice mail feature also uses Web services. Each Web service request and response to get a new message takes about 2500 bytes. Fetching additional voice mail messages in the same Web service request adds additional 100 bytes per voice mail message.
- Instant Messaging uses about 100 bytes for each message exchange (i.e. web socket message) in one direction assuming a message content size of 100 bytes.
- The MiCollab Desktop and Mobile Client softphones support G722, G722.1, G729, G711 u-law, G711 a-law codec and from Release 9.7 onwards Opus codec is also supported. ILBC is not supported. The values for one call (incoming and outgoing RTP stream) for each of the codecs are; G711 codec need 160 kbps bandwidth, G729

codec need 56 kpbs of bandwidth, G722 codec need 170 kbps of bandwidth, G722.1 codec need 106 kbps and Opus codec needs 64 kbps of bandwidth.

- For SIP Video calls, the bandwidth usage depends on the video resolution used. HD video uses 1600 kbps, High resolution uses 700 kbps, Standard resolution uses 576 kbps and web resolution uses 256 kbps.

The HD, High, Standard and Web resolution are choices available on desktop client for the video camera setting in softphone settings under Account configuration.

The resolution settings for the Mobile clients are found under the Advanced Settings (Softphone Settings).

> **ⓘ Note**:
>
> SIP Video is supported on the Desktop and Mobile clients (Android, iPad and iPhone). HD resolution is not supported on Mobile clients.

- Minimum requirements for SIP video calls on MiCollab Mobile Client devices

The below recommendations are only for the SIP video calls. The SIP audio calls are supported with lower requirements.

iOS Devices	
iPad	iPad 2 and newer versions
	iPad Mini and newer versions
iPhone	iPhone 4S and newer versions
Android Devices	
For video, Mitel recommends: • An Android device with a Dual-Core 1.2 GHZ CPU with a minimum of 1 GB of RAM. • Using the Web and Standard Video Resolutions.	

For MiCollab Audio, Web and Video Conferencing video calls and Web/video collaboration from MiCollab Client, refer to the bandwidth requirements information in the MiCollab Audio, Web and Video Conferencing Administrator Online Help.

> **ℹ Note**:
>
> Unless otherwise mentioned, the bandwidth numbers above are for voice/video in each direction (For a bi-directional call, the bandwidth requirement will be twice the number. If a call has multiple legs (such as conference calls) then the bandwidth provisioning needs to account for each of those legs.

> **ℹ Note**:
>
> The video bandwidth numbers do not include the audio stream bandwidth. Therefore, the total bandwidth required for a video will be the number of streams * (audio bandwidth + video bandwidth).

When using the MiCollab Client Desktop Client in Teleworker mode, keep in mind that the bandwidth required for voice, video, and signaling is in addition to bandwidth requirements for other applications running on the PC and other devices connected to the remote network.

MiCollab Client symptoms of insufficient bandwidth include degraded voice and/or video quality for the softphone or IP Desk phone, slow response, service interruption, or loss of service.

4.15.2   QoS and network traffic prioritization

Some of the MiCollab Client clients use DSCP fields to indicate network traffic priority for different network usage (such as voice, multimedia, etc.). It is up to the network deployment to support and adhere to the DSCP field values.

- Android and iOS Clients support user programmable DSCP values. For the recommended QoS settings, refer to the following tables.
- MiCollab Client Desktop client does not support user programmable DSCP values. Windows platform sets some default values. Windows 10 and 11 overwrite the MiCollab Windows Desktop Client DSCP values set by the application. Refer to DSCP configuration for Windows 7 and above.

Table 16: Mitel Recommended L2 and L3 QoS settings

SERVICE CLASS	L2 PRIORITY	L3 PRIORITY	WMM ACCESS CATEGORY	WMM CATEGORY
Network Control	6	48	AC_VO	Voice
Telephony (Voice)	6	46	AC_VO	Voice
Signaling	3	24	AC_BE	Best Effort
Multimedia Conferencing	4	34	AC_VI	Video
Real Time Interactive	4	32	AC_VI	Video
Multimedia Streaming	4	32	AC_VI	Video
Broadcast Video	4	32	AC_VI	Video
Low Latency Data	2	18	AC_BK	Background
OAM	2	16	AC_BK	Background
High Throughput Data	1	10	AC_BK	Background
Standard	0	0	AC_BK	Background
Low Priority Data	1	8	AC_BK	Background

Table 17: MiCollab Client for Android and iOS, Network configuration programming

Telephony (Voice)	Signaling	Multimedia Conferencing
DSCP=46	DSCP=24	DSCP=34

> ℹ️ **Note**:
>
> These are default values and can be modified.

Table 18: MiCollab Client for Windows, Network configuration programming

Telephony (Voice)	Signaling	Multimedia Conferencing
DSCP=56	DSCP=40	DSCP=40

> ℹ️ **Note**:
>
> MiCollab Client and Service do not support the use of inferred Cisco QoS values.

- DSCP configuration for Windows 7 and above

As of Windows 7, applications are no longer able to set DSCP QoS. Windows 7 and above overwrites the value with 0. The MiCollab Windows Desktop Client SIP and MiNET softphones are impacted by this change and the DSCP value 46 (the industry standard for RTP) cannot be set by the application.

Microsoft has taken steps in Windows 7 to enforce the view that QoS in a network should be decided by the Administrator and not to individuals or individual applications. It is a holistic approach to determine what in the network gets priority. Therefore, users and applications in a Windows Domain must rely on the Domain Administrator to configure Group Policies for the softphone application to apply specific DSCP values to RTP traffic.

Refer to the following article for more information: Microsoft article for Policy based QoS on Windows 7: http://technet.microsoft.com/en-us/library/dd919203(v=ws.10).aspx

- Recommendations

- **If QOS Policies are controlled by an IT organization, set group policies at the IT and network level.**

  To overcome this limitation, the Legacy MiCollab Desktop Client SIP Softphone should be used in conjunction with Group Policy based on QoS set at the network level. Policy based QoS can also be applied at the application level. The IT administrator creates a policy based on the application name, source and/or destination IP addresses, source and/or destination ports, and the protocol (TCP, UDP, or both). Application names on respective MiCollab Clients are:

  - Legacy MiCollab Desktop Client:

    UCA.exe for SIP softphone and *UCASoftphoneManager.exe* for MiNET softphone
  - MiCollab for PC Client: *MiCollab.exe*

    Refer to the following article from Microsoft to configure policy based QoS: http://technet.microsoft.com/en-us/library/dd919203(v=ws.10).aspx#BKMK_configuring

- **If no IT policies are imposed by an IT Organization, set group policy at the individual PC level.**

  A user can set Group policy local to the user machine using the Microsoft Group Policy editor. (Run gpedit.msc.) The user can create a policy based on the application name, source and/or destination IP addresses, source and/or destination ports, and the protocol (TCP, UDP, or both). Application names on respective MiCollab Clients are:

  - Legacy MiCollab Desktop Client: *UCA.exe* for SIP softphone and *UCASoftphoneManager.exe* for MiNET softphone
  - MiCollab for PC Client: *MiCollab.exe*

The following article provides an example of creating a local group policy at a user machine.

http://technet.microsoft.com/en-us/library/cc771283%28v=ws.10%29.aspx

---

ℹ Note:

> IT administrator policy based QoS takes precedence over local policy in the enterprise computer.

- Setting QoS for MiCollab Client

Use the following procedure to create Group Policy Objects (GPO) in the Local Group Policy on the user machine. Individual policies need to apply QoS for SIP and MiNET softphones because each softphone runs on different applications: SIP on uca.exe and MiNET on UCASoftphoneManager.exe on Legacy MiCollab Desktop Client. IT Administrator can also set policy at Enterprise or Network level using this procedure.

> 🛈 **Note**:
>
> GPO guides the Microsoft OS to grant permission to named programs, allowing the programs to access PC resources according to what the GPO states.

Voice QoS Policy

1. Start the Local Group Policy Editor on the target Windows PC. Type **gpedit.msc** at the Windows Start button. Alternatively, type **Edit Group Policy** at the Start button prompt. Navigate to **Policy-based QoS.**
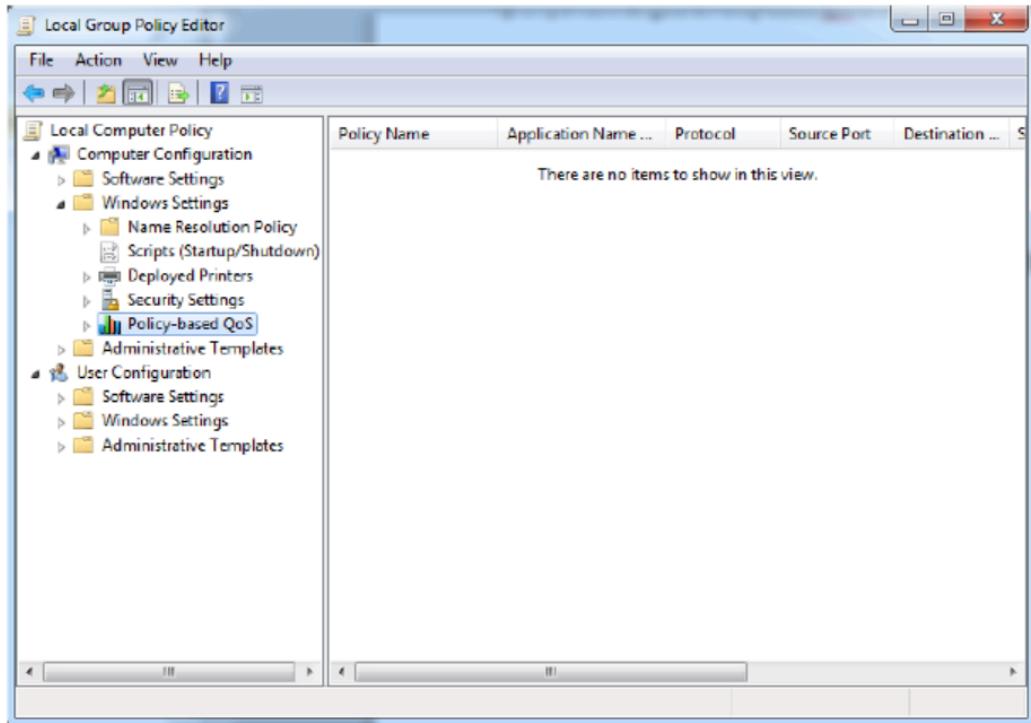
2. Right click **Policy-based QoS** and select **Create new policy…**
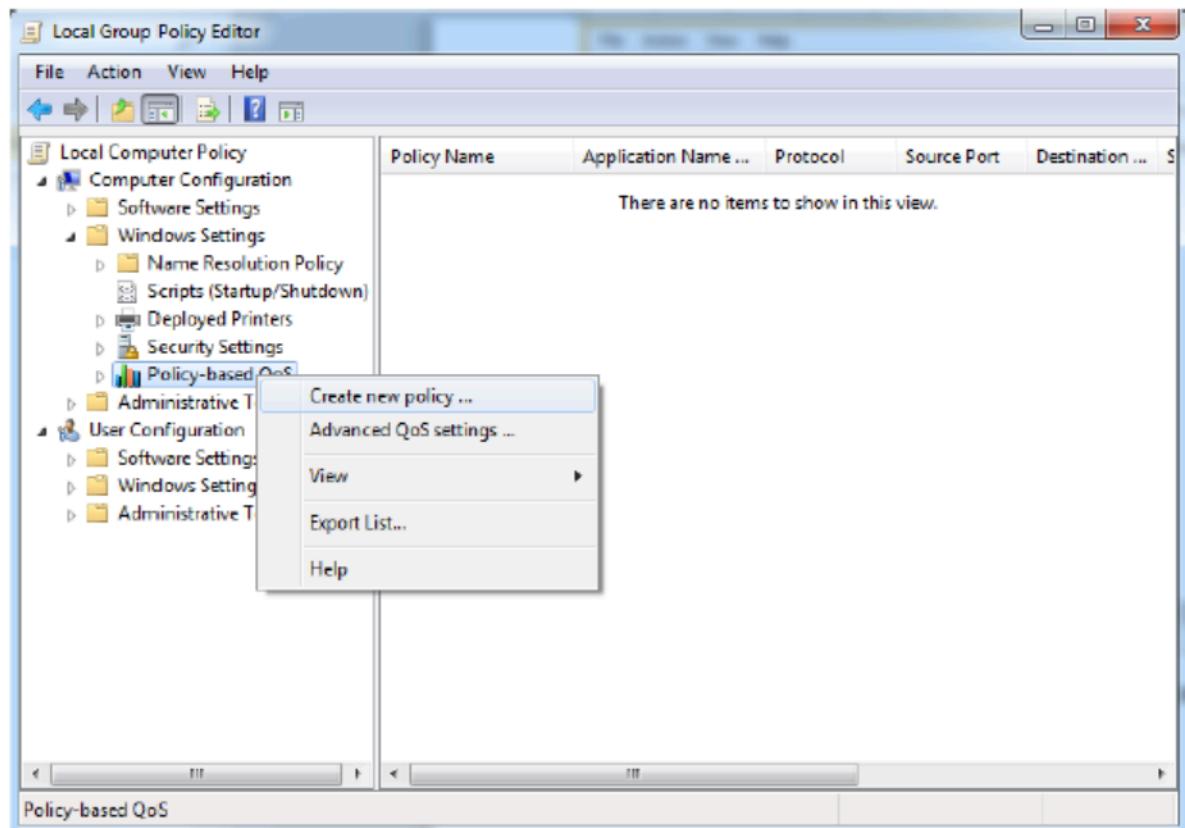
3. Type the **Policy name,** select the **Specify DSCP Value** checkbox and select the **DSCP Value**. Click **Next.**

- Legacy MiCollab Desktop Client: Policy name is UCA.
- MiCollab for PC Client: Policy name is MiCollab.
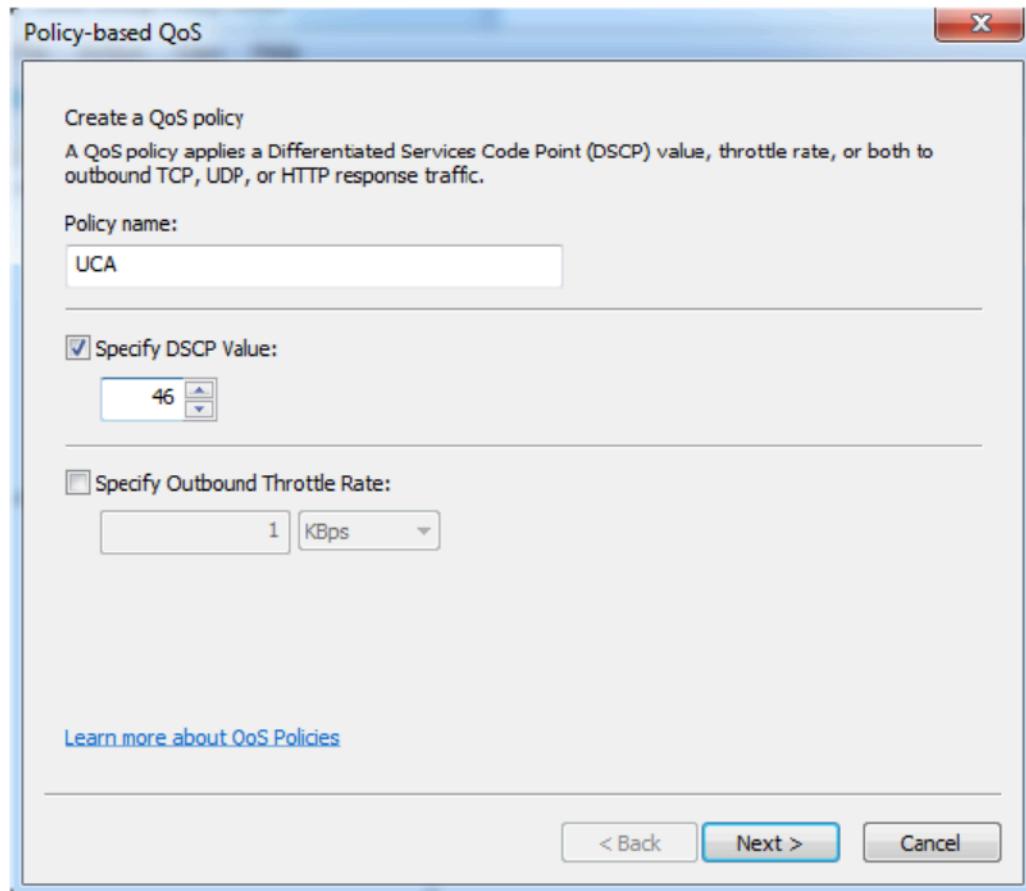
4. Select **Only applications with this executable name**. Type "uca.exe" for SIP softphone, or type "UCASoftphoneManager.exe" for MiNET Softphone. Click **Next**.

- Legacy MiCollab Desktop Client: *UCA.exe* for SIP softphone and *UCASoftphoneManager.exe* for MiNET softphone
- MiCollab for PC Client: *MiCollab.exe*
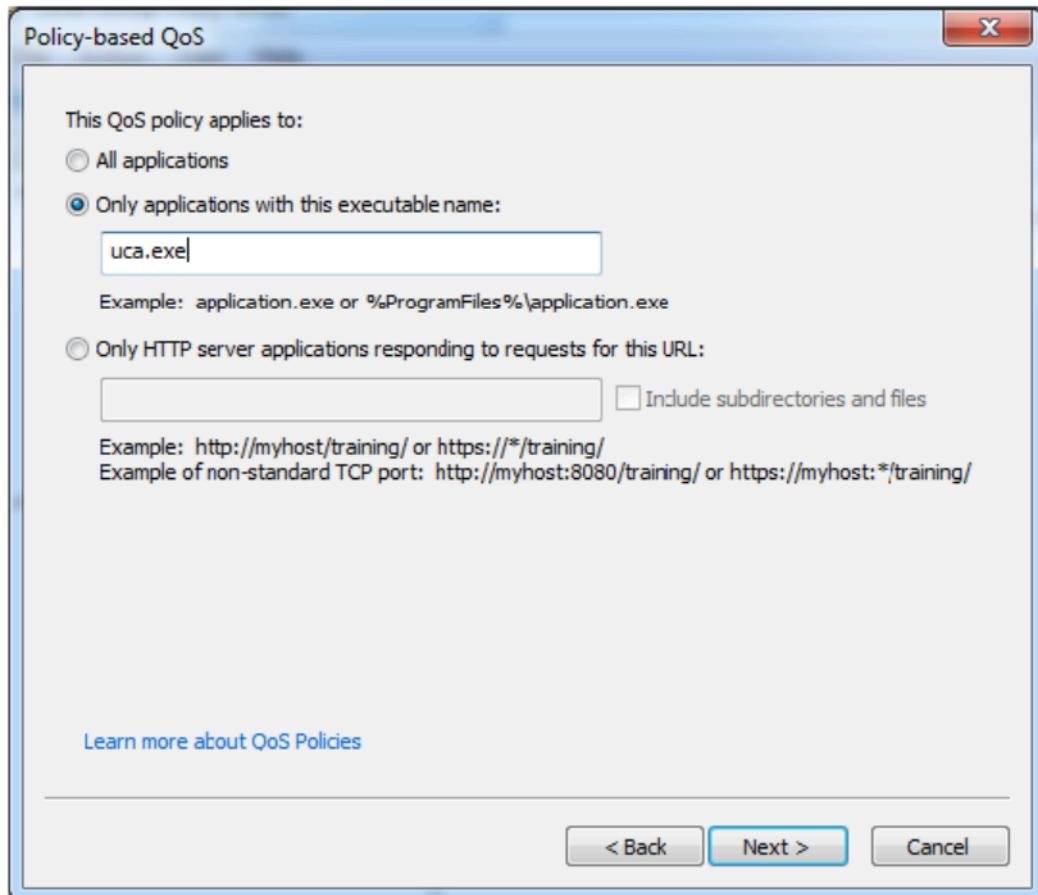
5. The source and destination IP addresses can be left with their default selections. Click **Next**.
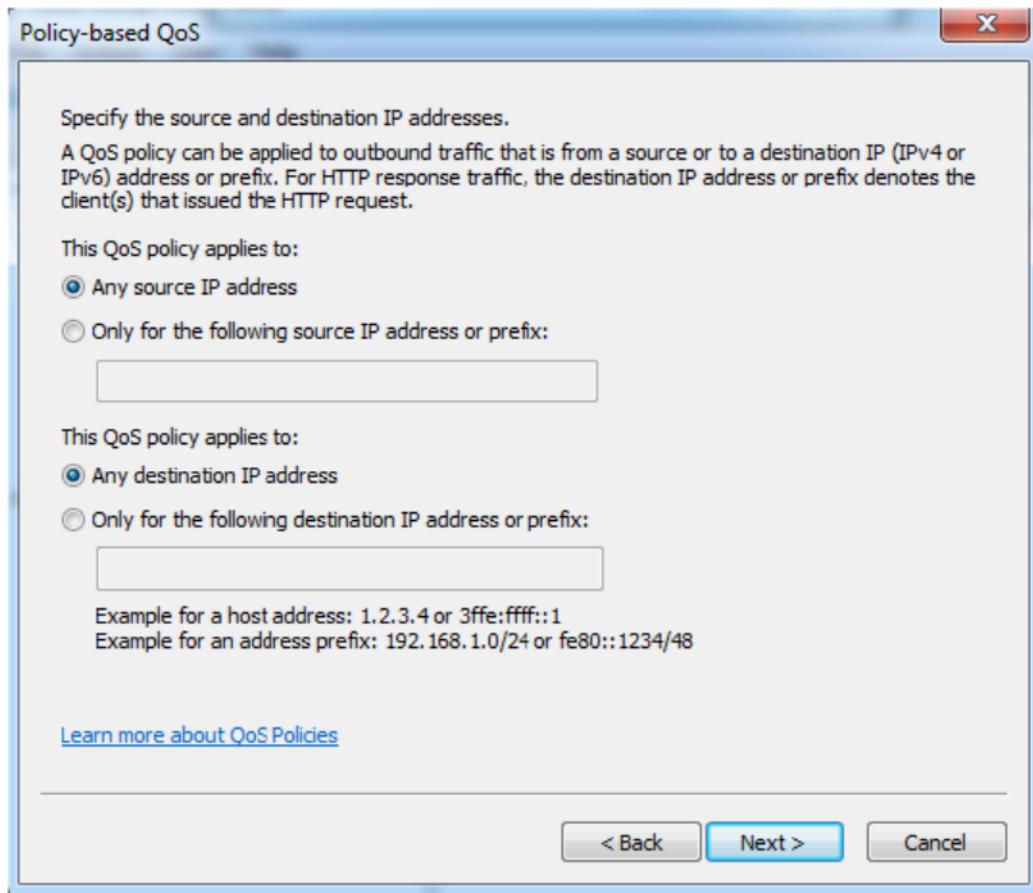
6. Select **UDP** as the protocol. The RTP voice packets are transported as UDP. Optionally, the destination port range can be specified. If desired, refer to *MiVoice Business Engineering Guidelines* for the IP ports range. Click **Next**.
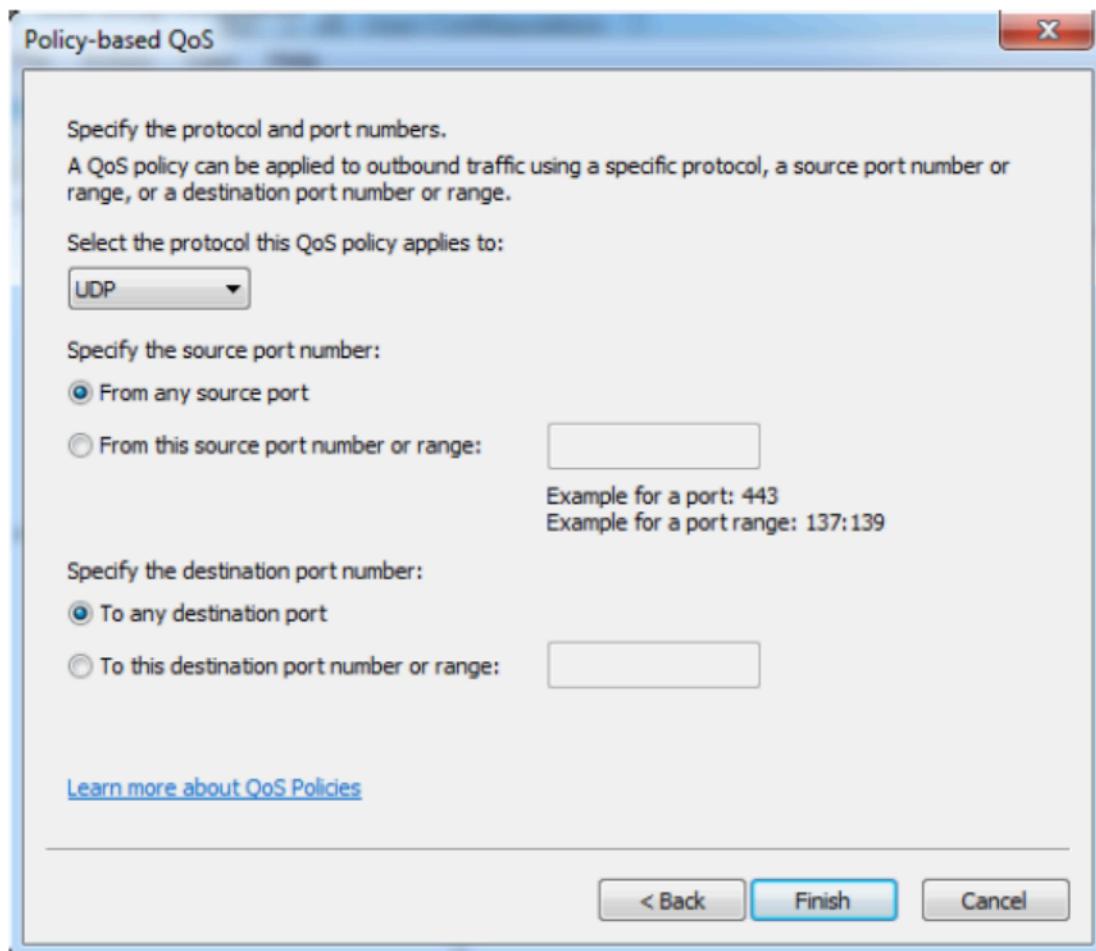
Signaling QoS Policy

Configuring the Signaling QoS Policy procedure is similar to configuring the Voice QoS Policy. Create a new policy, using the previous procedure, with the following changes:

- The Signaling policy uses the **UCA** policy name and a DSCP value of **24**.
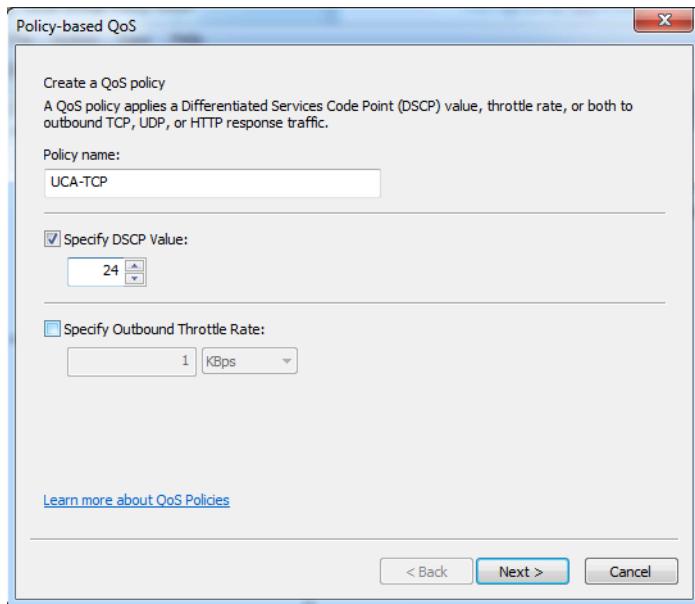
- The signaling for the console happens over TCP, so specify the use of TCP on the last window. Optionally, the destination ports can be specified. If desired, refer to *MiVoice Business Engineering Guidelines* for the IP ports that receive TCP packets between the PC Console and the MiBusiness controller (i.e. MiVoice Business).
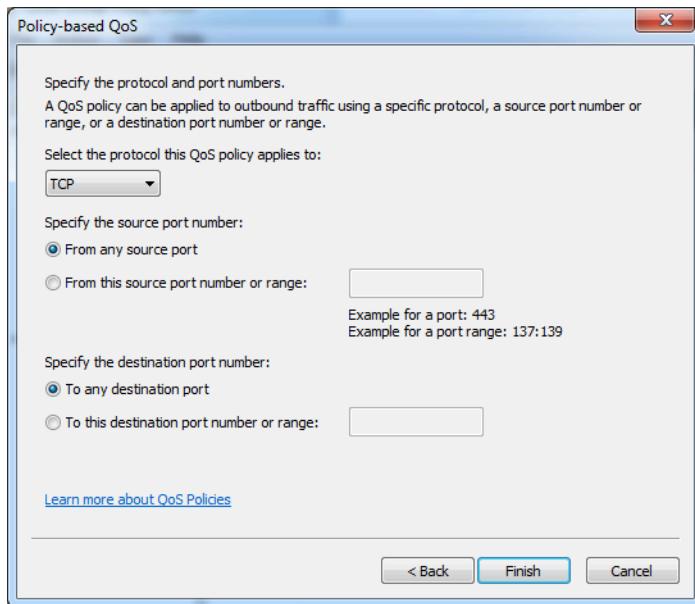
4.15.3   Wi-Fi network qualification

The importance of qualifying a Wi-Fi network for Voice/Video communications has increased with the increasing number of Wi-Fi softphones deployed in enterprises and

the emerging critical nature of work-flows that depend on a quality voice and video experience.

The intent of this section is not to provide step-by-step Wi-Fi deployment instructions, but to provide assessment and deployment guidelines. Installations and their individual challenges are too diverse to address the scope of all deployment concerns. Refer to the documentation provided by your Wi-Fi equipment manufacturer for specific deployment questions.

> **❗ Important**:
>
> **Wi-Fi network qualification is required when deploying MiCollab Desktop and Mobile Clients**. While this section provides key Wi-Fi network design considerations and assessment guidelines, Channel Partners are responsible for ensuring their networks can support real time communications. Additional information about Wi-Fi network considerations / design concepts and Wi-Fi assessment criteria is available on MOL https://www.mitel.com/document-center/. Also, Wi-Fi consulting and network assessment services are available through Mitel Professional Services to assist you. Please contact servicesolutions@mitel.com for more information.

- Wi-Fi network assessment

There are several key criteria to address in order to certify a Wi-Fi network environment for voice and video usage. The level of testing depends on the number of users, location, voice/video Wi-Fi usage, end-user location and movement, as well as the overall level of importance of Wi-Fi based communication to the enterprise.

Consider the following when conducting your assessment:

CHALLENGE	IMPACT
Limited range	Antennas have a large effect on the practically achieved range. A typical wireless access point using 802.11b or 802.11g with a stock antenna might have a range of around 30m indoors and 90m outdoors with no signal interference. Fitting higher gain or directional antennas can increase range, but there are regulations capping the maximum amount of power a Wi-Fi device can radiate, placing Wi-Fi at a comparative disadvantage with other technologies

CHALLENGE	IMPACT
Unlicensed band / Frequency interference	Wi-Fi networks are susceptible to interference, particularly in the 2.4 GHz band, which is used by a large number of other technologies. It can be very challenging, especially in Enterprise environments, to set up a proper Wi-Fi environment that both avoids interference and provides ample capacity. The limited availability of non-overlapping channels makes this even more difficult.
Planning and rolling out large infrastructures	The challenges in large roll outs include RF design and channel planning. The availability of only three non-overlapping channels in the 2.4 GHz makes covering a large campus, or even a multi-story building, very challenging. The often-limited ability of placing access points freely compounds this issue. While the 5 GHz band resolves some of those issues, the increased absorption of 5 GHz frequencies by walls, windows, etc. pose new challenges. Achieving the coverage and capacity required for a real-time communication ready Wi-Fi network therefore cannot be accomplished without proper planning and constant monitoring of the network.

- Wi-Fi infrastructure design considerations

Voice applications are very sensitive to latency, delay, jitter and packet loss.

There are many considerations that impact the performance of real-time capability on the network:

CONSIDERATION	DESCRIPTION	TIPS
Packet loss	Commonly due to interference and capacity issues	**Conduct a Site Survey** One of the key factors in ensuring the success of a Wi-Fi deployment is a proper site survey for commencing the planning. Before deploying your Wi-Fi, understand the users' needs in the current environment. Performing a site survey allows you to identify: • appropriate technologies to apply and frequency bands to use (802.11a/b/g/n, 2.4/5 GHz)

CONSIDERATION	DESCRIPTION	TIPS
		• obstacles for achieving good coverage to avoid, eliminate, or work around • ideal coverage patterns • approximate capacity required Ideally, the result of a proper site survey is a network design document that describes the suggested location of each access, its intended coverage area, and the 802.11a/b/g/n channel selections for the access point. A great deal of information can be obtained from a site survey, but even more important is how that information is analyzed to support cell planning, cell boundary threshold, range and throughput, interference/delay spread, bandwidth management for real-time applications, access point density and load balancing.
Delay	A number of factors contribute to one-way delay of VoIP	Wi-Fi can use only a small portion of the total delay budget
Interference	Data streams overload the Wi-Fi network temporarily saturating the medium capacity and cause delays and losses which impact voice quality	**Consider devices that can cause interference** Wi-Fi interference is an extremely common and troublesome issue. Interference is not only a prime concern in residential deployments where cordless phones, baby monitors and microwave ovens can cause problems, it has an even higher significance in enterprise infrastructures.
Capacity	Actual capacity throughput highly dependent on multiple client usage as interference/packet	**Design for Capacity** Simple site surveys, while guaranteeing coverage; do not guarantee that your organization's capacity or performance

CONSIDERATIO	DESCRIPTION	TIPS
	collisions have a detrimental impact on throughput capacity.	targets will be met. Because of the nature of the shared medium, and the dependence of effective throughput, packet sizes, and number of Wi-Fi clients present, the Wi-Fi traffic characteristics also need to be taken into account to ensure satisfactory performance for all users and applications. In larger deployments where many channels are reused, the Wi-Fi performance can be degraded by co channel interference, and a simple site survey, while verifying a specific data rate with no interfering traffic, may not take into account the data rate reduction due to the increase in noise from additional channels.
Roaming	The ability of devices and Wi-Fi access points to handle movement across multiple cells over a specific period of time	Design for CoverageMobility is a major reason that companies go wireless. Yet many discover that the wireless coverage is insufficient, hampered by dead-spots or has inadequately sized overlap of coverage between access points.
Network infrastructure	Connected Wi-Fi Access points must have sufficient capacity to support voice, video as well as data traffic	Connected Wi-Fi access points must have sufficient capacity to support voice, video as well as data traffic
Overlap	Multiple Wi-Fi Cells and Frequency Overlap	

4.15.4   MiTAI Monitor usage

The MiCollab Client Service sets up MiTAI monitors for all the numbers in a user's Personal Ring Group (PRG). When there is no PRG, it sets up MiTAI monitors for the desk phone and/or softphone. Also for every button programmed as multi-call or key line on an IP phone, the MiCollab Client Service sets up a MiTAI Monitor. This adds some

overhead processing to the ICP. "MiCollab Client System Capacities: MiCollab Client Standalone" provides some examples of the number of MiTAI monitors used. This table assumes each user has a PRG with 2 numbers. It also assumes each of the phones do not have buttons programmed as key lines or multi-call.

> **ⓘ Note**:
>
> The target number cannot be monitored more than 16 times. Maximum of 16 monitors can be allocated to a single DN. For more information about call control functionality, see *MiT AI Driver Developer Guide*.

4.16   Ports used by MiCollab Client Service

MiCollab Client Service binds to the following ports to provide the various features to the MiCollab Client desktop and mobile clients. Please note that the list below only refers to ports that MiCollab Client Service listens on for incoming client connections. For full details on ports to which MiCollab Client Service connects to with other servers refer to figure 5 and 6 in this document.

- TCP Ports 18100, 18101, 18102, 18103, 18104, 18105, 18106, 6070, 1099, 5106, 5347, 5269, 36009 and 36008
- UDP ports 18101, 18102,18103,18104,18105, and 18100

Details

- 18100 (TCP and UDP) - SIP port used by SIP_PROXY
- 18101 (TCP and UDP) - SIP ports used by ACCTPRES module
- 18102 (TCP and UDP) - SIP ports used by PRES module
- 18105 (TCP and UDP) - SIP ports used by SIPREG module
- 18103 (TCP and UDP) - SIP ports used by IM_EVENTS module
- 18104 (TCP and UDP) - SIP ports used by SIPIMS module
- 18106 (TCP) - SIP port used by WSP module
- 6070 (TCP) - SIP port used by FEDERATION_GW module
- 5106 (TCP) - port used for inter-module communication in MiCollab Client (called MBUS). Proprietary protocol
- 1099 (TCP) - For java naming service (JNDI) by JBOSS module
- 5269 (TCP) - for XMPP protocol by third party library called Prosody
- 5347 (TCP) - for XMPP protocol by FEDERATION_GW module
- 36008 (SSL/TCP) - Port used by web socket protocol

- 36009 (SSL/TCP) – Port used for MiCollab Client Service peering
- 443 (HTTPS 443) – For web services access by MiCollab Desktop, Web and Mobile clients and MiTeam Cloud-based solution

> **ℹ Note**:
>
> To support the iOS Push Notification, the MiCollab server connects to the Apple server *api.push.apple.com:443* on port 443. Also, if you are using Wi-Fi behind a firewall on your iOS device, the iOS device requires a direct, unproxied connection to the Access Point Name (APN) servers on ports 5223, 2195, 2196, and 443 to use iOS Push Notification service.

- 80 (HTTP) – For Exchange calendar integration
- The audio port ranges from 50098 to 50508 for Legacy MiCollab Desktop Clients and 55004 to 55505 for MiCollab for PC Clients.
- The video port range is from 50000 to 50501 for MiCollab for PC Clients. RTCP uses the RTP+1 port.

> **ℹ Note**:
>
> In the MiCloud solution, MiCollab Client Service listens to the management services on port 35600.

> **ℹ Note**:
>
> The amount of simultaneous calls is limited by the availability of video ports. MiCollab Client SIP Softphone calls will use audio as well as video ports, regardless of video being used. See the *MBG Online Help > Configure Port Ranges* for more information on the port ranges.

4.17 Heap Memory Configuration to support more than 2500 users

To provision MiCollab Client Service for more than 2500 users, the heap memory of the WSP module needs to be increased. Commands to increase heap memory to 768 MB, are as follows:

- db configuration setprop ucserver-ws HeapMax 768m
- expand-template /opt/intertel/bin/startWsp.sh
- restart_module WSP

Table 19: Recommended Heap Memory Configuration

Application	Minimum software level or service pack requirements
2500 (5000 Clients)	512 MB
4000 (8000 Clients)	768 MB
5000 (10000 Clients)	1024 MB

MiCollab Client Service is tested up to 5000 users and 10000 clients only.

4.18 Heap Memory Configuration to support 15000 users

To provision MiCollab Client Service for 15000 users, the heap memory of the DSM module needs to be increased. Commands to increase heap memory to 512 MB, are as follows:

- db configuration setprop ucserver-dsm HeapMax 512m
- expand-template /opt/intertel/bin/startdsm.sh
- restart_module DSM

4.19 Disable "Forgot My Password" mechanism

Due to security concern, we have provided an option in MiCollab Client Service to disable "Forgot My Password" mechanism. After disabling this, user will not able to reset password and need to contact administrator for resetting the password.

By default this mechanism will be enabled. Command to disable "Forgot My Password" mechanism is as follows:

- serviceproperty setsystemsvcprops props=forgot_my_password_service_enabled\;f
- Command to enable "Forgot My Password" mechanism
- serviceproperty setsystemsvcprops props=forgot_my_password_service_enabled\;t

Appendix A –Configuration of XMPP federation (example)

This section shows an example configuration of XMPP federation with the Skype for Business Server 2015.

In the example below, the following scenario is assumed:

- Company ABC owns "abc.com" domain and is configuring its MiCollab Client Service, "micollab.abc.com".
- Company XYZ owns "xyz.com" domain and uses Skype for Business 2015.
- Company ABC wishes to configure Skype for Business Server 2015 federation with company XYZ.
- Domain Name Service (DNS) SRV records are used to determine the IP addresses of the XMPP servers by resolving their FQDNs. Skype for Business Server federation uses a server-to-server connection over TCP port 5269. For more information about XMPP, consult RFC 3920. Both the MiCollab Client Service and the Skype for Business Server act as XMPP servers. The recommended setup on the DNS servers (the external DNS in figures 10 and 11) used by the Skype for Business Server to resolve the MiCollab Client Service FQDN is shown below.

- User from XYZ wants to federate with user from ABC

  1. The initiating entity constructs a DNS SRV query whose inputs are:

     - A Service of "xmpp-server" (for server-to-server connections)
     - A Proto of "tcp"
     - A Name corresponding to the "origin domain" of the XMPP service to which the initiating entity wishes to connect (e.g., "abc.com")
  2. The result is a query such as "_xmpp-server._tcp.abc.com".

If the initiating entity is UserX@xyz.com and it wants to talk to UserA@abc.com, XYZ's Skype for Business Server 2015 would construct a DNS query for _xmpp-server._tcp.abc.com and the DNS server would respond with the XMPP server FQDN ("micollab.abc.com") and the IP address from an A record lookup of the FQDN. If no SRV record exists, company XYZ's XMPP server (the Skype for Business Server 2015) performs a normal A record query. In this case, the A record lookup needs to return company ABC's XMPP server (the MiCollab Client Service). If no SRV record exists for XMPP, XYZ's XMPP server will query the A record for abc.com and will probably get an IP address that doesn't belong to company ABC's MiCollab Client Service. If this happens, the connection will fail.

DNS SRV Query: _xmpp-server._tcp.abc.com

```
Non-authoritative answer:

_xmpp-server._tcp.abc.com SRV service location:

priority = 0

weight = 0

port = 5269

svr hostname = micollab.abc.com

micollab.abc.com internet address = XXX.XXX.X.XX
```

Company XYZ's Skype for Business Server 2015 would then use IP address XXX.XXX.X.XX (which belongs to company ABC's MBG) to contact the XMPP server used by company ABC (the MiCollab Client Server).

- User from ABC wants to federate with user from XYZ

    - The initiating entity constructs a DNS SRV query whose inputs are:

        - A Service of "xmpp-server" (for server-to-server connections)
        - A Proto of "tcp"
        - A Name corresponding to the "origin domain" of the XMPP service to which the initiating entity wishes to connect (e.g., "xyz.com")
    - The result is a query such as "_xmpp-server._tcp.xyz.com".

      ```
      Non-authoritative answer:

      _xmpp-server._tcp.xyz.com SRV service location:

      priority = 20

      weight = 0

      port = 5269

      svr hostname = lync.xyz.com

      lync.xyz.com internet address = XXX.XXX.X.XXX
      ```

Company ABC's MiCollab Client Server would then use IP address XXX.XXX.X.XXX to contact the XMPP server used by company XYZ.

Appendix B – Installing Lync 2013 server

System set-up

Windows 2008 R2 with SP1.

Prerequisites

Some of the prerequisites for the Lync system are:

- One AD server (installed on 64bit Windows server 2008/2012R2) and one Lync Server O/S (installed on 64bit Windows server 2008/2012R2)
- Windows Server 2008 R2 SP1/ Windows Server 2012 should be installed on the Front-End Server.

> **ℹ Note**:
>
> The Front-End server provides links and services for user authentication, registration, presence, etc. and this is part of the Lync server installation.

- The system on which the Lync Server would be deployed should be in the Lync Server domain.
- The following roles should be running on the AD Server:

  - AD-DS (Directory Services)
  - DNS
  - AD-CS (Certificate Authority)
- Create a user lyncfe in the AD.
- Install the following software on Lync Sever O/S by logging in as system administrator.

  - .Net Framework 4.5 or above
  - Silverlight 4.0 or above
  - Windows Powershell 3.0 or above
  - Windows Identity Foundation
  - Windows6.1-KB2646886-v2-x64

- Setup

  - AD Server: ad.ucs.com/10.112.87.220
  - Lync Server: lyncfe.ucs.com/10.112.87.221

Front-end server setup

1. Go to **Start > Run** and enter **Server Manager**.
2. Under the **Roles** section, add the following Web Server (IIS) roles and services:

   - Common http features installed

     - Static
     - Default doc
     - Https errors
   - Health and diagnostics

     - Http logging
     - Logging tools
     - Tracing
   - Performance

     - Static content compression
     - Dynamic content compression
   - Security

     - Request filtering
     - Client certificate mapping authentication
     - Windows authentication
   - Management Tools

     - IIS management console
     - IIS management scripts and tools
   - Application development

     - ASP.NET 3.5
     - ASP.NET 4.5
     - NET extensibility 3.5
     - NET extensibility 4.5
     - ISAPI extensions
     - ISAPI Filters

3. Add the following features in the Feature section:

- Message Queuing | Message Queuing Services
- Remote Server Administration Tools | Role Administration Tools | AD DS and AD LDS Tools
- User Interfaces and Infrastructure | Desktop Experience
- Windows Identity Foundation 3.5
- .NET Framework 3.5 Features
- .NET Framework 3.5
- HTTP Activation (Important!)
- Non-HTTP Activation
- .NET Framework 4.5 (all options)

4. Add the following roles:

- AD DS
- AD LDS

5. Reboot the Front-end server and login as lyncfe.

Installing Lync Server 2013

Below are examples with screenshots that provide guidance for installing the Lync Server 2013.

- Insert the CD and Run Setup.exe. You will be prompted to install Visual C++, click Yes.(as shown in the following figure)
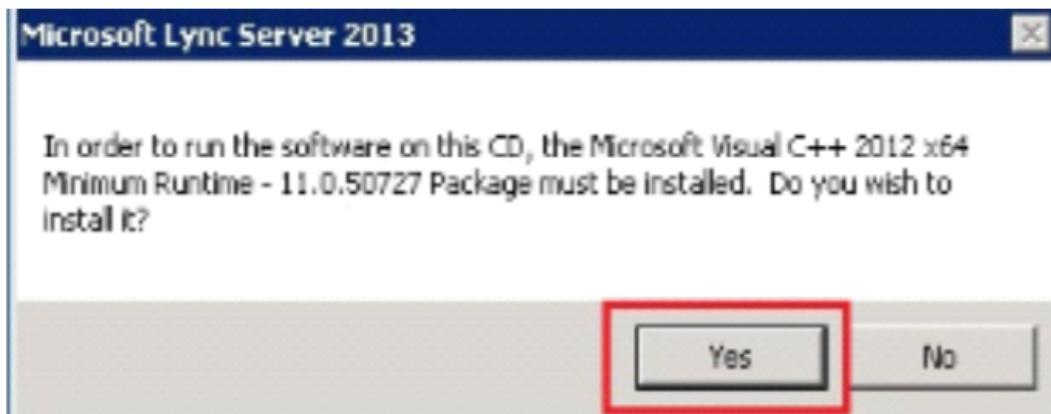
- You can accept the default location or choose the location where you want to install and then click on the **Install** button.

- Accept the Terms and click on **OK** to install.

When installation is complete the apps below on your server and the Lync Server Deployment Wizard will appear.

- Lync Server Manager
- Lync Server Deployment Wizard

Prepare Active Directory

• Click on Prepare Active Directory link in the deployment wizard.
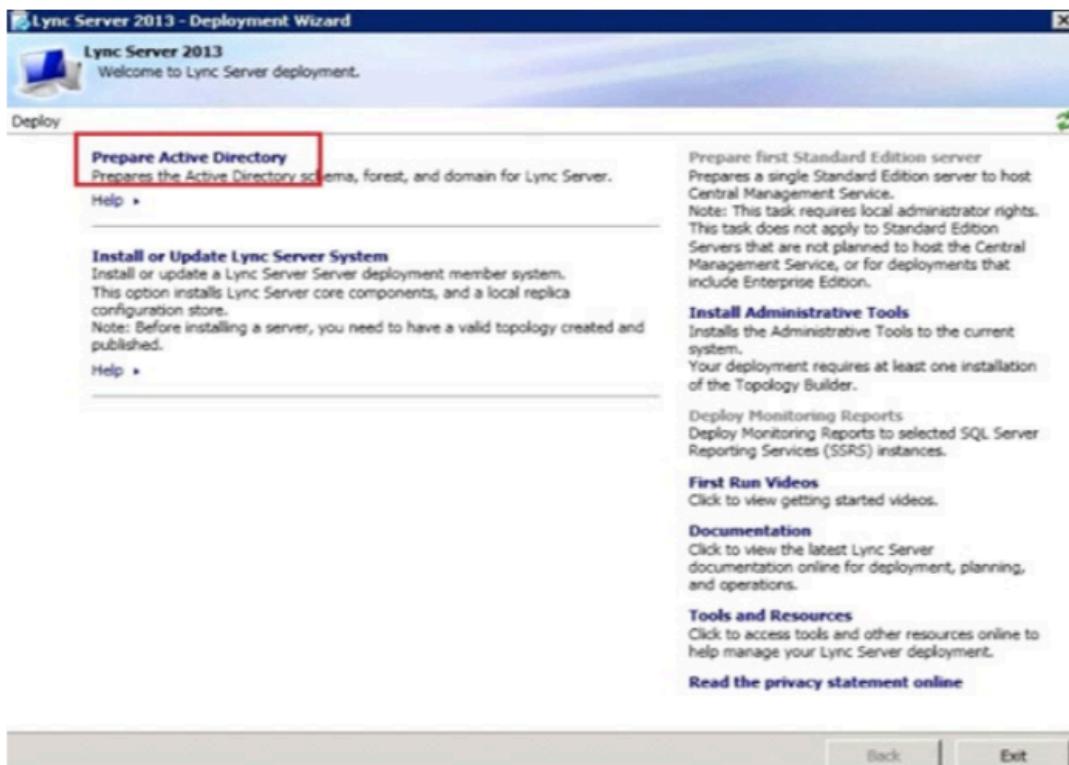
- **Step 1:** Prepare Schema.

  Step 2: The Verify Replication of Schema step is not necessary if this is a lab setup and there is only one AD server. You can skip this step and go to step 3.

  Step 3: Prepare **Forest > Next > select Local Domain > Next Button**.

  Step 4: Prepare **Domain > Next Button**.

  Step 5: Add Administrator to the following groups: CS Administrator, RTC Universal Server Admin and Group Policy Creator Owners
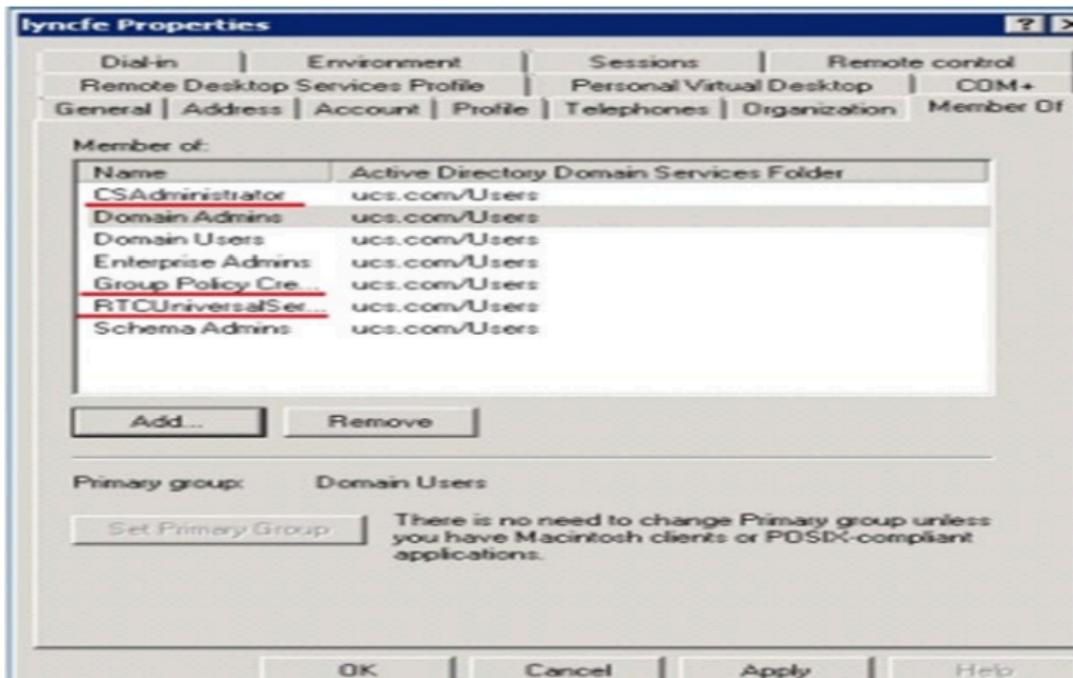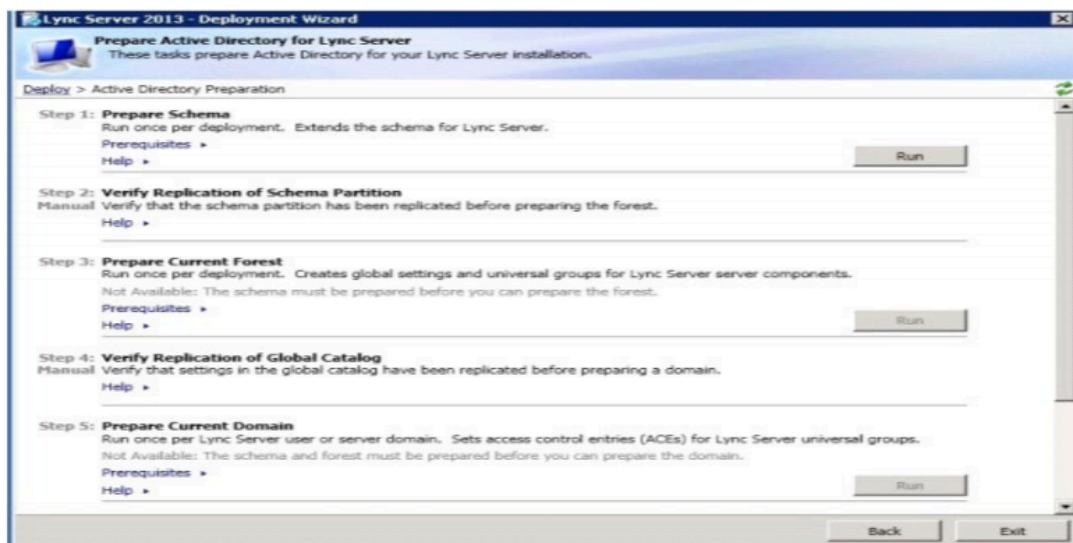
Prepare first standard edition server

In the Deployment Wizard, click **Prepare first Standard Edition server**.

You will see the **Prepare single Standard Edition Server** wizard window. Click **Next**.

During this process the following will be installed:

- SQL Server 2008 Express Edition
- RTC databases will be created and populated
- Lync Server installation files will be put in place

> **ℹ Note**:
>
> As noted in prerequisites, Windows Identity Foundation 3.5 must be installed for this process for successful completion.
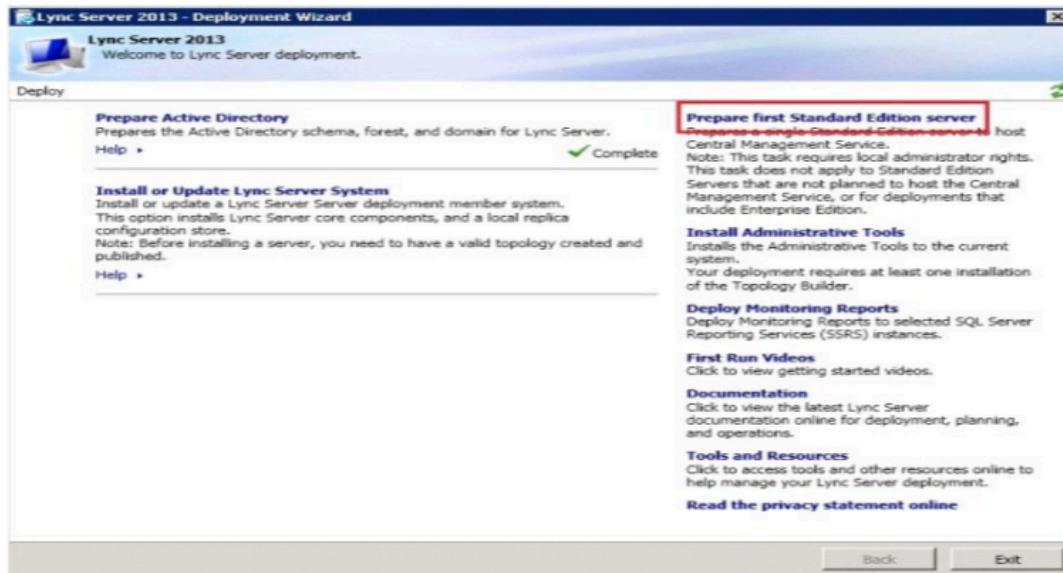
Configure DNS record

- Open **DNS Manager** on AD server.
- Right-click on your domain (in our case ucs.com) under Forward Lookup Zones.
- Click **Other New Records** and scroll down to **Service Location (SRV)**.

- Click **Create Record**.
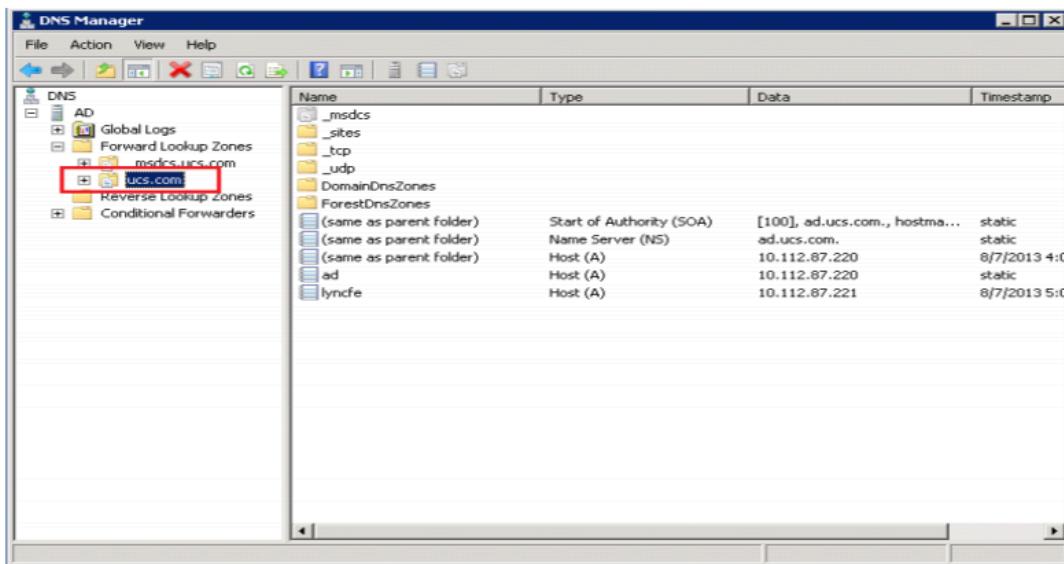
- Enter the following details:

  - Protocol = _tcp
  - Service = _sipinternaltls
  - Port number = 5061
  - Host Offering the service = fqdn of Lync Std. FE server or Pool. (In our caselyncfe.ucs.com)
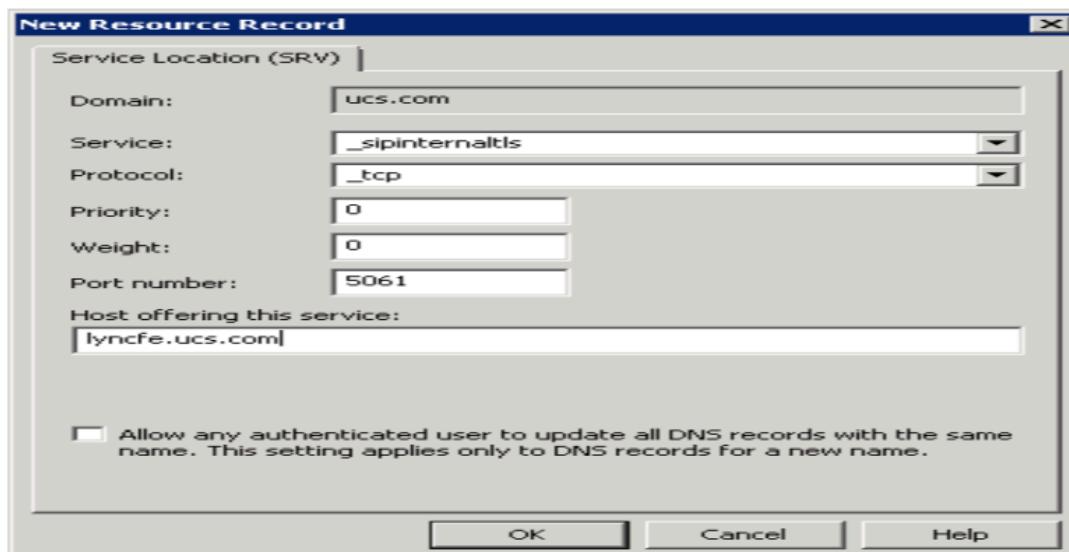
- Create 3 DNS A Records.
- Right-click and select New Host (A or AAAA)

- Add a DNS A record for :

  - Meet
  - dialin
  - admin

  Name: meet/dialin/admin

  IP address: IP address of Lync Server (In our case 10.112.87.221)
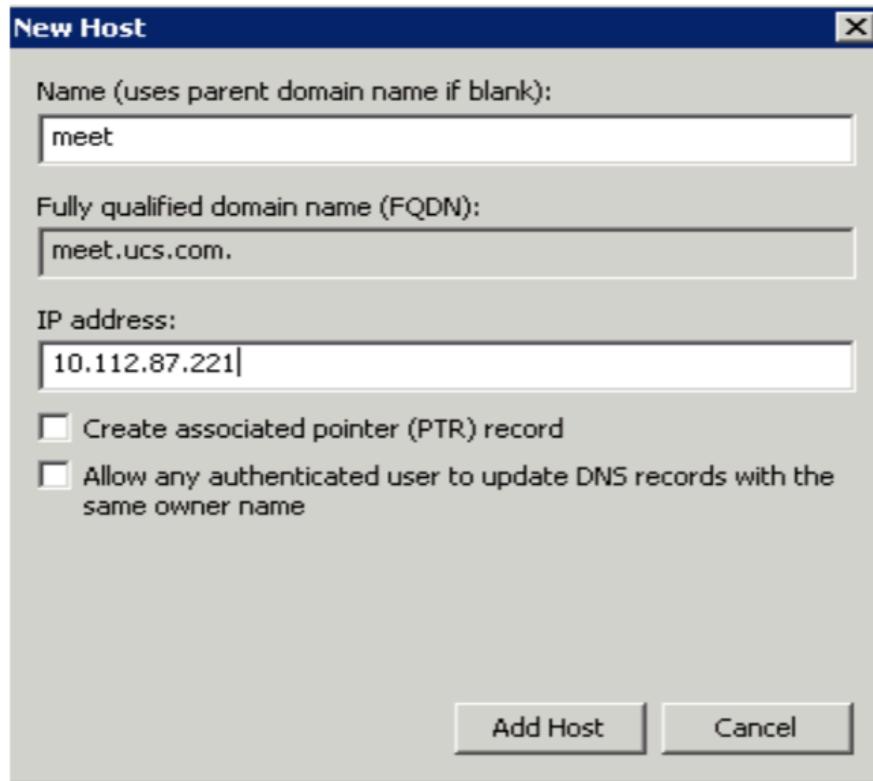
- Return to the Deployment Wizard on Lync Server and click **Install Administrative Tools**.

  This takes just a second to run.
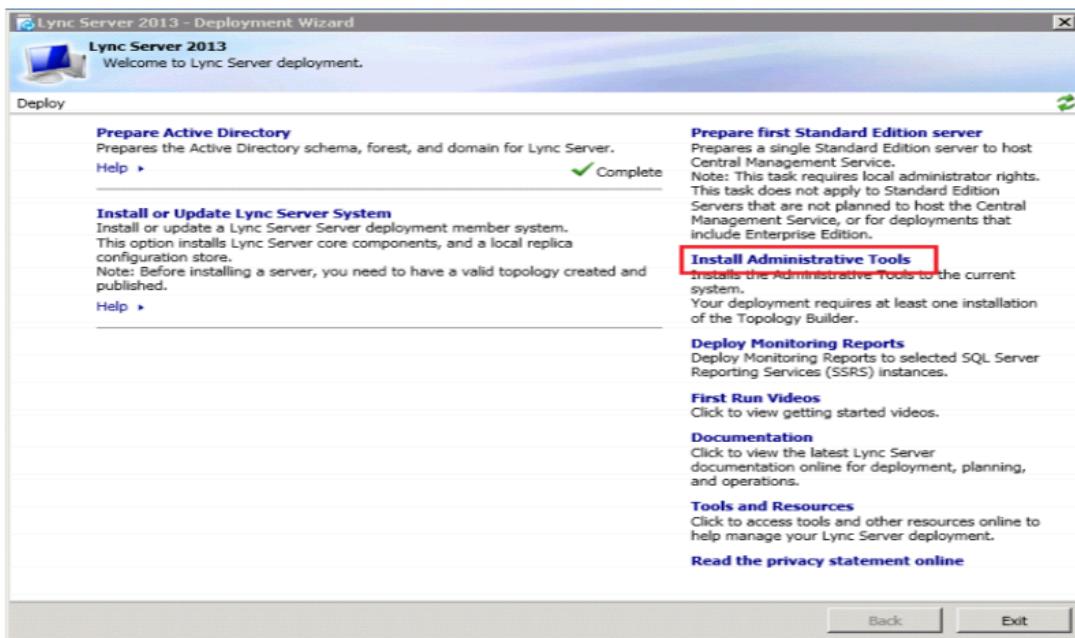
Build and publish topology

- Start and run **Lync Server Topology Builder** from the program menu with **run as administrator**.

- Select **New Topology** and then add a topology name (e.g. plugin.tbxml)
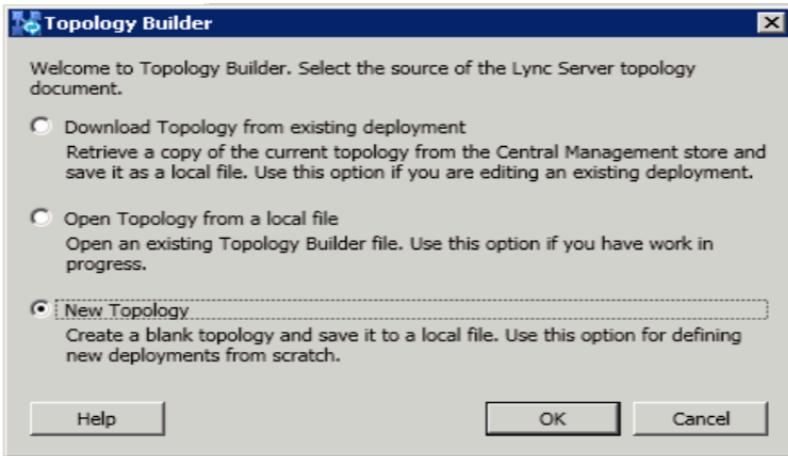
- Add Primary SIP domain as: ucs.com and click **Next** button.
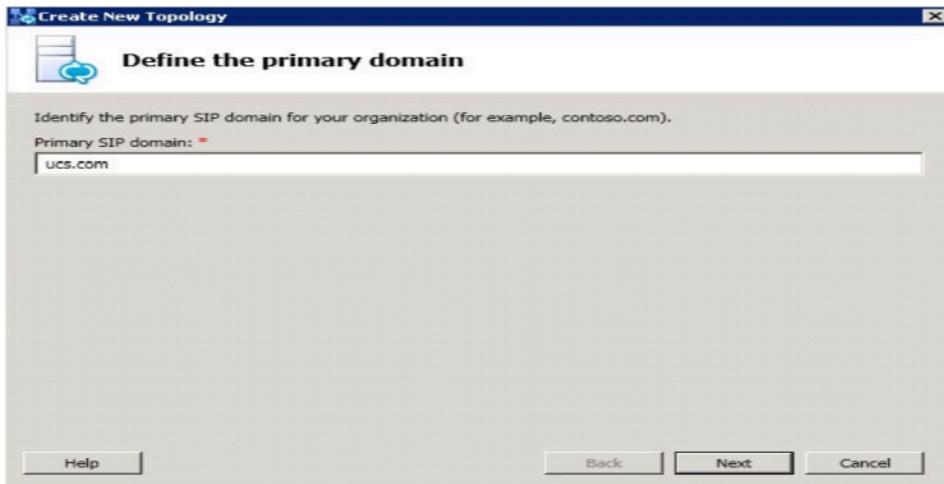
- Specify additional supported domains: **Remains Empty > Next Button**.

- Define the First site

  - Name: Lync Plugin
  - Description: Lync Plugin (not mandatory)
  - Click on Next button
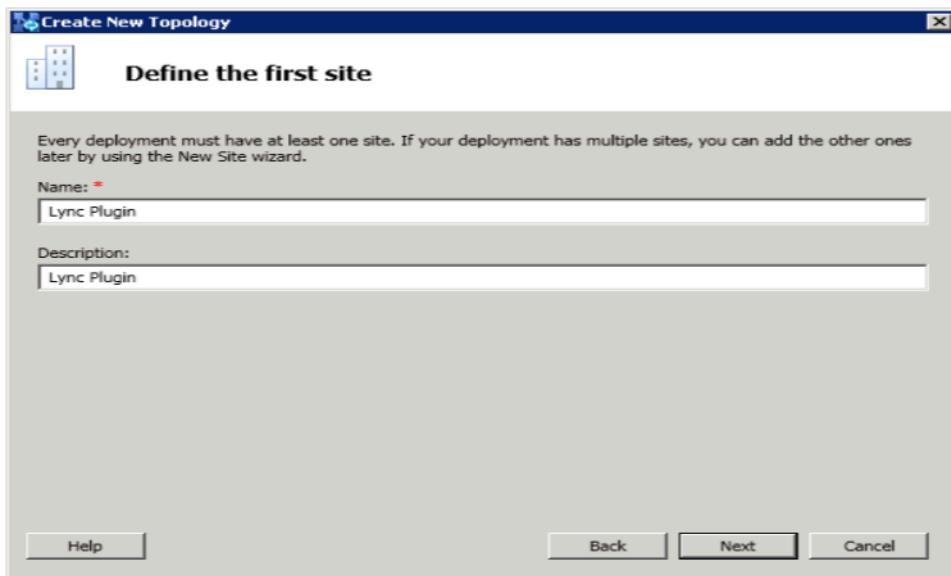
- Specify site details

  - City
  - State
  - Country
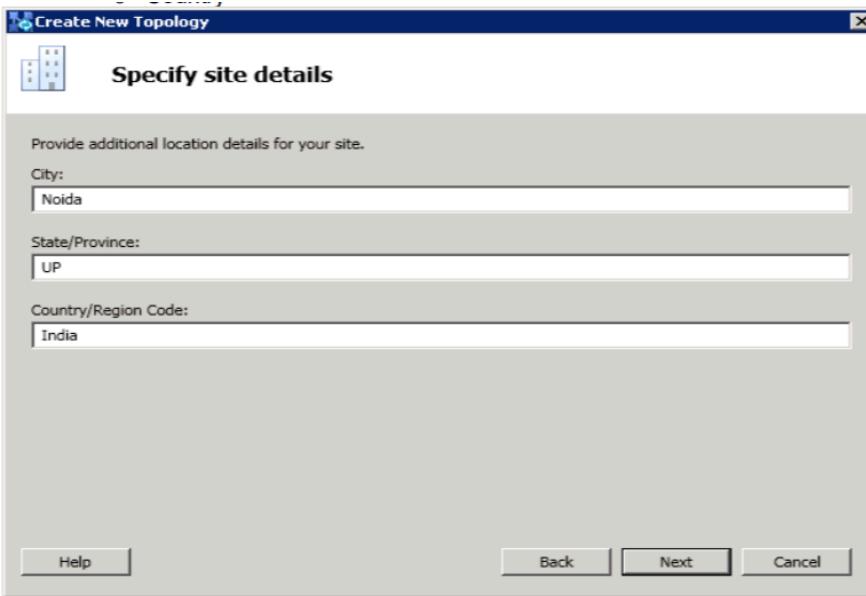
- Click Finish.
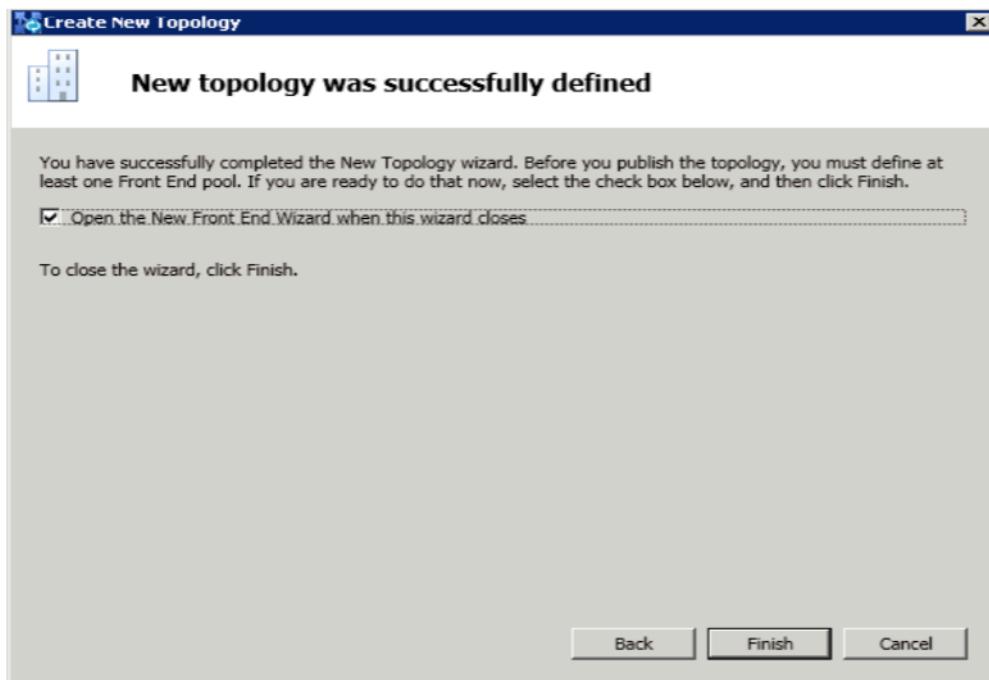
- Define a new Front-End pool. Click Next.

- FQDN: lyncfe.ucs.com

> **ℹ Note**:
>
> If this is a Standard Edition, this FQDN will be the same FQDN as your FE server(lyncfe.ucs.com in this case).
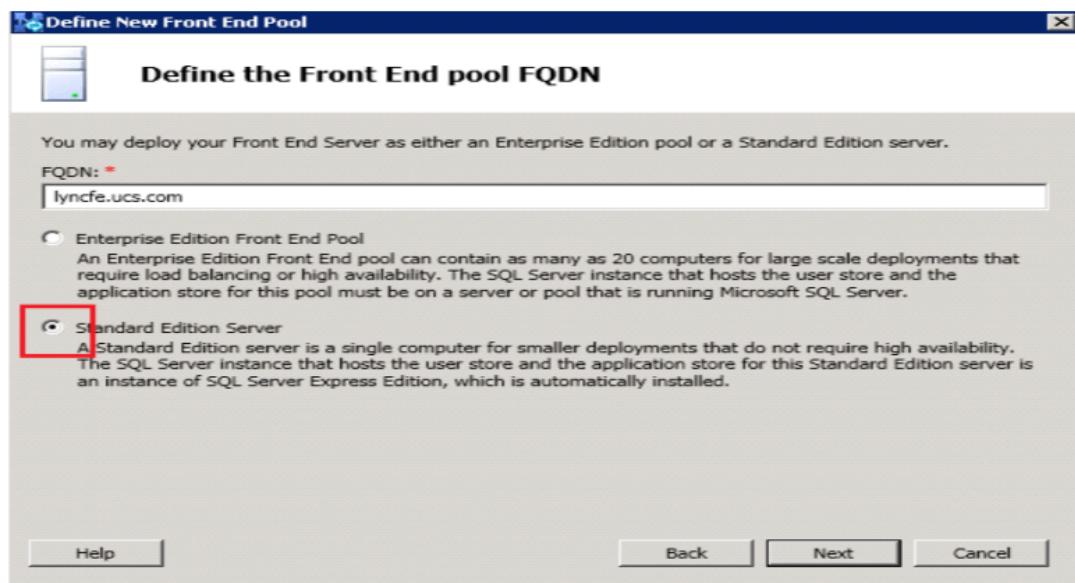
- Select the following features for the Front End Pool and click Next.

  - Conferencing
  - Enterprise Voice
  - Call Admission Control (CAC)
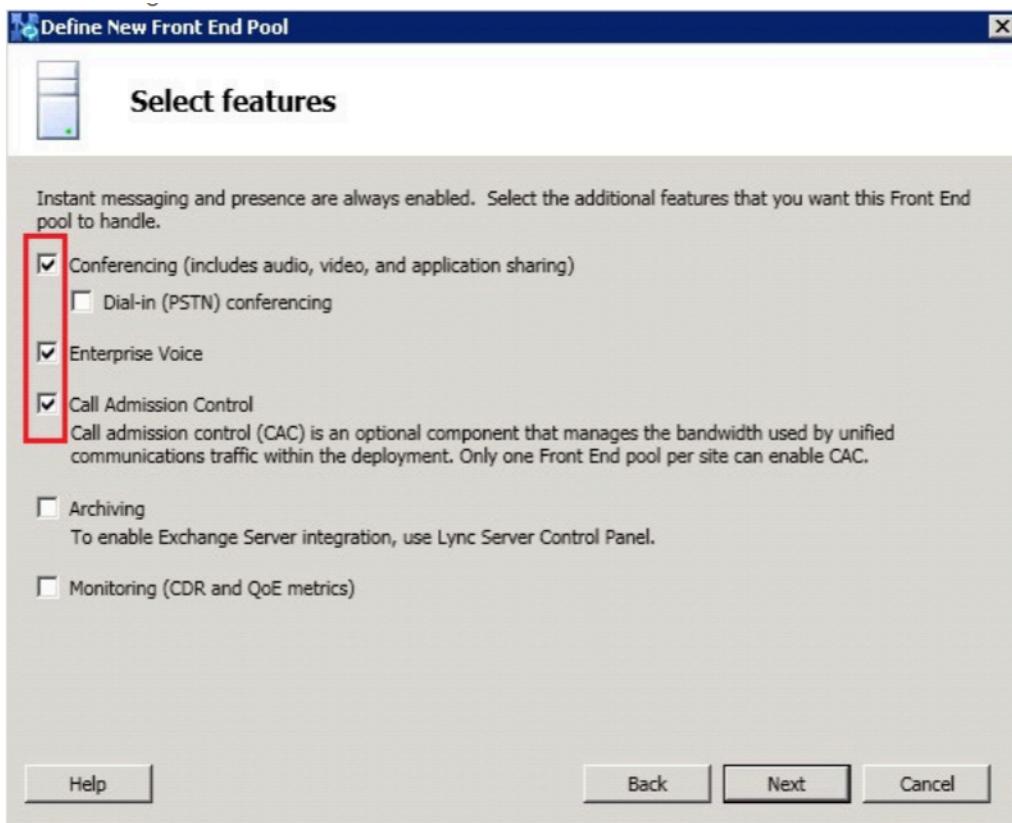
- Check **Collocate Mediation Server** check box on the Select collocated server roles page.
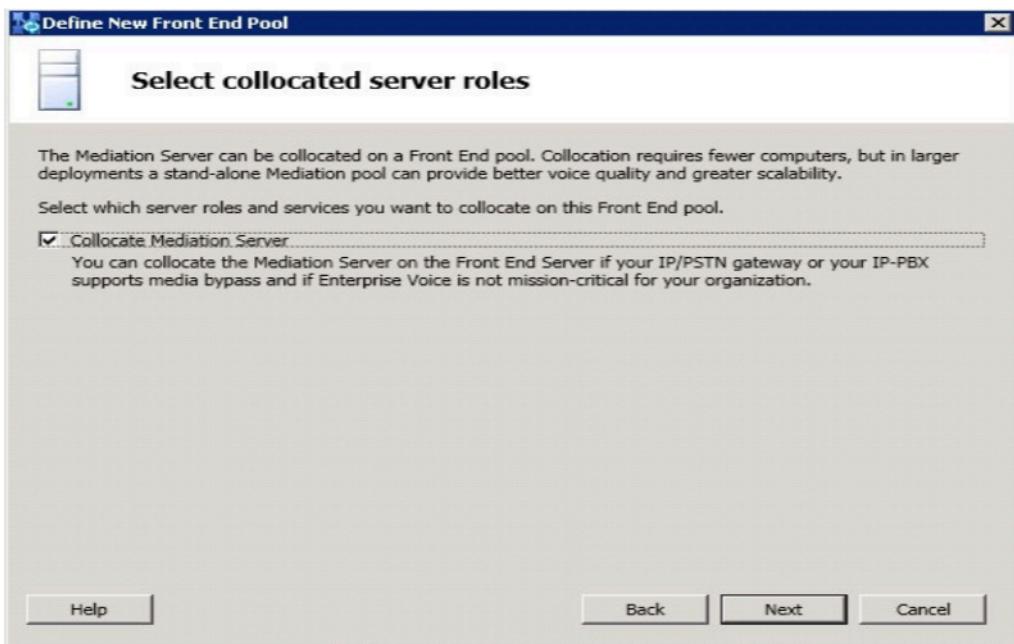
- In the **Associate server roles with this Front End pool** page, the **Enable an Edge pool** checkbox should remain unchecked.

  Then click the **Next**button.

- In the **Define the SQL Server Store** page, click on **Next** button.
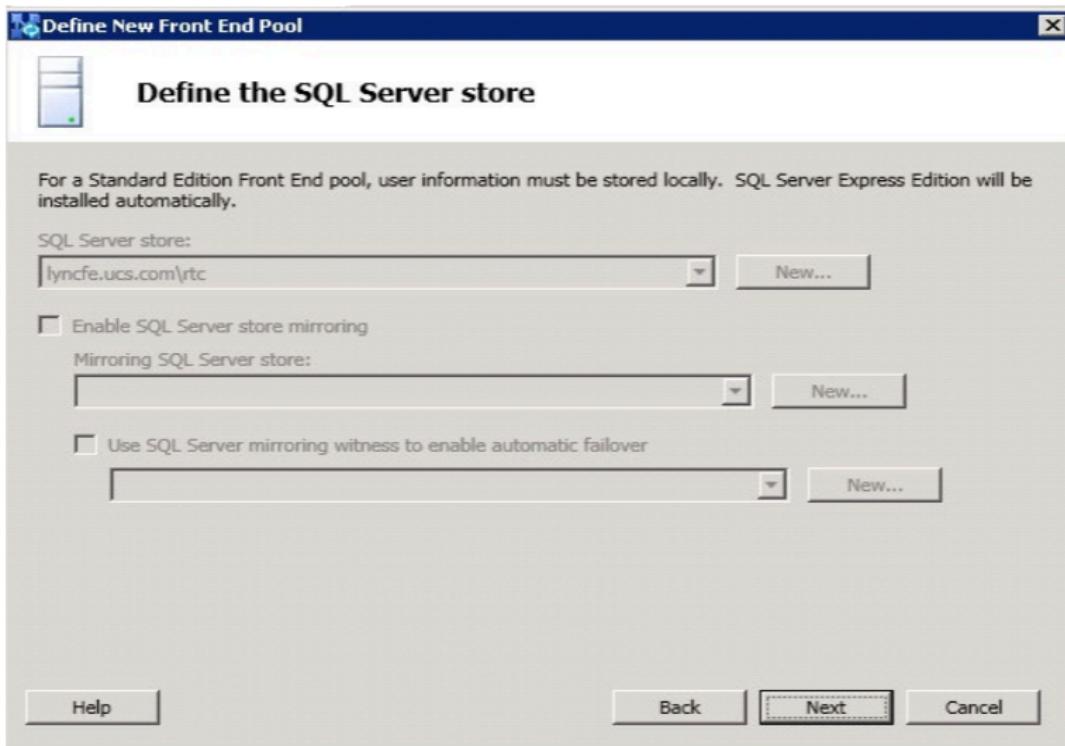
- You can create a folder in any location, but in this setup create a folder called **Share** in <u>C:\</u> <u>of the Lync Server</u>.

  Next go into the properties of the folder and give full access permissions to these groups:

  - RTCHS Universal Services
  - RTC Component Universal Services
  - RTC Universal Server Admins
  - RTC Universal Config Replicator
  - Administrator
  - Everyone

  Click on the **Sharing** tab, click **Share**.
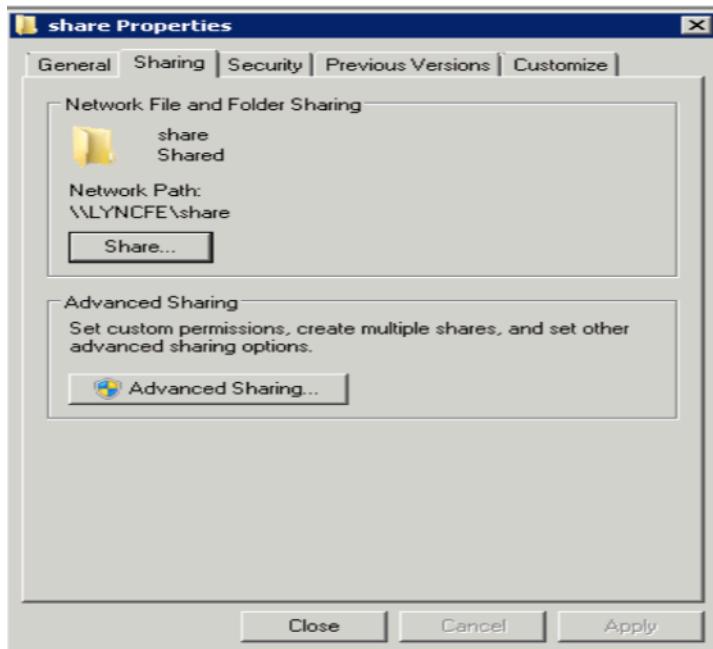
- In the File Sharing Wizard, click the dropdown beside Add and select **Find People** and in **Enter the object names** to select type **RTC**. Now press the CTRL key and select the

above groups. Next you will need to change each group to Read/Write and click Share to finish the sharing Wizard.
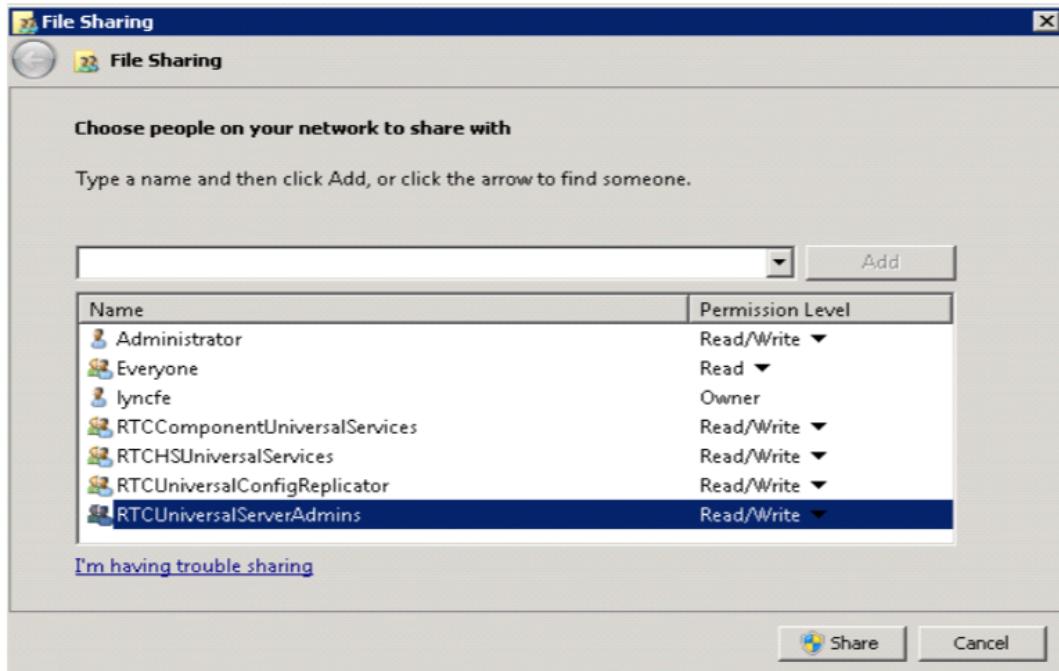
- Now click on **Advanced Sharing** > **Properties** and provide full access to all groups except Everyone.
- Specify the web services URL: Since this is a lab we can let the External Base URL the default.
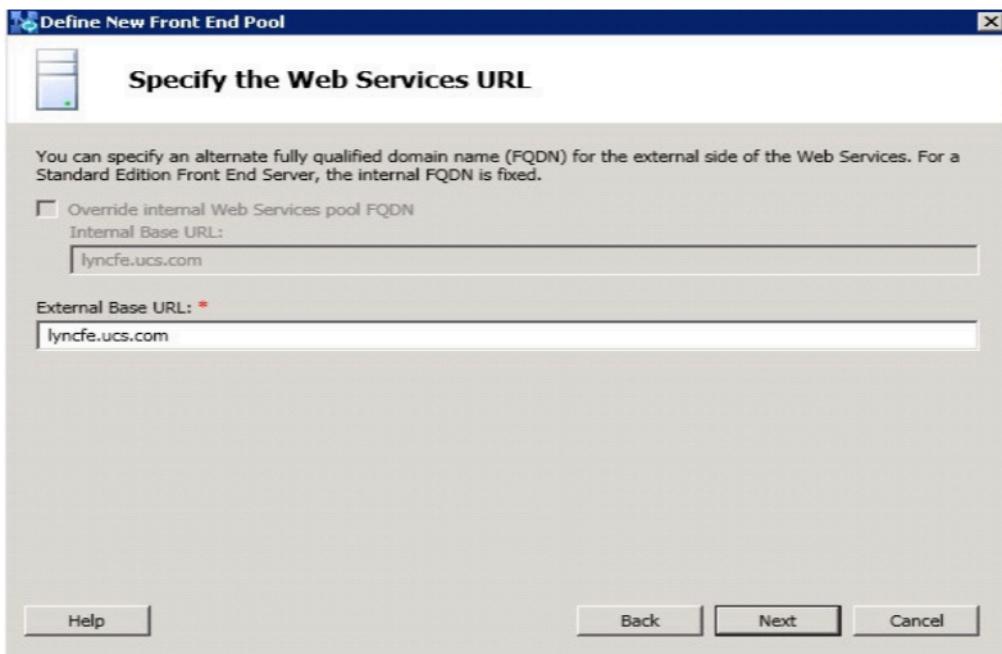
- Since we don't have an OWA configured yet we will point it to OWA.ucs.com

  Click **Finish**.
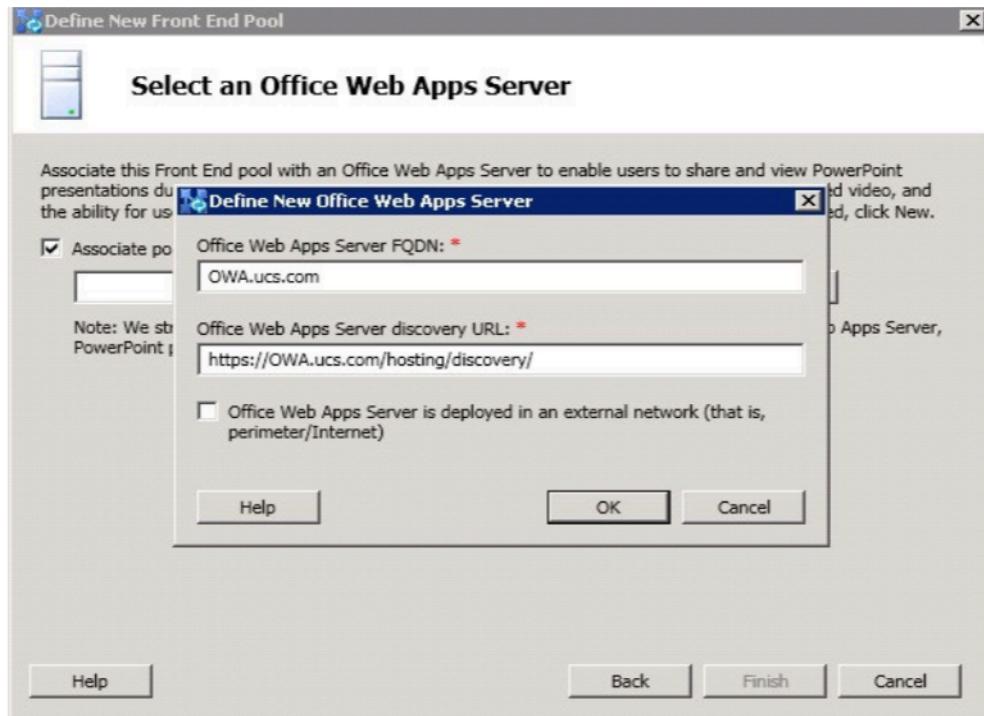
Edit properties of topology

- Right-click on **Lync Server 2013** and then click **Edit Properties**.
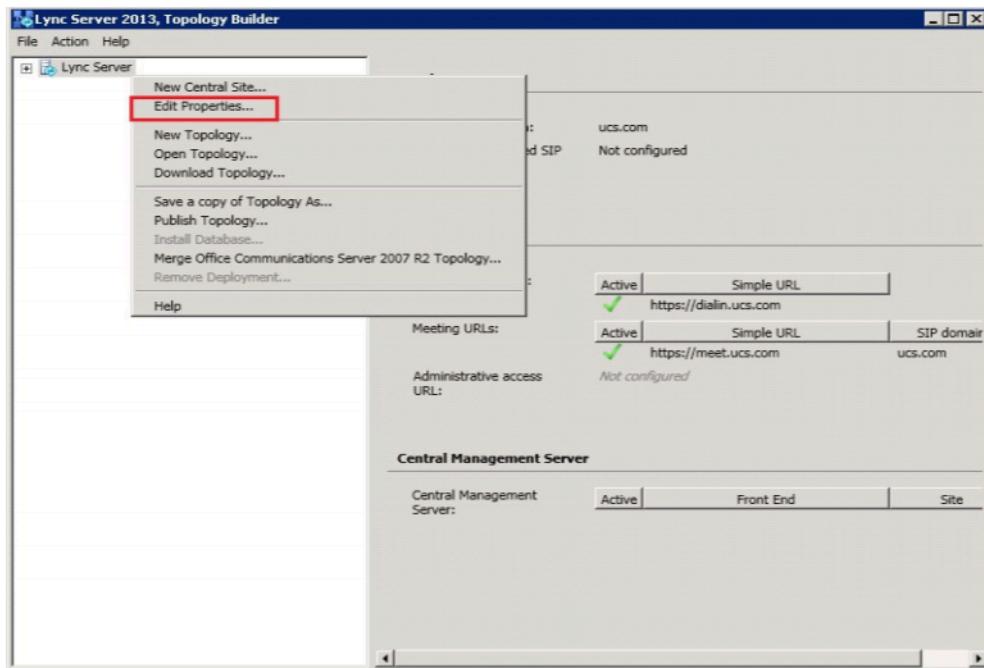
- Scroll down to Administrative access URL field and define the admin URL as https:// admin.ucs.com and select **Front End Server** (lyncfe.ucs.com).
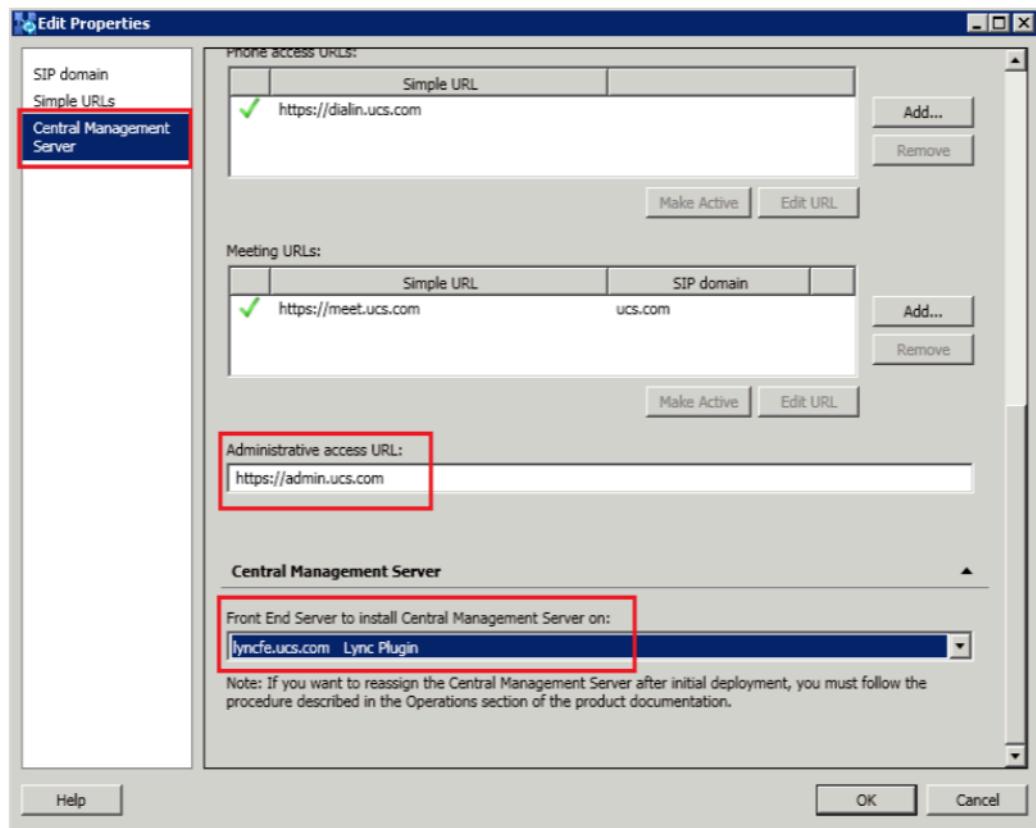
- Go to Action > Publish Topology > Next > Next.
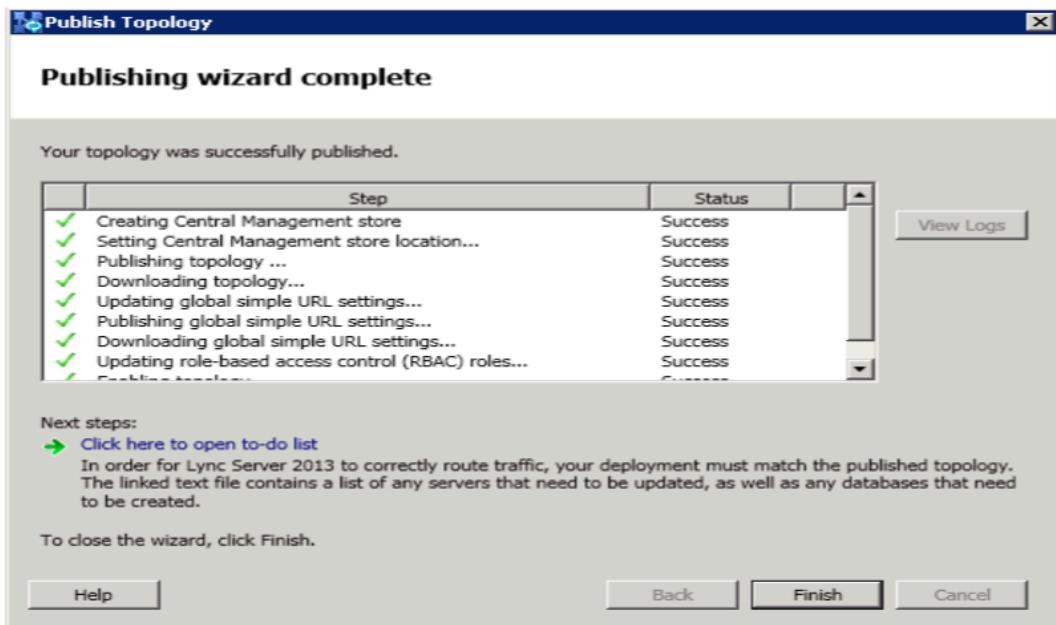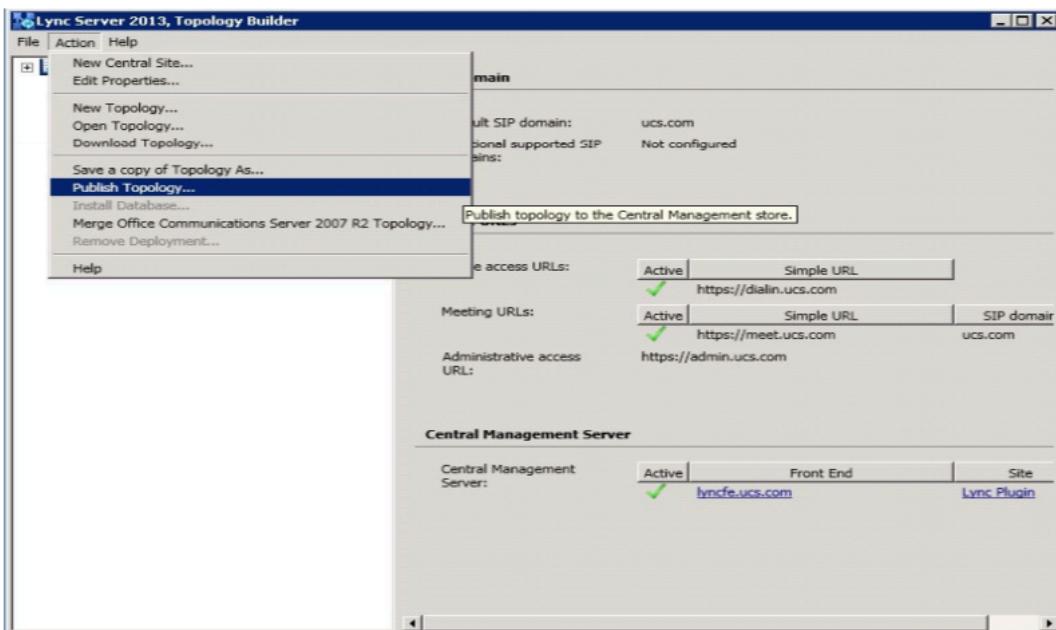
Install Lync Server System

- Open Deployment Wizard and click on **Install** or **Update Lync Server System**.
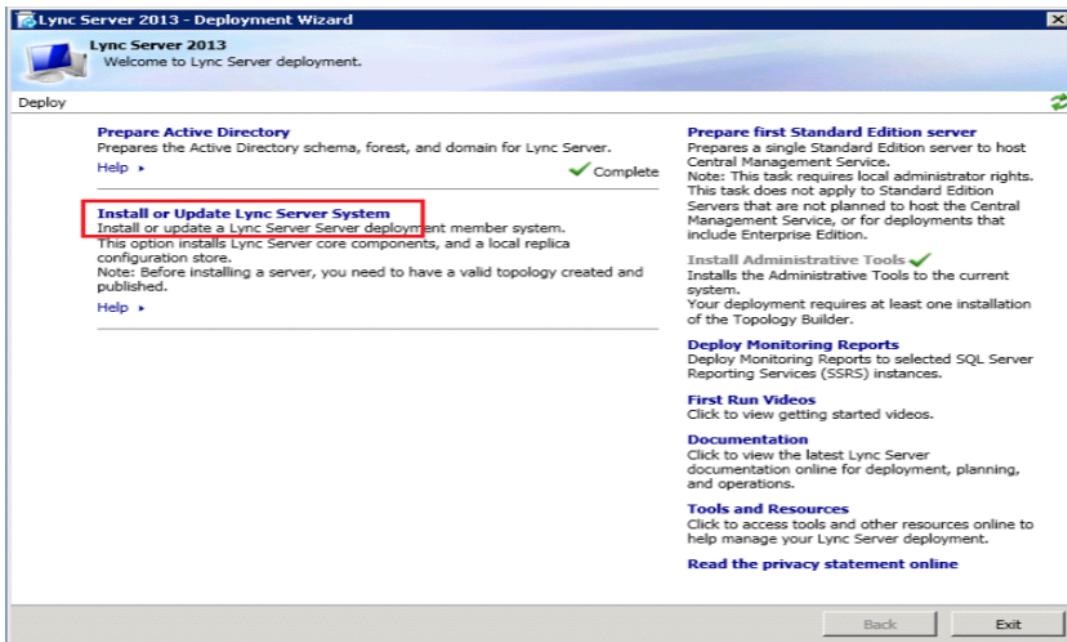
- Install the Lync Server System components, put Certs in place and Start Services:

  - Step1 : Install RtcLocal database
  - Step 2: Install Speech files, etc.
  - Step 3: Setup Certs
  - Step 4: Start Lync Services

See detailed steps below:
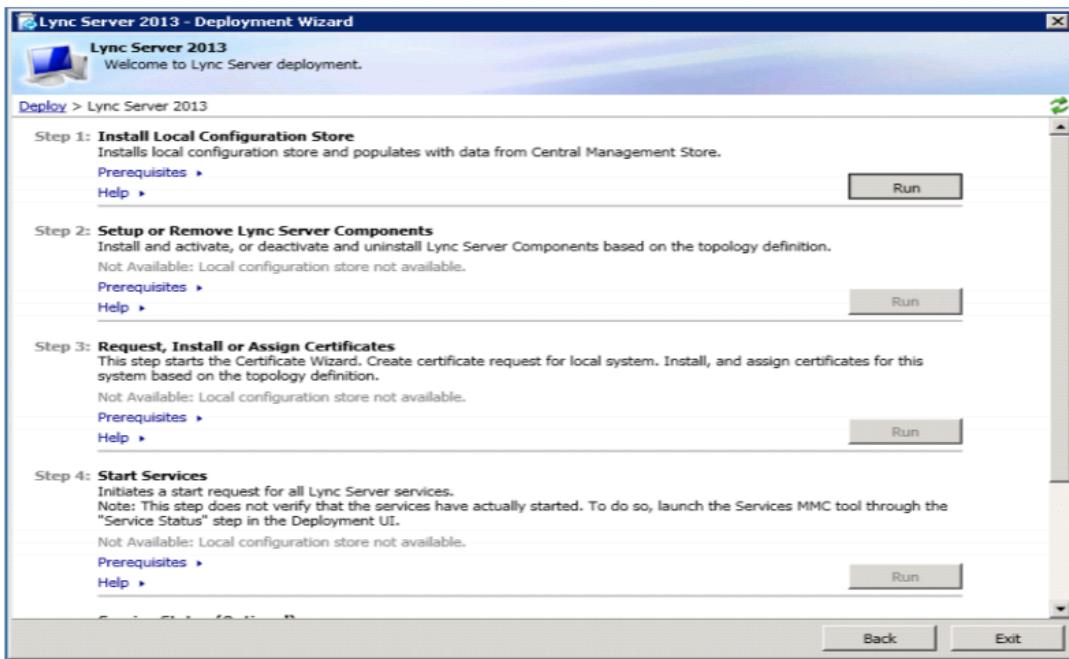
Step1 Install Local Configuration Store (will install RtcLocal)

- Run
- Retrieve Directly from the CMS… radio button

Step2 Setup Lync Server components (will install Speechfiles, etc)

- Run
- Next (15 minutes on new lab systems)

> ℹ **Note**:
>
> if you designated the archive/monitoring server, this will fail because SQL for those stores is not there yet.)

The following settings need to be done in **Control Panel > User Accounts > Change account type > Add**.

Add an entry for :

- Username : lyncfe

  Domain: ucs.com

  Group Membership: Administrator

- Username : Administrator

 Domain: ucs.com

  Group Membership: Administrator
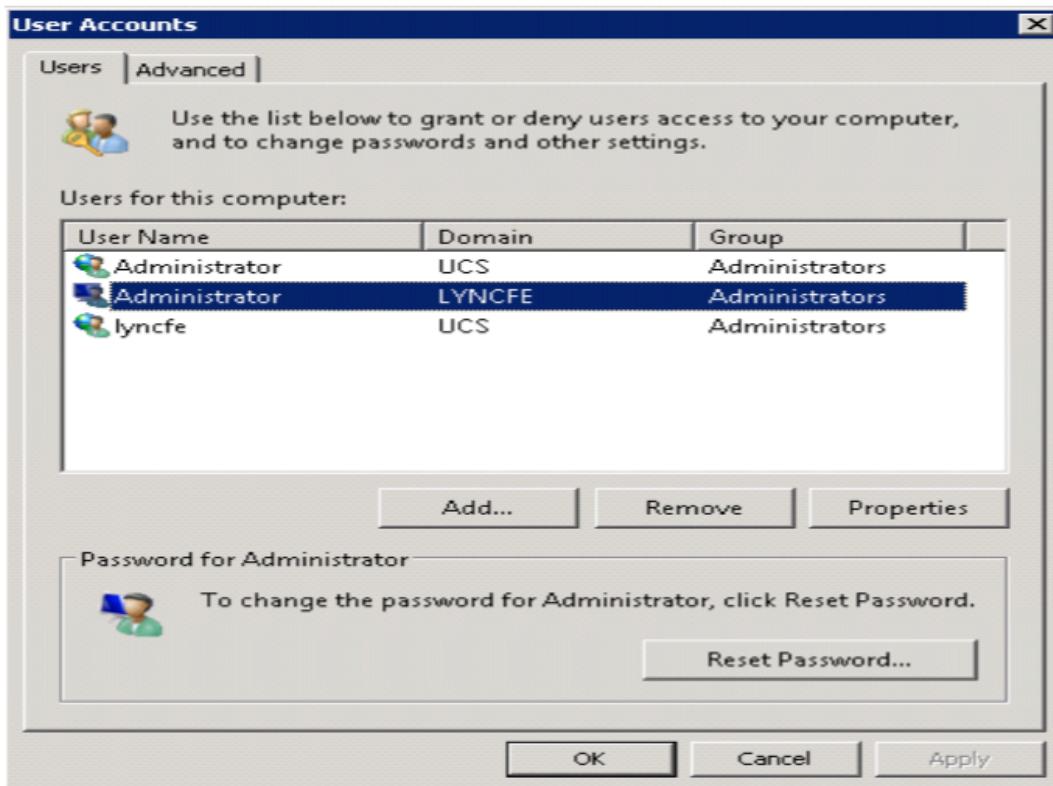
Step3 Request Certs

> **Note**:
>
> If this is a lab setup, and you have installed both AD and Lync FE OS's, remember the FE needs to be rebooted after you install the certificates on Lync Server so that it can recognize the CA.)

- Run
- Select **Default Certificate** then click **Request**.
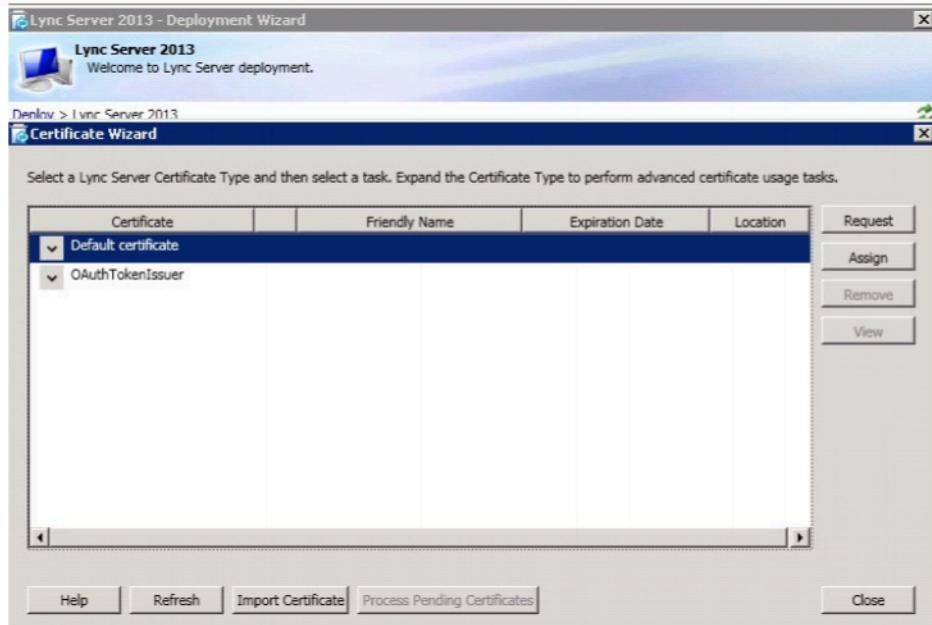
In the Certificate Request page click **Next**.

For Delayed or Immediate Request, send the request immediately to an online cert authority.

Choose a Certificate Authority (CA): Select a CA from the list.
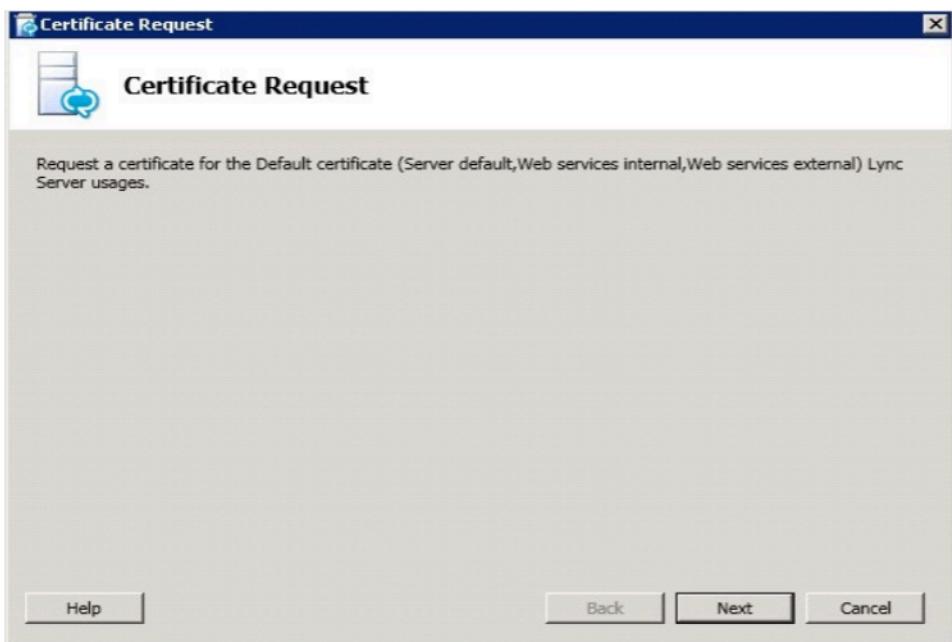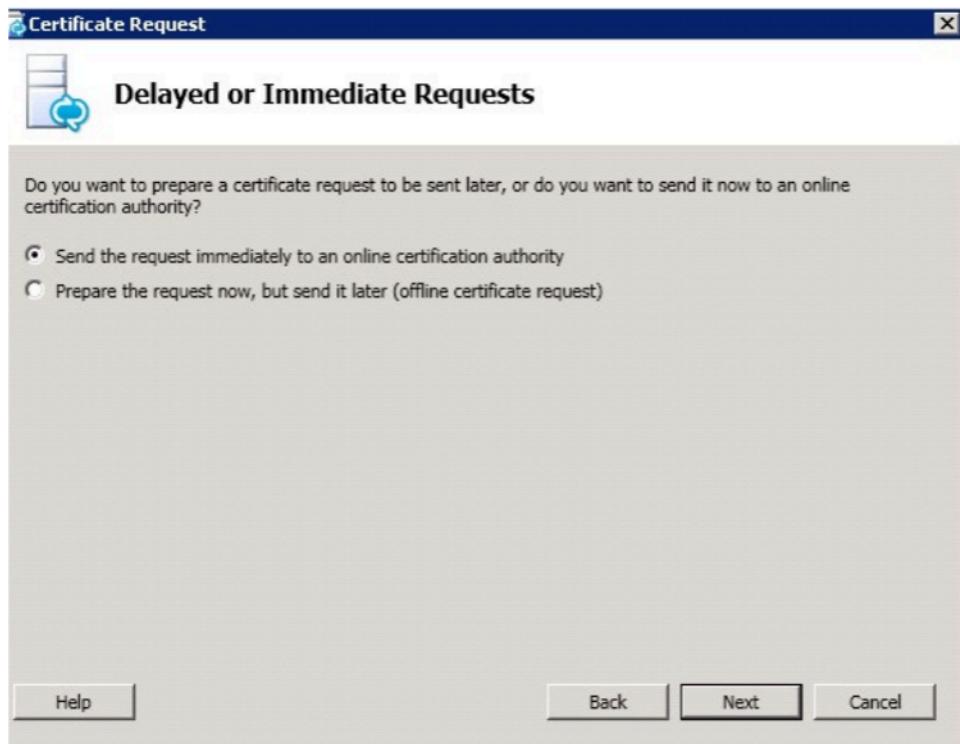
In the Certification Authority Account page click **Next**.


Specify Alternative Certificate Template and click **Next**.

In the **Name and Security Settings** window, under Friendly Name add some name.

Organization Information: fill in Org and Org Unit

Geographical Information: fill in

Subject Name/Subject Alternative Names:Next

SIP Domain Setting on SAN: Select SIP Domain (example: ucs.com) and then click Next.
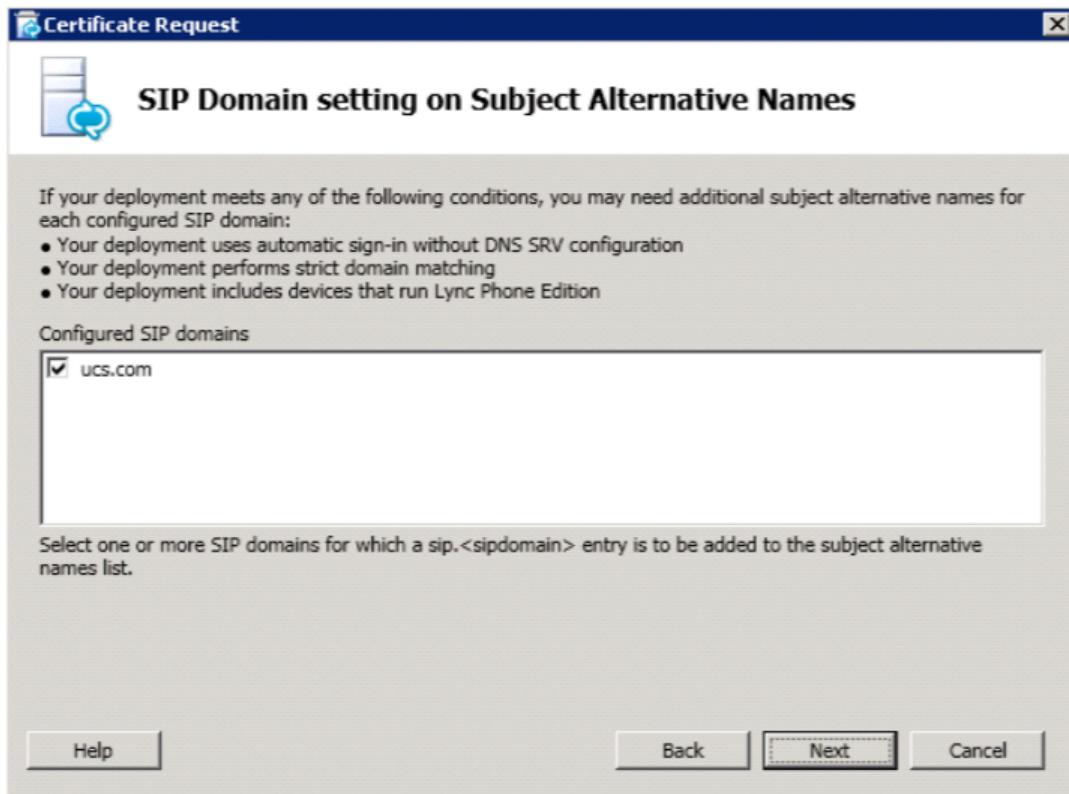
Configure Additional SAN: Next

Certificate Request Summary: Next

Executing Commands: Completed: Next

Online Certificate Request Status: Finish

Certificate Assignment: Next

Certificate Assignment Summary: Next

Executing Commands: Finish

Select "Default certificate" and click Assign certs
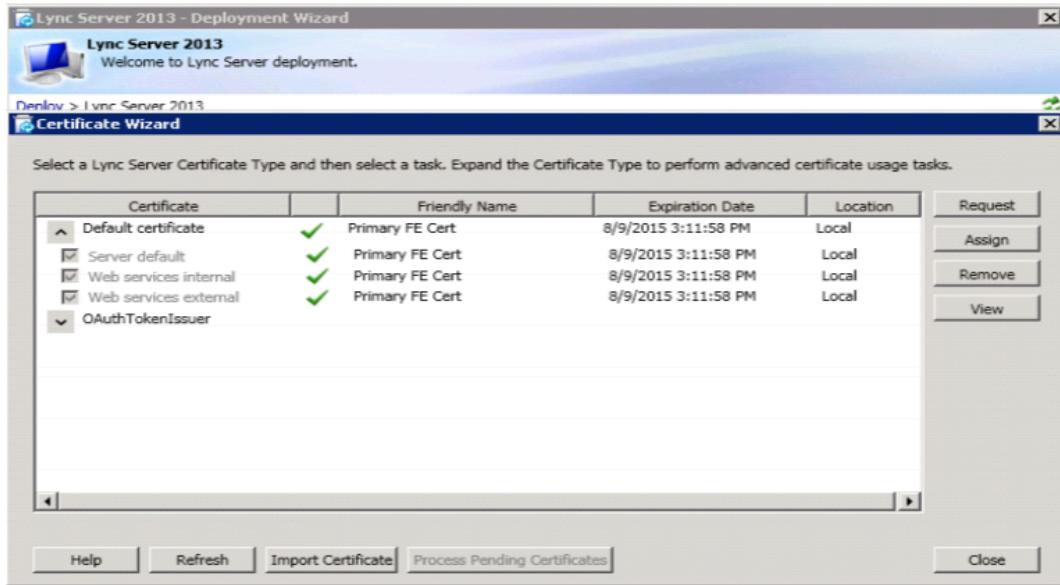
Now repeat the Certificate Wizard steps for the OAuthTokenIsuer.

Step 4: Start Services

After services are started you can open the Services to verify all the Lync Services are running.
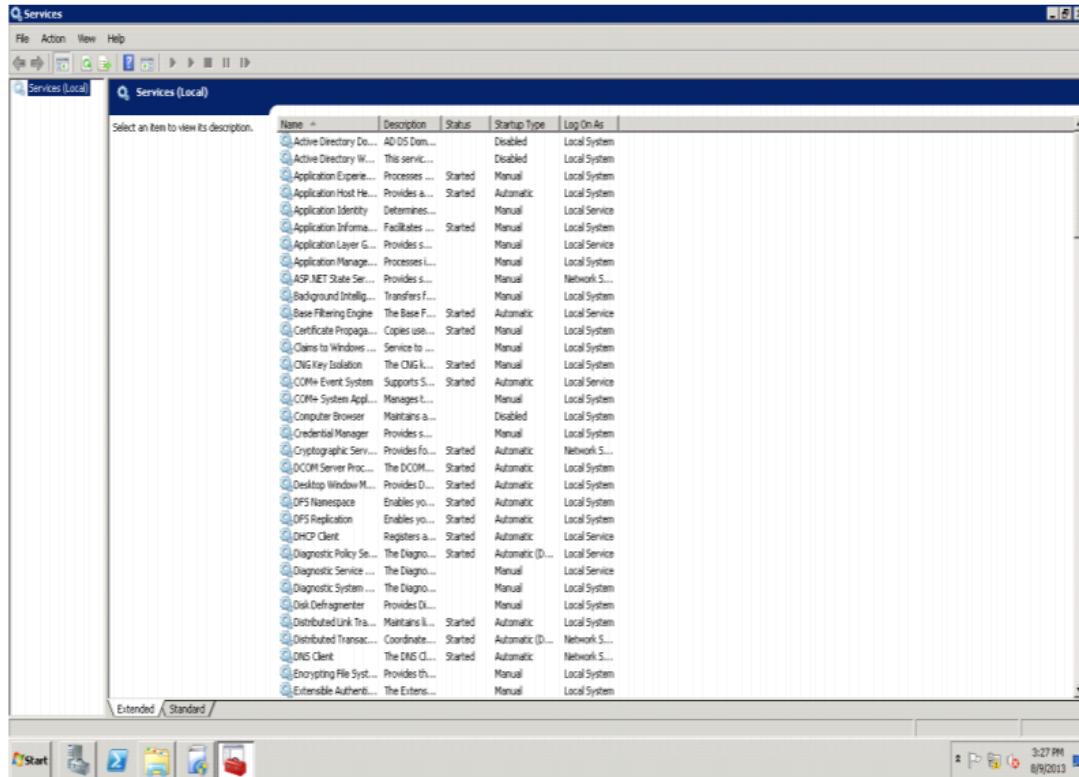
Go to Start and run Lync from the Control Panel.

You will be asked to type in Administrator credentials. If this is a new server, you will also be asked to install Silverlight (already installed in prerequisites).
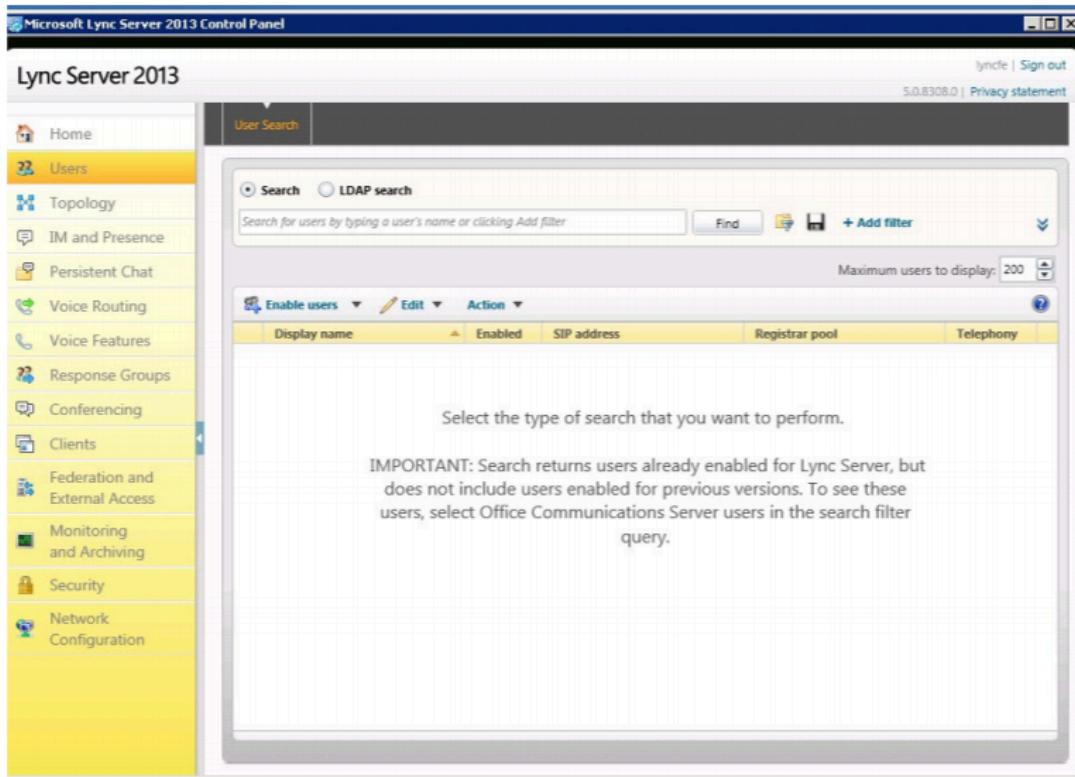
Appendix C – Supported MiVoice Business features

> **ⓘ Note:**
>
> This table provides references to only UC Endpoints and SIP ACD sets.

Features	MiCollab Client	
	Deskphone	**Softphone**
Ability to work offline	✓	✓
Account Codes[17]– Default	✓	✓
Account Codes – System	✓	✓
Account Codes – Verified and Non-verified	Non-verified[2]	Non-verified[2]
ACD Support	✓	✓
Add Held	✓	✓
Advisory Message	✓	✓

---

[17] Account code dialing is not supported on SIP softphone.

Features	MiCollab Client	
	Deskphone	**Softphone**
Auditory Alerts (accessibility/disability)	✓	✓
Auto Answer	✓	✓
Auto-Answer	✓	✓
Auto-Hold	✓	✓
Broker's Call	✗	✗
Calculator	✗	✗
Call Duration Display	✓	✓
Call Forward	✓	✓
Call Forward – Cancel All	✓ 2	✓ 2
Call Forward – Delay	✓ 2	✓ 2
Call Forward – Follow Me – End Chaining	✓	✗
Call Forward – Follow Me – Reroute when Busy	✓	✗

Features	MiCollab Client	
	Deskphone	**Softphone**
Call Forward – Forced	✓	✓
Call Forward – Override	✓ 2	✓ 2
Call Forward profiles	✓	✓
Call Handoff	✓	✓
Call History	✓	✓
Call history / logs – local	✓	✓
Call history / logs – server-based	✓	✓
Call Me Back	✓	✓
Call Park	✘	✘
Call Park Retrieve	✘	✘
Call Pickup (Dialed, Directed, Clustered)	✓ 2	✓ 2
Call Privacy	✘	✘

Features	MiCollab Client	
	Deskphone	**Softphone**
Call timer and annotation tools	✓	✓
Call Waiting – Swap Automatic	✗	✗
Callback	✓	✓
Caller ID-based call routing	✓	✓
Camp-on	✗	✗
Clear All Features	✗	✗
Compression Support	✓	✓
Conference[18]	✓	✓ 3
Conference Application (controls Conference Unit)	✗	✗
Conference Split	✓ 2	✓ 2
Conference Unit Support (5305/5310)	✗	✗

---

[18] Conference feature is not supported on SIP-based softphone.

Features	MiCollab Client	
	Deskphone	**Softphone**
Contact sync from Outlook to MiCollab Client	✓	✓
Corporate Directory	✓ 2	✓ 2
Corporate Directory – LDAP sync (inc. Active Directory)	✓	✓
Corporate Directory – sync to MiVoice Business directory	✓	✓
Destination-based Call Display	✗	✗
Dial from PIM – Outlook 2003, 2007, 2010 (32 and 64 bit), 2013 (32 and 64 bit), 2016 (32 and 64 bit)	✓	✓
Dial Tone – Outgoing Calls	✓	✓
Dialed Number Editing	✓	✓
Direct Outward Dialing (DOD)	✓	✓
Direct Page – Initiate	✓ 2	✓ 2
Direct Page – Receive	✗	✗

Features	MiCollab Client	
	Deskphone	**Softphone**
Do Not Disturb	✓	✓
Drag-and-drop conference calls	✓	✓
Favorites menu	✓	✓
Feature Keys	✗	✗
Flash – Calibrated	✗	✗
Flash – Switchhook	✗	✗
Flash – Trunk	✗	✗
Flexible Answer Point	✓	✓
Gigabit Ethernet Stand Support	✓	✓
Group Listen	✗	✗
Group Page – Initiate	✗	✗
Group Page – Receive	✗	✗

Features	MiCollab Client	
	Deskphone	**Softphone**
Handset Receiver Volume Control	✓	✓
Handsfree Answerback	✗	✗
Handsfree Operation	✓	✓
Headset Mute Switch	✓	✓
Headset Operation	✓	✓
Hold	✓	✓
Hold Key Retrieves Last Held Call	✓ [2]	✓ [2]
Hold on Hold	✓	✓
Hot Desking	✓	✓
Hot Line	✗	✗
In-call control window allowing transfer, conference, hold and hang up	✓	✓
Knowledge Management	✓	✓

Features	MiCollab Client	
	Deskphone	**Softphone**
Language Change	✓	✓
Launch of MiCollab Client at computer start	✓	✓
LCS integration	✗	✗
Licensing through the Mitel AMC	✓	✓
Line Interface Module Support	✗	✗
Line Types and Appearances	✓	✓
Meet Me Answer	✗	✗
Messaging – Advisory	✓ 2	✓ 2
Messaging – Callback	✗	✗
Messaging – Dialed	✓	✓
Mobile Extension	✓	✗
Multiple Message Waiting Indicator	✗	✗

Features	MiCollab Client	
	Deskphone	**Softphone**
Music	✓	✗
Mute Key	✓	✓
Off-Hook Voice Announce	✗	✗
Override	✗	✗
Override Security	✗	✗
PC Programming Application Support (Desktop Tool)	✓ 2	✓ 2
Personal Directory	✓	✓
Phonebook	✓	✓
PIM Integration – ACT!	✓	✓
PIM Integration – Lotus Notes	✓	✓
PIM Integration – Outlook	✓	✓
PKM Support	✓	✓

Features	MiCollab Client	
	Deskphone	**Softphone**
Presence Indicator – Busy Lamp Field (BLF)	✓	✓
Presence Indicator – Computer	✓	✓
Privacy Release	✗	✗
Record a Call	✗	✓
Redial	✓ 2	✓ 2
Redial – Saved Number	✓ 2	✓ 2
Release	✓ 2	✓ 2
Reminder	✗	✗
Resiliency Support	✓	✓ 1
Ringer Control (Pitch and Volume)	✗	✓
Ringing Line Select	✗	✗

Features	MiCollab Client	
	Deskphone	**Softphone**
RSS Window	✓	✓
Screen-pops on calls with ability to forward, send to voice mail	✓	✓
Secure instant messaging (chat) with file transfer	✓	✓
Silent Monitor	✗	✗
Simplified Account Code Entry	✗	✗
SIP Support	✗	✗
Softkey Support	✗	✗
Speaker Volume Control	✓	✓
Speed Call – Pause	✗	✗
Speed Call – Personal	✓ 2	✓ 2
Speed Call – System	✗	✗
Speed Call Keys	✓	✓

Features	MiCollab Client	
	Deskphone [2]	**Softphone** [2]
Station-to-Station Dialing	✓	✓
SuperKey	✗	✗
Swap	✓	✓
System tray status icon	✓	✓
Tag Call (Malicious Call Trace)	✗	✗
Teleworker Support	✓	✓
Tone Demonstration	✗	✗
Transfer	✓	✓
Trunk Access	✗	✗
Trunk Answer from Any Station (TAFAS)	✗	✗
Visual Voice Mail	✓	✓
Voice Mail	✓	✓

Features	MiCollab Client	
	Deskphone	**Softphone**
Web browser	✓ 2	✓ 2
Wireless LAN Stand Support	✓	✓

Table 20: MiVoice Business Supported Feature Access Codes

Feature number	Feature name	Desk phone	Softphone
2	ACD Silent Monitor	✓	✓ 19
3	ACD Agent Login	✓	✗
4	ACD Agent Logout	✓	✗
5	Make Busy Setup	✓	✗
6	Make Busy Cancel	✓	✗
10	Call Forwarding – Busy – External Only	✗	✓
11	Call Forwarding – Busy – External and Internal	✗	✓

---

[19] ACD Silent Mointor is supported for ACD hot desk agents on MINET softphones only.

Feature number	Feature name	Desk phone	Softphone
12	Call Forwarding – Follow Me	✓	✓
13	Cancel Call Forwarding – Busy – External and Internal	✗	✓
16	Call Forwarding – Follow Me	✓	✓
17	Cancel Call Forwarding – Follow Me	✓	✓
21	Call Forwarding – I Am Here	✓	✓
22	Call Forwarding – No Answer – External Only	✓	✓
23	Call Forwarding – No Answer – External and Internal	✓	✓
24	Call Forwarding – No Answer – Internal Only	✓	✓
25	Cancel Call Forwarding – No Answer – External and Internal	✓	✓
27	Cancel All Forwarding	✓	✓
29	Call Hold – Remote Retrieve	✓	✓

Feature number	Feature name	Desk phone	Softphone
32	Call Pickup – Dialed	✓	✓
33	Call Pickup – Directed	✓	✓
40	Do Not Disturb	✓	✓
41	Do Not Disturb – Cancel	✓	✓
42	Do Not Disturb – Cancel Remote	✓	✓
43	Do Not Disturb – Remote	✓	✓
47	Last Number Re-dial	✓	✓
48	Message Waiting – Activate	✓	✓
49	Message Waiting – Deactivate	✓	✓
50	Message Waiting – Inquire	✓	✓

Appendix D – MiVoice Office 250 Communication Platform features

Feature name	Code	MiCollab Client	
		Desk phone	Softphone
Account Code[20] – All Calls Following	391	✓	✓
Account Code – Optional	390	✓	✓
ACD Agent Login	326	✓	✓
ACD Agent Logout	328		
ACD Agent Login/ Logout Toggle	327		
ACD Agent Wrap-Up Terminate	329	✓	✓
Activate Door Relay[21]	332	✓	✓
Agent Help	375	✗	✗
Agent Help Reject	376	✓	✓
Answer (Ringing Call)	351	✓	✓

---

[20] Account code dialing is not supported on SIP softphone.
[21] This feature requires an HX Controller and MiVoice Office 250 v4.0 software.

Feature name	Code	MiCollab Client	
		Desk phone	**Softphone**
Audio Diagnostics	320	✖	✖
Automatic CO Access On/Off	360	✓	✖
Automatic IC Access On/Off	361	✓	✖
Automatic Trunk Answer	350	✓	✖
Background Music On/Off	313	✓	✓
Barge-In	386	✖	✖
Call Forward All Calls	355	✓	✓
Call Forward If Busy	357	✓	✓
Call Forward If No Answer	356	✓	✓
Call Forward If No Answer/Busy	358	✓	✓
Call Logging	333	✓	✓

Feature name	Code	MiCollab Client	
		Desk phone	Softphone
Change Language	301	✓	✗
CO Hookflash	330	✓	✓
Conference[22]	5	✓	✓ 3
Data	340	✓	✗
Default Phone	394	✓	✗
Directories	307	✓	✗
Display Outside Party Name On/Off	379	✓	✗
Display Time/Date (ITP) Show IP Address (SIP)	300	✓	✗
Do-Not-Disturb Do-Not-Disturb Cancel Do-Not-Disturb On/Off	370 371 372	✓	✓
Do-Not-Disturb Override	373	✗	✗

---

[22] Conference feature is not supported on SIP-based softphone.

Feature name	Code	MiCollab Client	
		Desk phone	**Softphone**
Dynamic Extension Express On Dynamic Extension Express Off Dynamic Extension Express On/Off	363 362 364	✓	✓
Dynamic Extension Express – Handoff	388	✓	✓
Enhanced Speakerphone Enable	310	✗	✗
Feature Key Default	395	✓	✗
Group Listen	312	✗	✗
Handsfree On/Off	319	✓	✓
Headset Enable Headset Disable Headset On/Off	315 316 317	✓	✗
Hold – Individual	336	✓	✓
Hold – System	335	✗	✗

Feature name	Code	MiCollab Client	
		Desk phone	**Softphone**
Hot Desk On/Off[23]	348	✓	✗
Hunt Group Remove	322	✓	✓
Hunt Group Replace	323		
Hunt Group Remove/ Replace	324		
LCD Contrast Adjustment	303[24]	✓	✗
Message	365	✓	✗
Message – Cancel	366	✓	✓
Message – Cancel Current	368	✓	✓
Message – Silent	367	✓	✓
Mute On/Off	314	✓	✓
Page	7	✓	✓
Page On/Off	325	✓	✗

---

[23] This feature requires MiVoice Office 250 v5.0 software.
[24] This feature must be completed on the phone.

Feature name	Code	MiCollab Client	
		Desk phone	**Softphone**
Program Buttons	3975	✓	✗
Program Phone Password	392	✓	✗
Queue Request	6	✓	✓
Record-A-Call	385	✓	✓
Redial	380	✓	✓
Redirect Call	331	✓	✓
Reminder Message Reminder Message Cancel	305 306	✓	✗
Remote Configuration – Disable	343	✓	✓
Remote Configuration – Display License Key	347	✓	✗
Remote Configuration – Enable	342	✓	✓
Remote Configuration – Reset	344	✓	✓

Feature name	Code	MiCollab Client	
		Desk phone	Softphone
Remote Programming	359	✓	✗
Reverse Transfer (Call Pick-Up)	4	✓	✓
Review Keys	3965	✓	✗
Ring Intercom Always On/Off	377	✓	✓
Ring Tone Selection	398	✓	✗
Routing Off	304	✓	✓
Station Monitor	321	✓	✓
Station Speed Dial	382	✓	✗
Station Speed Dial Programming	383	✓	✗
Steal	387	✗	✗
Switch Keymap	399	✓	✗
System Forward Enable	352 353	✓	✓

Feature name	Code	MiCollab Client	
		Desk phone	Softphone
System Forward Disable System Forward On/Off	354		
System Speed Dial	381	✓	✓
Transfer to Hold	346	✗	✗
Transfer to Ring	345	✓	✓

Appendix E – VMWare Horizon View Server Details

<div style="text-align: right">9</div>

MiCollab Installation on VMWare Horizon View Server

Navigate to the RDS server in VMWare Horizon View setup and perform the following steps:

1. Install application in RDS Server

Install the MiCollab PC Client on the RDS server.

2. Deploy an application pool on connection server

- Open the View Administrator console and navigate to **Inventory > Application Pools**.
- Click on **Add** button to create a new application pool.

- From the **Application Pool Type**, select **RDS Farm** which was previously created and select the applications to create an application pool.

- Click **Next**.
- Edit the **ID** or the **Display Name** field and then click **Submit** to create the application pool.
- Since we did not entitle any user to view desktops and applications yet, the **Add Entitlements** window appears. You can click **Cancel** to close the window.
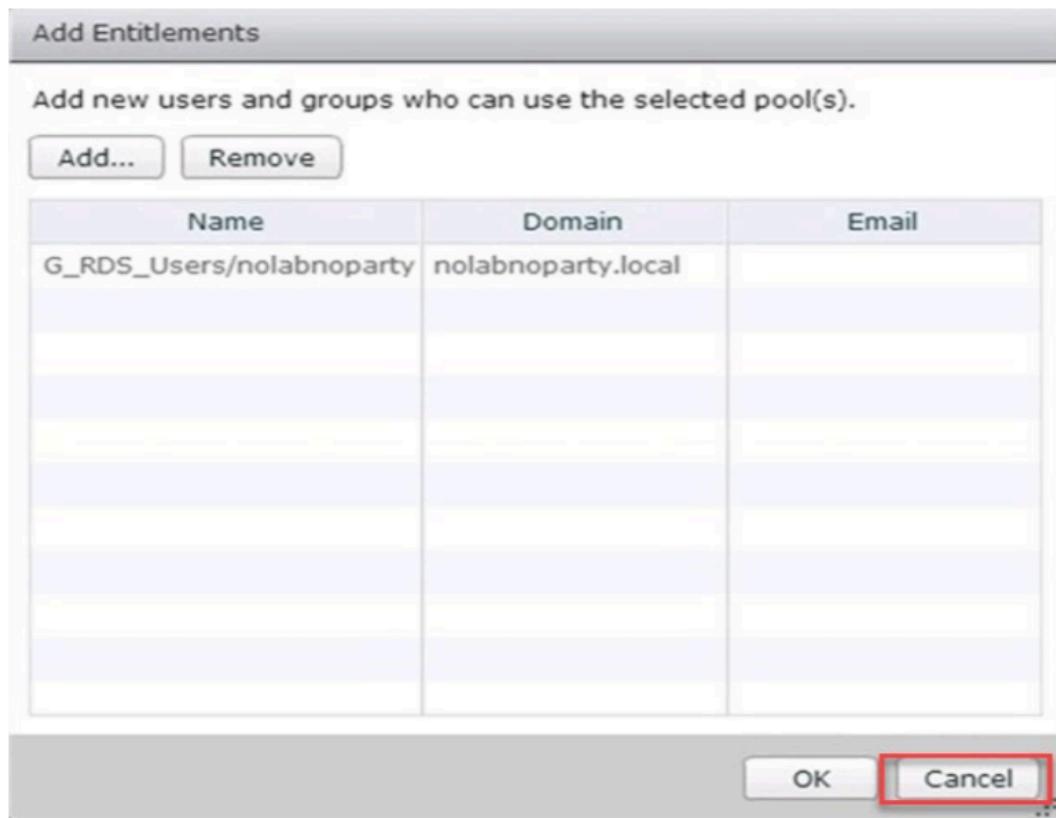
The MiCollab PC Client is now listed in the Application Pool.

3. Entitle users to a Desktops Pool on Connection Server

- Open the View Administrator console and navigate to **Inventory > Desktop Pools**.
- Select the Desktop Pool for entitlement.
- Click on **Entitlements** drop-down tab and select **Add Entitlement** option.
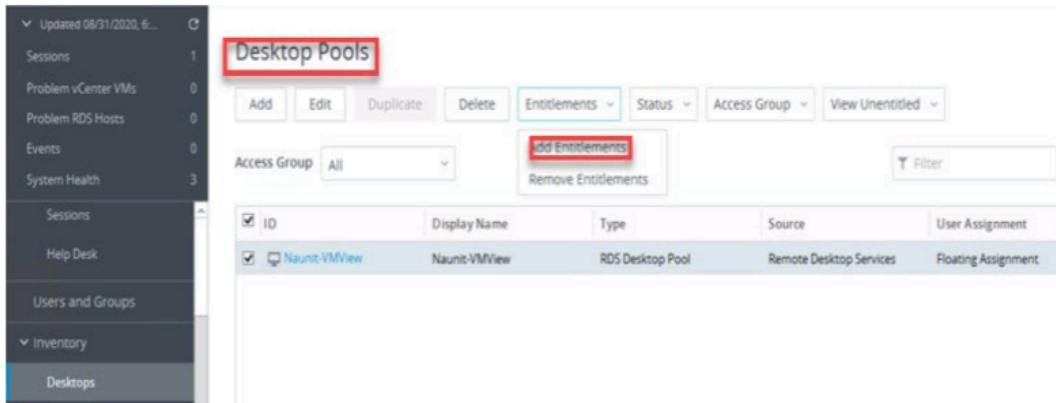
- Click **Add** to add users and groups.
- Click on **Find** and select from the list the users or groups to add, and then click **OK**.

- When done, click OK to entitle selected users and groups to the selected Desktop Pool.
- In the Entitled column you can check the number of entitlements.

Appendix E – VMWare Horizon View Server Details
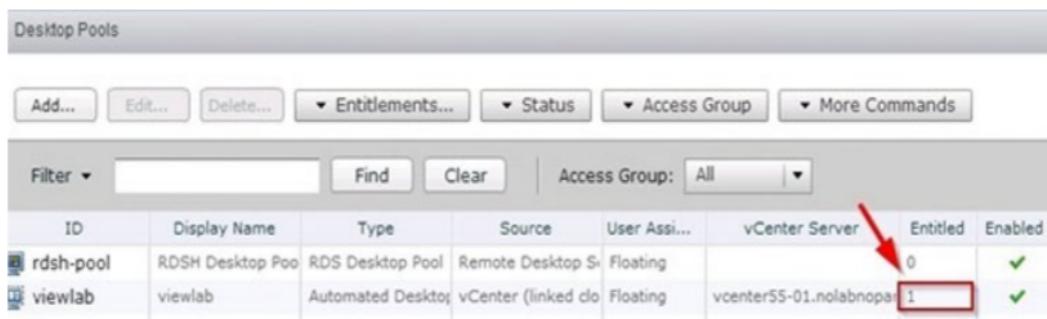
4. Entitle users to an Application Pool on Connection Server

- Open the **View Administrator** console and navigate to **Inventory > Application Pools**.
- Select the applications to entitle, click on **Entitlements** tab and select **Add** entitlementoption.
- Click **Add** to add users and groups.
- Click on **Find** and select from the list the users or groups to add then click **OK**.
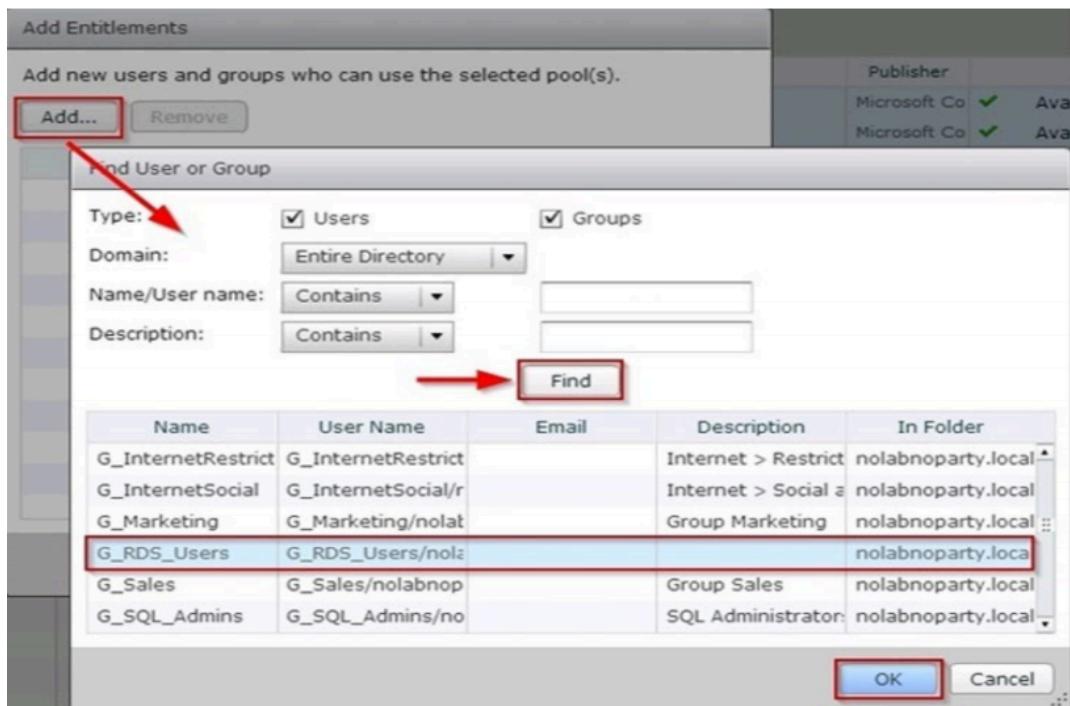
- When done, click **OK** to entitle users and groups to the selected Application Pool.
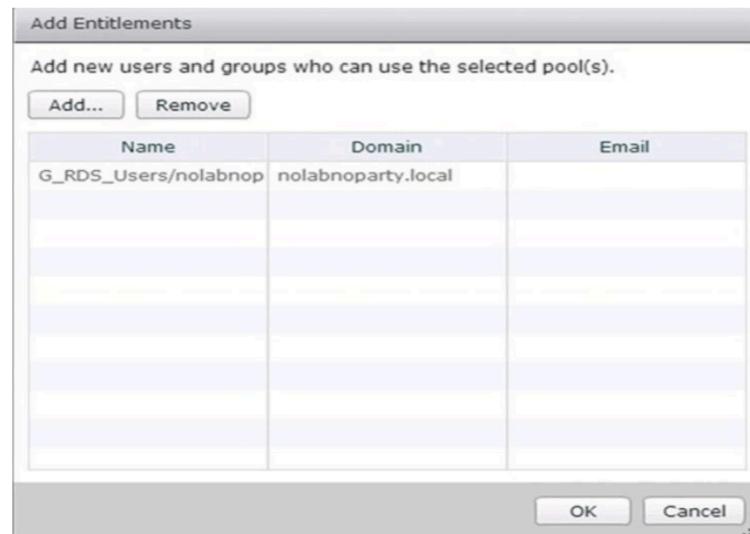
- Repeat same steps to entitle/unentitled additional users/groups.

Connecting to MiCollab Client on VMWare Horizon View

1. To launch the VMWare Horizon View Client, click on the default Connection Server set during the setup or click on **New Server** button to connect to a different server and under that click on the New Server item.
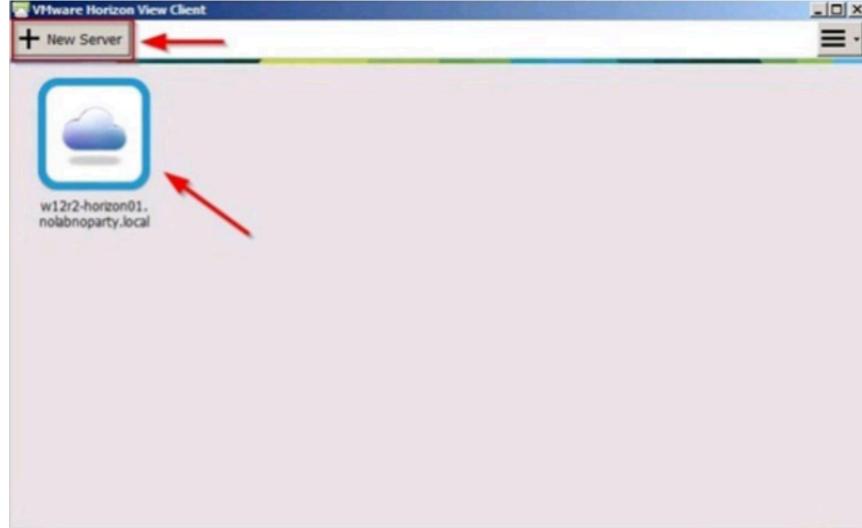
**2.** Type the FQDN of the Connection Server and click on **Connect**.

The client starts connecting to the server.
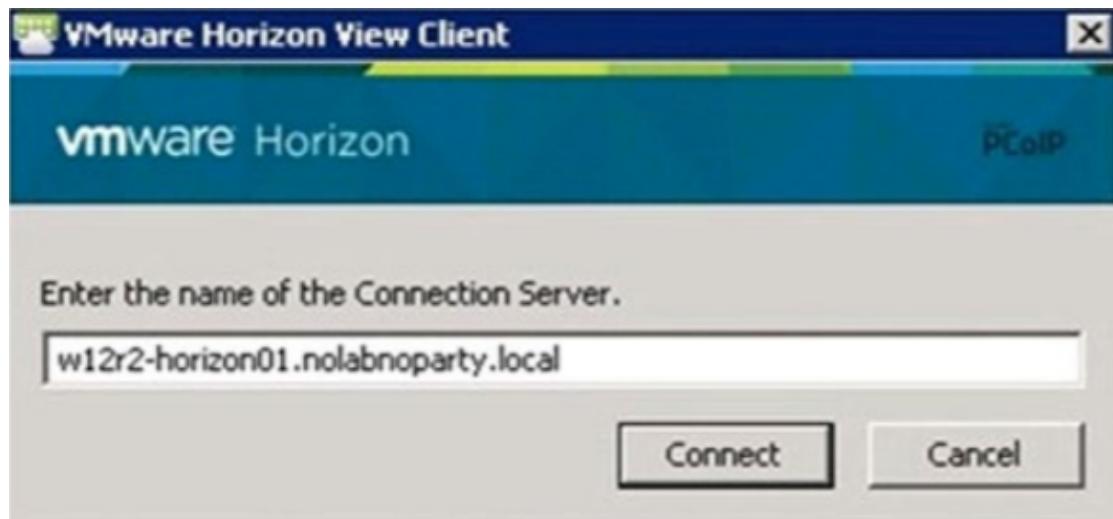
3. Enter the user credentials and click on **Login**.

4. When the main screen comes up, double-click in the MiCollab Client icon.
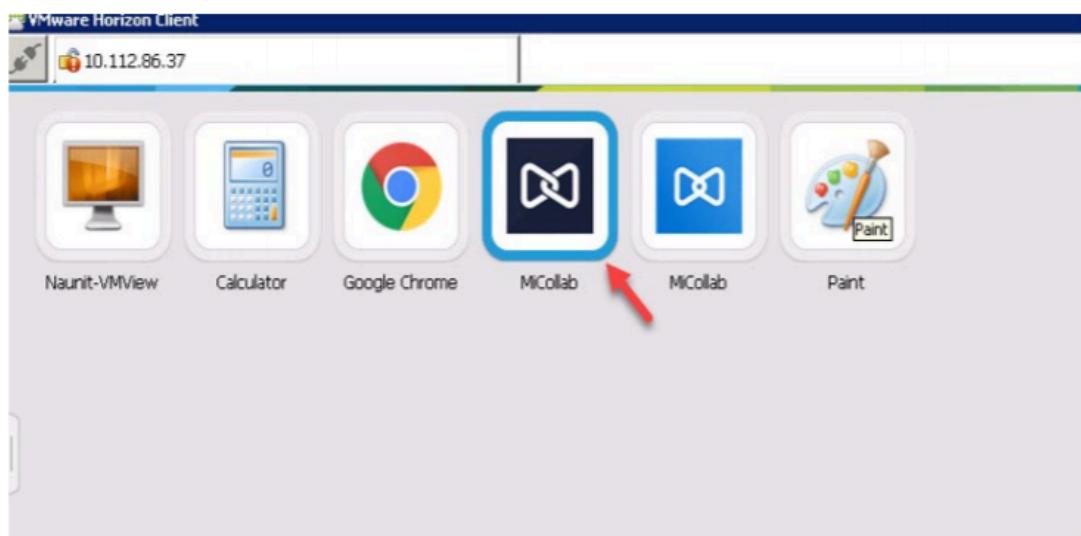
The selected application opens.
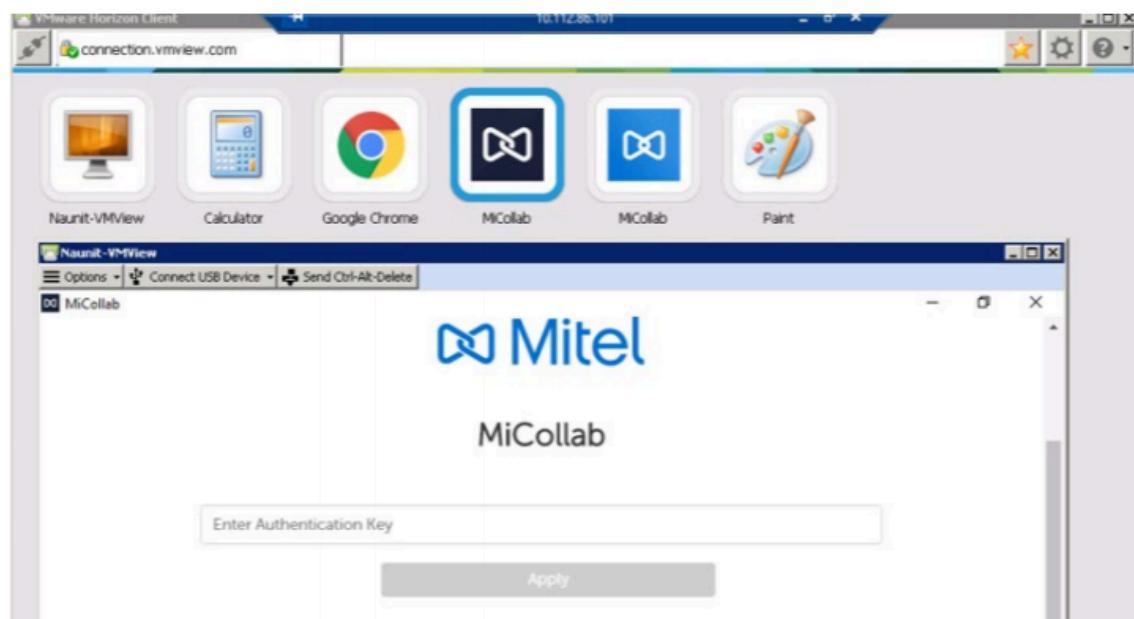
Appendix F - WLAN to WWAN Handover and Local Streaming

WLAN to WWAN Handover

WLAN to WWAN feature is supported in MiCollab from Release 9.7 onwards. MiCollab Client Application should be configured to register with the same public MBG whether connecting to MBG via WLAN (Wireless LAN) or WWAN (mobile telecommunication cellular network). If resiliency is configured and if the client connects to a different MBG after handover because of a fail-over during the call, there may be loss of audio or the call may be dropped. For more details on Softphone resiliency, refer to the MiCollab Client Resiliency Guide.

Local Streaming

Local Streaming mode is supported by MBG since Release 11.2. When the underlying network topology allows it, SIP Local streaming mode permits the media – whether RTP or SRTP – to be streamed directly between SIP devices without ever going through MBG.

For detailed information about Local Streaming, see the MBG Engineering Guidelines.