

Microsoft Office 365 X-UM with IP PBXs using AudioCodes CloudBond X-UM Standard

Version 0.1

Table of Contents

1	Introduction	11
1.1	Installation Flow	12
2	Planning X-UM Architecture	13
2.1	Skype for Business Preparation	13
2.2	Exchange UM Online Feature List	13
2.3	Call Flows	16
2.3.1	Call answering – Leave Voicemail Message to User – Direct Call to X-UM	16
2.3.2	Call Answering – Leave Voicemail Message to User – Call from Lync Client	17
2.3.3	Message Waiting Indication (Unsolicited)	17
2.3.4	Message Waiting Indication (SIP Subscription)	18
2.3.5	Outlook Voice Access– User Access to Mailbox via Telephone	18
2.3.6	Play-on-Phone	19
2.3.7	Outlook Voice Access Call Out – User Access to Mailbox via Telephone and Call out	20
2.4	Debugging tools	21
2.5	Re-image X-UM Standard	21
3	Default Configuration and Login Information	23
3.1	X-UM Standard Server information	23
3.1.1	Login	23
3.1.2	IP Address Information	23
3.1.3	X-UM Standard Domain Information	23
3.1.4	X-UM Standard Default Skype for Business Topology	23
3.2	SBC Mediant 800 Information	24
3.2.1	Login	24
3.2.2	IP Address Information	24
4	Changing Default Hyper-V Settings & Importing X-UM Connector	25
4.1	Stop the Reverse Proxy	25
4.2	Change Front-End Memory Size	25
4.3	Add the X-UM Connector Virtual Machine	25
4.4	Re-Join the X-UM to the Domain	30
5	Assigning Manual IP Address	33
5.1	Planning Your Network Changes	33
5.2	Making Changes to X-UM Standard	33
5.2.1	Using Local Monitor, Keyboard, and Mouse	33
5.2.2	Use RDP Sessions	33
5.3	Changing IP Addresses	33
5.3.1	Changing IP Addresses for Each Individual Server	34
5.3.2	Confirming IP Addresses on DNS Server	35
5.3.3	Changing X-UM Connector Pool Entry	37
5.3.4	Changing Topology Entries	37
5.3.4.1	Changing Default SIP Domain	37
5.3.4.2	Changing Simple URL's	38
5.3.4.3	Changing Edge Settings	39
5.3.5	Publishing the Topology Changes	41
5.3.6	Changing Static DNS Records	41
5.3.6.1	Modifying the Edge Server Hosts File	42

5.3.7	Changing the IP Address of AudioCodes Devices	43
5.3.7.1	Changing Mediant 800B IP Address	43
6	Changing or Adding a SIP Domain	45
6.1	Skype for Business and the SIP Domain	45
6.1.1	DNS and Simple URLs	45
6.1.2	DNS and Certificates	46
6.1.3	X-UM Standard and the SIP Domain.....	46
6.2	Changing X-UM Standard SIP Domain	46
6.2.1	Process Overview	46
6.2.2	Connecting to X-UM Standard Controller using RDP	47
6.2.3	Using the Topology Builder	47
6.2.3.1	Adding the New SIP Domain to the Topology	50
6.2.3.2	Changing the Default (Primary) SIP Domain	51
6.2.3.3	Managing Simple URLs.....	51
6.2.3.4	Editing External Web Services	53
6.2.3.5	Editing Edge Services Properties.....	54
6.2.3.6	Publishing Topology	55
6.2.4	Running Deployment Wizard	58
6.2.4.1	Installing or Updating Skype for Business Server System.....	59
6.2.5	DNS Entries	60
6.2.5.1	Skype for Business Internal Records	60
6.2.5.2	Skype for Business External Records.....	60
6.2.6	Certificates	61
6.2.6.1	AudioCodes X-UM Standard Certificates Configuration Note.....	61
6.2.7	Enabling Configuration	61
7	Connecting Edge Server to a Full DMZ Deployment.....	63
7.1	Connecting the Edge Server	63
8	Describing Deployment Requirements	67
8.1	Before Deploying CloudBond X-UM.....	67
8.1.1	Public Key Infrastructure	67
8.1.2	IP Addresses.....	67
8.1.3	DNS	68
8.1.4	Forest and Domain Levels	69
8.2	Integrating CloudBond X-UM	70
8.2.1	Connecting CloudBond X-UM to the Enterprise Domain.....	70
8.2.2	Verifying the Time and Time Zone Settings for CloudBond X-UM Servers.....	70
8.2.3	Verifying DNS Settings on NIC Adapters	70
8.2.4	Verifying the Enterprise Domain and Forest Levels	71
8.2.5	Setting up Cross Forest DNS Stub Zones.....	72
8.2.6	Active Directory Synchronization	81
8.2.7	Delegate Control	82
8.2.8	Certificates	84
8.3	Skype for Business DNS Records	84
8.3.1	Skype for Business Internal Records	85
8.3.2	Skype for Business External Records	85
8.3.3	Skype for Business DNS Records without the Entire DNS Zone	86
8.3.3.1	DNS Records for Non-Windows Clients	89
8.4	Firewall Port Requirements.....	89
8.4.1	CloudBond 365 Deployment Overview.....	89
8.4.1.1	References	89
8.4.2	Perimeter Network Port Requirements.....	93
8.4.2.1	Edge Server.....	93
8.4.2.2	Management Server.....	97

8.4.3	Other Port Requirements	97
8.4.3.1	Network Ports Used by Trusts	97
8.4.3.2	Ports and Protocols Used by the Skype for Business Internal Servers	99
8.4.4	Windows Update and SysAdmin Update Port Requirements	104
8.4.4.1	Port Requirements for Integration with Exchange 2010 SP1 Unified Messaging	104
9	Office 365 Integration.....	109
9.1	Overview	109
9.1.1	What is Office 365?	109
9.1.2	Office 365 and Voice	110
9.1.3	How does Skype for Business use Office 365?	110
9.1.4	What is Skype for Business Federation?.....	110
9.1.5	Domain Names and Shared Name Spaces.....	111
9.1.5.1	Skype for Business Hybrid Deployment.....	111
9.1.6	Replicating Users.....	112
9.1.6.1	DirSync.....	113
9.1.7	Active Directory Federation Services	114
9.2	Pre-Requisites.....	115
9.2.1	Infrastructure Prerequisites	115
9.2.2	Install DirSync.....	115
9.2.3	Ensure DirSync is Functioning	116
9.2.4	Deploy Skype for Business Schema Attributes	116
9.2.4.1	Using LDIFDE	116
9.2.5	Deploy CloudBond 365.....	117
9.2.6	Prepare the User Forest Active Directory for Write Access	117
9.3	Configuring Office 365 Integration	121
9.3.1	Prepare CloudBond 365 for Skype for Business Hybrid and Exchange UM.....	121
9.3.1.1	Start a Skype for Business Online PowerShell Session	121
9.3.1.2	Configuring Shared SIP Address Space	121
9.3.1.3	Allowing Federation.....	121
9.3.1.4	Removing Existing Hosting Provider.....	122
9.3.1.5	Creating a Hosting Provider for Skype for Business Online	122
9.3.2	Obtaining the Customer Specific Office 365 Information	122
9.3.2.1	Determining Hosted Migration Service Override URL	124
9.3.2.2	Determining Override Admin Domain	124
9.3.3	Using Exchange Online for Voicemail	125
9.3.3.1	Preparing Office 365 For Unified Messaging	125
9.3.3.2	Allowing Users to Dial-in to Access Exchange Online Voicemail	125
9.4	Initial Replication	127
9.4.1	After Initial Replication	128
9.4.1.1	Update DNS Records.....	128
9.4.1.2	Assigning User Registrar Pool	129
9.5	Ongoing Replication.....	130
9.6	Adding a Dial Plan to Exchange Online	131
9.7	Skype for Business PowerShell	136
9.8	PowerShell for Skype for Business Online.....	137
9.8.1	Connecting to Office 365 using PowerShell:	138
9.9	Troubleshooting	139
9.10	Custom User IDs for Cross Domain Updates	143
9.10.1	Updating the User Forest AD.....	143
9.10.2	Retrieving User Data from Office 365.....	144

10	Configuring Certificates	147
10.1	Background	147
10.1.1	Public Key Infrastructure.....	147
10.1.2	What Purpose does Certificates Serve?.....	147
10.1.3	Trust.....	147
10.1.3.1	Trust and Certificate SANs.....	148
10.1.3.2	Wildcard Certificates	148
10.1.4	Privacy	148
10.1.5	Certificate Authorities.....	148
10.1.5.1	Where to Obtain Certificates?	149
10.1.5.2	How to Obtain a Certificate?	149
10.2	CloudBond 365 Default Certificates	150
10.2.1	CloudBond 365 Included Certificates	150
10.2.2	CloudBond 365 External Certificates.....	150
10.3	CloudBond 365 Certificate Requirements	151
10.3.1	Notes.....	151
10.4	Public Certificates	152
10.4.1	Minimizing Cost	152
10.4.2	Planning	152
10.4.2.1	Minimize the Number of SIP Domains	152
10.4.2.2	Minimize the Variations in Simple URLs	153
10.4.2.3	The External Web Services.....	155
10.4.2.4	Minimize the Edge External Service Names	155
10.4.2.5	What About LyncDiscover?	155
10.4.2.6	Are There Other SAN Entries?.....	156
10.4.2.7	So What is the Minimum Configuration / Certificate Request?	156
10.5	Using the Topology Builder	156
10.5.1	SIP Domain.....	158
10.5.1.2	Managing Simple URL's.....	161
10.5.1.3	Using External Web Services.....	162
10.5.1.4	Configuring Edge Services.....	164
10.5.1.5	Publishing Topology and Deploy.....	165
10.6	Obtaining and Deploying Certificates	171
10.6.1	Certificate Requests	171
10.6.2	Generating a Certificate.....	171
10.6.3	Importing the Certificate.....	171
10.6.4	Assigning a Certificate to a Skype for Business Role	171
10.7	Using an Internal Certificate Authority	171
10.7.1	How to Trust the Enterprise Root CA	172
10.7.1.1	Obtain the Enterprise Root Certificate	173
10.7.1.2	Install the Enterprise Root Certificate on CloudBond 365.....	173
10.8	Skype for Business Certificate Wizards	177
10.8.1	Using the Certificate Wizards	177
10.8.1.1	Accessing the Certificate Wizard	177
10.9	Requesting New Internal Certificates.....	180
10.9.1	Enterprise CA Accessible	180
10.9.2	Enterprise CA Not Accessible.....	180
10.9.3	Requesting Certificates (CA Accessible).....	181
10.9.3.1	Generating the Certificate Request.....	181
10.9.3.2	Generating and Installing the Certificate	188
10.9.3.3	Assign the Certificate to a Skype for Business Role	188
10.9.4	Requesting Certificates (CA is Not Available)	190
10.9.4.1	Generating the Certificate Request.....	190
10.9.4.2	Generating the Certificate	192
10.9.4.3	Installing the Certificate on the CloudBond 365 Server	193

10.9.4.4 Assign the Certificate to a Skype for Business Role	196
10.10 Requesting External Certificates	198
10.11 Certificate Summary	199
10.12 Setting Up a Certificate Authority	201
10.12.1 Setting Up a Certificate Authority on Windows Server 2003	201
10.12.2 Setting up a Certificate Authority on Windows Server 2008	202
10.12.3 Setting Up a Certificate Authority on Windows Server 2012	206
10.12.3.1 Configure the Certificate Services	211
11 Miscellaneous Actions	219
11.1 Installing the Product License	219
11.1.1 Uploading the CloudBond 365 License	219
11.1.2 Uploading the X-UM Standard License	220
11.2 Activating Windows	221
11.3 Running Windows Updates	223
11.4 Skype for Business Cumulative Update	226
11.5 CloudBond Support and Responsibility Program	226
11.6 Antivirus Application	226
11.7 Running the Skype for Business Deployment Wizard	226
11.8 Forwarding DNS Requests	229
12 X-UM Connector Configuration	233
12.1 Set X-UM Connector configuration	233
12.2 Create Users in CloudBond 365	233
12.3 Adding Users to X-UM Connector	234
12.3.1 Using REST API	235
13 Configure the SBC in X-UM Solution	237
13.1 MWI Notify	237
13.2 X-UM Connector SIP Interface	238
13.3 SBC Configuration Important points	238
14 Using X-UM Connector Debugging tools	239
14.1 X-UM Log	239
14.2 X-UM Connector Running in Console Mode	239
14.3 Syslog	239
14.4 OCS Logger and Wireshark	240
15 Re-Image X-UM Standard	241
15.1 Download Latest Version	241
15.2 Create the X-UM Connector VM	241
15.3 Configuring X-UM Connector VM	246
15.4 Starting the X-UM Connector Virtual Machine	249
15.5 Windows 2012R2 Server Role & Features	250
15.6 Set IP	250
15.7 Add X-UM Connector to Domain	250
15.8 Install UCMA 5	253
15.9 Installing Skype for Business Component	254
15.10 Installing X-UM Connector Wizard	258

15.11 Activating X-UM Connector.....	260
15.12 Adding DNS A Record	262
A HA and DR	265
A.1 HA/DR On Skype Level.....	265
A.2 HA On X-UM Level.....	265
A.2.1 Conditions for HA.....	265
A.2.2 Incoming Messages Redirection	266
A.2.2.1 Proxy Configuration.....	267
A.2.3 Web GUI Swagger	267
B Known Issues	269
B.1 User File Name does not Support “\$” Char.....	269
B.2 Using the REST Swagger Client with Internet Explorer	269
B.3 Replication Fail.....	269

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: January-29-2019

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at <https://www.audiocodes.com/services-support/maintenance-and-support>.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name
X-UM Connector Installation Manual

Document Revision Record

LTRT	Description
26790	Initial document release for Version 0.1
26791	Update for version 0.1.39: Added Software Revision Record below. Replaced references to X-UM Connector Wizard with X-UM Application.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <https://online.audiocodes.com/documentation-feedback>.

Software Revision Record

The following table lists the software versions released in Version 0.1.

Table 1-1: Software Revision Record

Software Version	Date
0.1.22	Feb 2018
0.1.30	Mar 2018
0.1.31	Mar 2018
0.1.36	Jun 2018
0.1.38	Sep 2018
0.1.39	Dec 2018



Note: The latest software versions can be downloaded from:

https://s3.eu-central-1.amazonaws.com/downloads-audiocodes/Download/AC_XUM_Install.html

Unzip the file to a temporary directory.

1 Introduction

Microsoft announced that they are going to discontinue the support for Session Border Controllers in Exchange Online Unified Messaging (UM):

"In July 2018, we will no longer support the use of Session Border Controllers (SBC) to connect third-party PBX systems to Exchange Online Unified Messaging (UM)."

This means that the connection between companies' PBX/IP-PBX and Exchange Online UM that was done using SBC/Gateway will no longer work. As a result, the UM features will stop working due to lack of connectivity between the PBX/IP-PBX and Exchange Online.

For the full announcement refer to:

<https://blogs.technet.microsoft.com/exchange/2017/07/18/discontinuation-of-support-for-session-border-controllers-in-exchange-online-unified-messaging/>

The AudioCodes response to this change is the X-UM solution, which is available in two main configurations:

- **X-UM Standard based on CloudBond Standard Plus**

In this configuration, the X-UM Connector is installed in the CloudBond environment (Mediant 800) as an additional virtual machine. It is activated in the CloudBond Skype for Business server environment.

The customer needs to connect this CloudBond server to the company's environment (Skype / PBX / exchange).

- **X-UM Connector as a standalone server**

In this configuration, the customer needs to dedicate a machine for the X-UM Connector, and install and activate it, as described below, on an existing Skype for Business server topology configured to work with Office 365 Microsoft Exchange Online Unified Messaging.

This document:

- Describes how to set up the **X-UM Standard**. To install the X-UM Connector refer to *LTRT-40725 X-UM Connector Installation Manual*. X-UM Standard is based on CloudBond Standard Plus. CloudBond runs in its own Active Directory resource forest and offers an easy Web-based management console for administering the CloudBond environment. With the CloudBond Active Directory connector, enterprise Active Directory users can be added to the appliance without needing to extend the enterprise Active Directory Schema. In addition to the CloudBond, the X-UM Standard contains an extra Virtual Machine that runs the X-UM Connector, which acts as a bridge between the PSTN side and the Exchange UM.
- Provides full step-by-step instructions for setting up the system. The system is installed before it is shipped and only needs to be configured for the basic architecture.
- Assumes you are familiar with the Windows 2012 R2 network configuration, modifying and deploying the Skype for Business topology, editing the hosts file, and verifying DNS entries.



Note: We recommend you review the CloudBond manuals which describe the CloudBond solution and suggested architecture. The X-UM Standard is based on it.

1.1 Installation Flow

The following describes the installation steps with the corresponding references to the relevant section in the document.

1. Default configuration and login information - see Chapter 3
2. Change the default HyperV settings and import the X-UM connector - see Chapter 4
3. Assigning Manual IP Address - see Chapter 5
4. Changing or Adding a SIP Domain - see Chapter 6
5. Setting Edge Server to Full DMZ deployment - see Chapter 7
6. Deployment of X-UM Standard within an existing corporate domain network – see Chapter 8
7. Integrating with Office 365 - see Chapter 9
8. Configuring Certificates - see Chapter 10
9. Miscellaneous - see Chapter 11
10. X-UM Connector Configuration - see Chapter 12
11. Configure the SBC in X-UM Solution - see Chapter 13

2 Planning X-UM Architecture

SfB topology is built from sites, pools, servers and more. The X-UM is based on Skype trusted application end point and user end points. Trusted application end point belongs to one Trusted application pool – every trusted application pool is associated with one registrar pool. Every X-UM can handle 5000 users – to be able to support more than 5000 users need to use several X-UM servers that will work in Active-Active mode, when one X-UM is down the other active X-UM will reallocate the users. For more information regarding HA, refer to Appendix A



Note:

- The X-UM will register every user on the Registrar Pool for retrieving calls and MWI. This registration will be considered like a regular Skype client registration. By default every user can register from 8 devices, one of them being the X-UM.
- X-UM can provide service to users homed to different pools on different sites; however, if the associated registrar pool is down, the X-UM associated with this pool will not be able to provide full service – this why need to have at least two X-UM servers (in case the topology includes multi registrar pools) which are associated with different registrar pools.

2.1 Skype for Business Preparation

- User must be UM enabled and set to Enterprise Voice.
- Configure Skype for Business to work with ExchangeUM – verify that the Skype client can connect with ExchangeUM to leave and retrieve messages.
- Configure PSTN access for the users –some of the X-UM flows configurations pass via the PSTN access to Skype for Business.

2.2 Exchange UM Online Feature List

From: [https://technet.microsoft.com/en-us/library/jj938142\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj938142(v=exchg.150).aspx)

The features name mark in **Red** are relevant and can be handled by the X-UM.

When you configure UM for your organization, users can access voice mail, email, personal Contacts and calendar information that's located in their mailbox from an email client, for example, Microsoft Outlook or Outlook Web App, from a mobile phone with Microsoft Exchange ActiveSync set up, such as a Windows Phone, or from a telephone. Additionally, users can use the following features:

- **Access to their Exchange mailbox:** Users can access a full set of voice mail features from Internet-capable mobile phones, Outlook 2007 or later versions, and Outlook Web App. These features include many voice mail configuration options and the ability to play a voice message from either the reading pane, using an integrated Windows Media Player, or the message list, using computer speakers.
- **Play on Phone:** The Play-on-Phone feature lets users play voice messages over a telephone. If the user works in an office cubicle, is using a public computer or a computer that isn't enabled for multimedia, or is listening to a voice message that's confidential, they might not want to or be able to listen to a voice message through computer speakers. They can play the voice message using any telephone, including a home, office, or mobile telephone.
- **Voice mail form:** The voice mail form resembles the default email form. It gives users an interface for performing actions such as playing, stopping, or pausing voice messages, playing voice messages on a telephone, and adding and editing notes.

The voice mail form includes the embedded Windows Media Player and an Audio notes field. The embedded Windows Media Player and notes field are displayed either in the reading pane when users preview a voice message or in a separate window when they open the voice message. If users aren't enabled for UM, or if a supported email client hasn't been installed on the client computer, they view voice messages as email attachments, and the voice mail form isn't available.

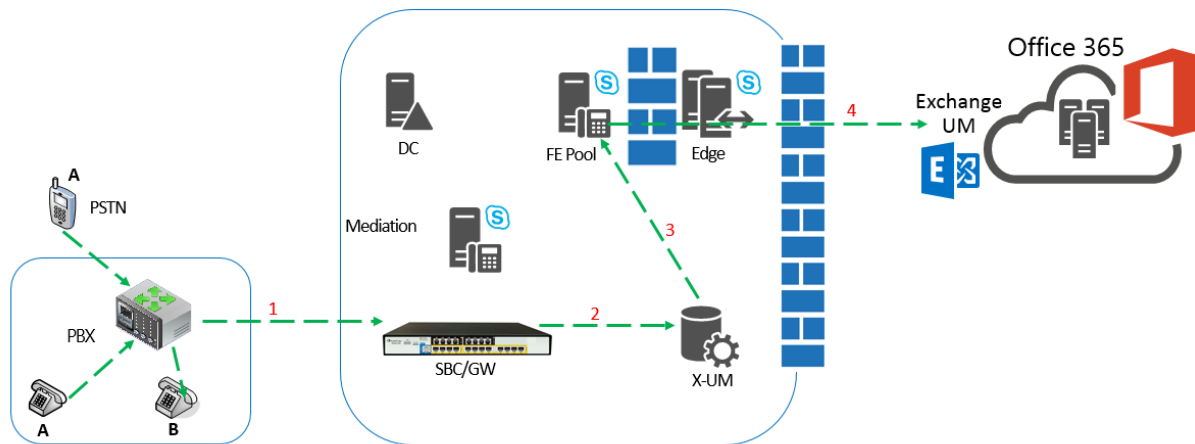
- **User configuration:** Users can configure several voice mail options for UM using Outlook Web App. For example, the user can record personal greetings, configure missed call and text message notifications and a voice mail Play on Phone number, and reset a voice mail access PIN.
- **Call answering:** Call answering includes answering incoming calls on behalf of users, playing their personal greetings, recording messages, and then sending the voice mail to their Inbox as an email message.
- **Call Answering Rules** The Call Answering Rules feature lets users who are enabled for voice mail determine how their incoming call answering calls should be handled. The way call answering rules are applied to incoming calls is similar to the way Inbox rules are applied to incoming email messages. By default, no call answering rules are configured. If an incoming call is answered, the caller is prompted to leave a voice message for the person being called. By using call answering rules, a caller can:
 - Leave a voice message for the user.
 - Transfer to an alternate contact of the user.
 - Transfer to the alternate contact's voice mail.
 - Transfer to other phone numbers that the user has configured.
 - Use the Find Me feature or locate the user through a transfer from an operator.
- **Voice Mail Preview:** Unified Messaging uses Automatic Speech Recognition (ASR) on newly created voice mail messages. When users receive voice messages, the messages contain both a recording and text that's been created from the voice recording. Users see the voice message text displayed in an email message from within Outlook Web App or another supported email client.
- **Message Waiting Indicator:** Message Waiting Indicator is a feature found in most legacy voice mail systems and can refer to any mechanism that indicates the existence of a new message. Enabling or disabling Message Waiting Indicator is done on the user's mailbox or on a UM mailbox policy.
- **Missed call and voice mail notifications using SMS:** When users are part of a hybrid or Office 365 deployment, and they configure their voice mail settings with their mobile phone number and configure call forwarding, they can receive notifications about missed calls and new voice messages on their mobile phones in a text message through the Short Messaging Service (SMS). However, to receive these types of notifications, the users must first configure text messaging and also enable notifications on their account.
- **Protected Voice Mail:** Protected Voice Mail is a feature that enables users to send private mail. This voice mail is protected and users are restricted from forwarding, copying, or extracting the voice file from email. Protected Voice Mail increases the confidentiality of voice mail messages, and lets users limit the audience for voice messages.
- **Outlook Voice Access:** There are two UM user interfaces available to users: the telephone user interface (TUI) and the voice user interface (VUI). These two interfaces together are called Outlook Voice Access. Outlook Voice Access users can use Outlook Voice Access when they access the voice mail system from an external or internal telephone. Users who dial in to the voice mail system can access their mailbox using Outlook Voice Access. However, when a user is searching the directory for your organization, they must use the key pad on their phone to search for a user. Using their voice to search the directory isn't available.

- Using a telephone, a UM-enabled user can:
 - Access voice mail
 - Listen to, forward, or reply to email messages
 - Listen to calendar information
 - Access or dial contacts who are stored in the organization's directory or a single contact or contact group located in their personal Contacts.
 - Accept or cancel meeting requests
 - Set a voice message to let callers know the called party is away
 - Set user security preferences and personal options
 - Search for users in the directory of the organization
- **Group addressing using Outlook Voice Access:** Users can send a single email message to a single user in their personal Contacts, to multiple recipients from the directory by adding each recipient individually, or by adding the name of a distribution list from the directory for your organization. In UM in Office 365, when a user signs in to their mailbox using Outlook Voice Access, they can also send email and voice messages to users in a group stored in their personal Contacts.

2.3 Call Flows

2.3.1 Call answering – Leave Voicemail Message to User – Direct Call to X-UM

Figure 2-1: Call Answering – Leave Voicemail Message to User – Direct Call to X-UM



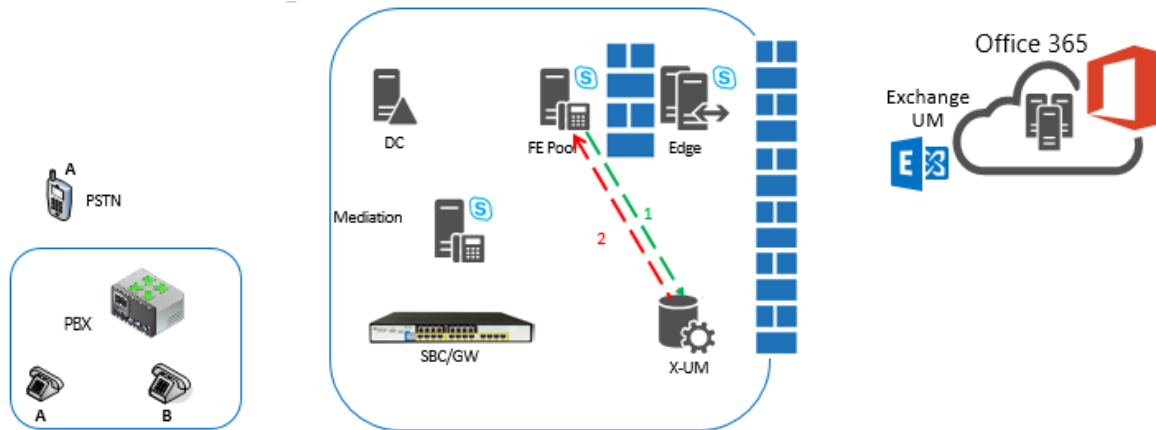
1. A calls B and the call is forwarded to the SBC.
2. The SBC forwards the call to X-UM and adds prefix (*55) to mark the call as deposit to voicemail.
3. X-UM validates that the mailbox is managed by the users file 0 and then forwards the call to FE as direct deposit to voicemail call.
4. The call is sent to Office365 Exchange UM.



Note: Another option for this flow – the call is forwarded to the Mediation server instead of X-UM for direct deposit by converting to SIP URI via Active Directory, or if forwarded to the Phone URI, the X-UM can reject the call so it is sent to the Exchange UM.

2.3.2 Call Answering – Leave Voicemail Message to User – Call from Lync Client

Figure 2-2: Call Answering – Leave Voicemail Message to User – Call from Lync Client



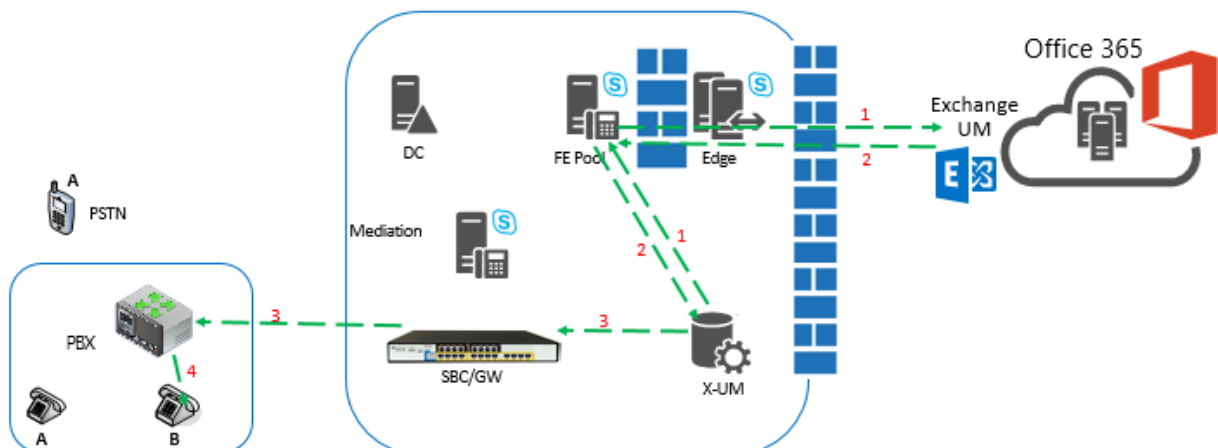
1. FE forwards incoming call to user to X-UM
2. By default, X-UM rejects all incoming calls to user, except for calls from Exchange UM (see slide below). If other user devices are registered then they'll keep ringing, otherwise call is terminated (or forwarded to Exchange).



Note: X-UM can be configured to accept incoming calls from Lync side. In this case, X-UM will forward the call to the SBC, and ultimately the call will reach the users PBX phone.

2.3.3 Message Waiting Indication (Unsolicited)

Figure 2-3: Message Waiting Indication (Unsolicited)

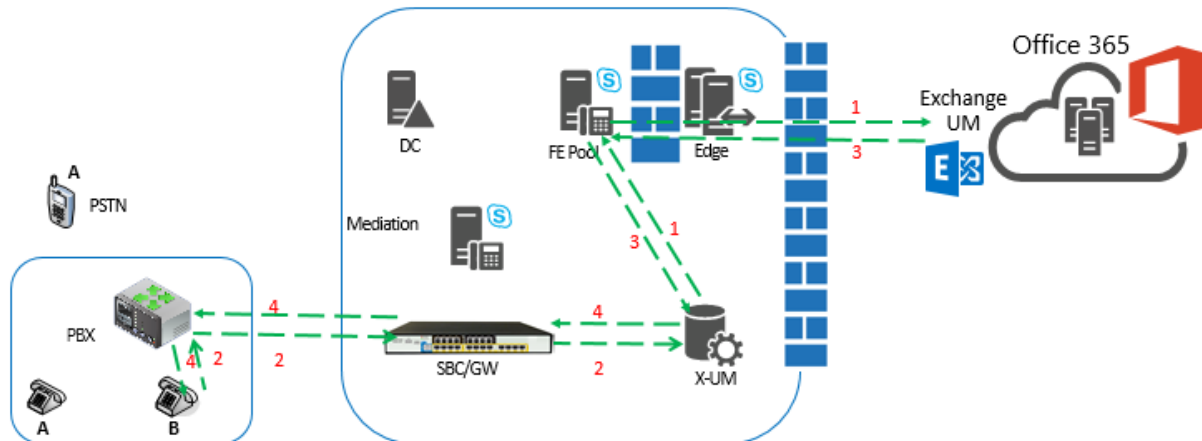


1. X-UM Application subscribes for Exchange MWI via the FE and Edge.
2. Due to voicemail status change, Office365 sends MWI message to the X-UM via the FE and Edge.

3. X-UM replaces the SIP URI with Phone extension and sends the MWI to the PBX via the SBC.
4. The PBX sends the MWI to the phone.

2.3.4 Message Waiting Indication (SIP Subscription)

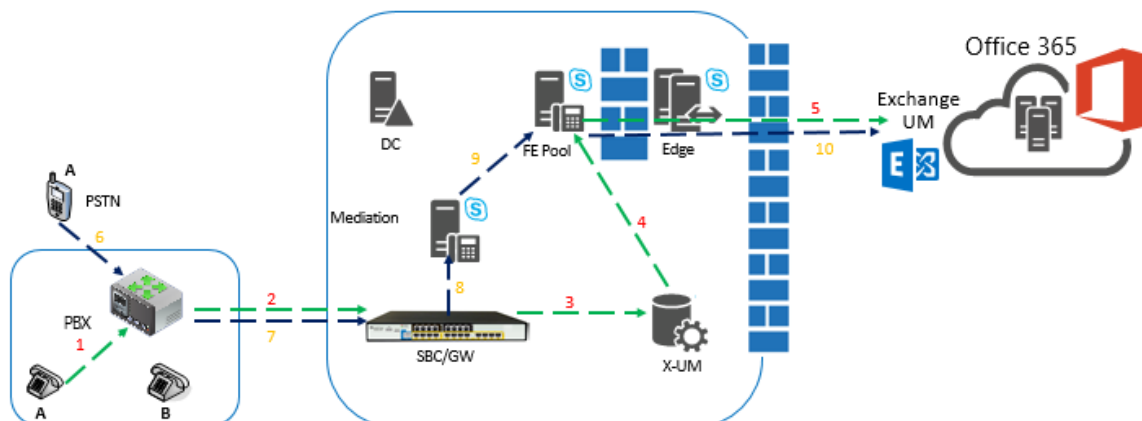
Figure 2-4: Message Waiting Indication (SIP Subscription)



1. X-UM Application Subscribes for Exchange MWI via the FE and Edge.
2. The phone subscribes to MWI notifications. The subscription is forwarded by PBX and SBC to X-UM.
3. Due to voicemail status changes, Office365 sends the MWI message to the X-UM via the FE and Edge.
4. X-UM replace the SIP URI with the phone extension and sends the MWI notification in the SIP subscription dialog to the PBX via the SBC.
5. The PBX sends the MWI to the phone.

2.3.5 Outlook Voice Access– User Access to Mailbox via Telephone

Figure 2-5: Outlook Voice Access– User Access to Mailbox via Telephone



Access from Extension:

1. A calls Special number (Voice Mail key on the phone).

2. The PBX forwards the call to the SBC.
3. SBC forwards the call to X-UM – DN must be the number which was set on X-UM for subscriber login.
4. X-UM validates that the caller is managed by the users file and forwards the call to FE as a direct subscriber login to voicemail.
5. The call is sent to Office365 Exchange UM via the Edge server.



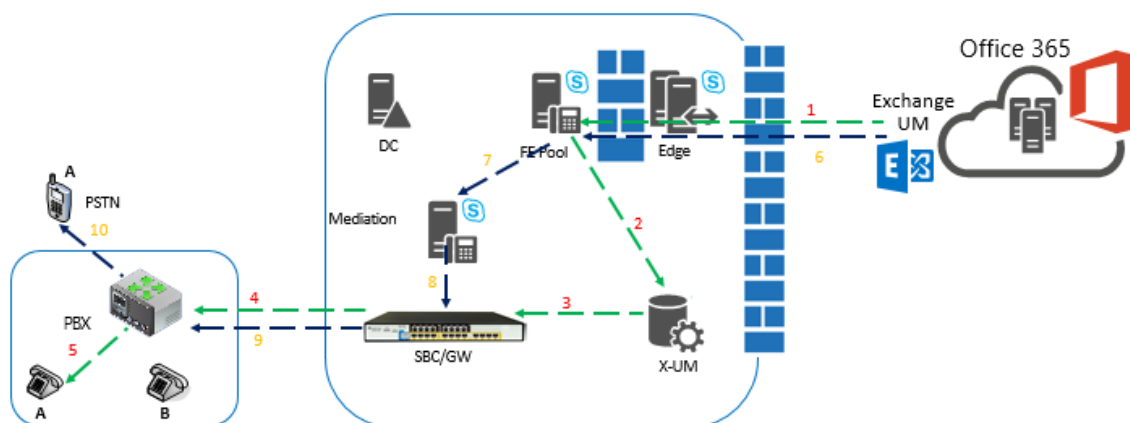
Note: By default in this flow, Exchange UM does not ask for password, which can be changed on the X-UM setup.

Access from External phone:

6. A calls from PSTN to Special ATT number.
 7. The PBX forwards the call to the SBC.
 8. SBC forwards this call to the Mediation server.
 9. The Mediation server forwards the call to FE.
 10. FE forwards the call to Exchange UM via the Edge server.
- Exchange UM prompts for the mailbox number and password.

2.3.6 Play-on-Phone

Figure 2-6: Play-on-Phone



Call to User SIP URI/or user Extension:

On Outlook, User A requests to play the message on his phone:

1. Exchange UM dials to user A via Edge and FE.
2. X-UM receives the call because it registers as user A.
3. X-UM forwards the call to SBC replacing the SIP URI user extension.
4. SBC calls user extension on the PBX.
5. PBX calls user phone.

Call to External number:

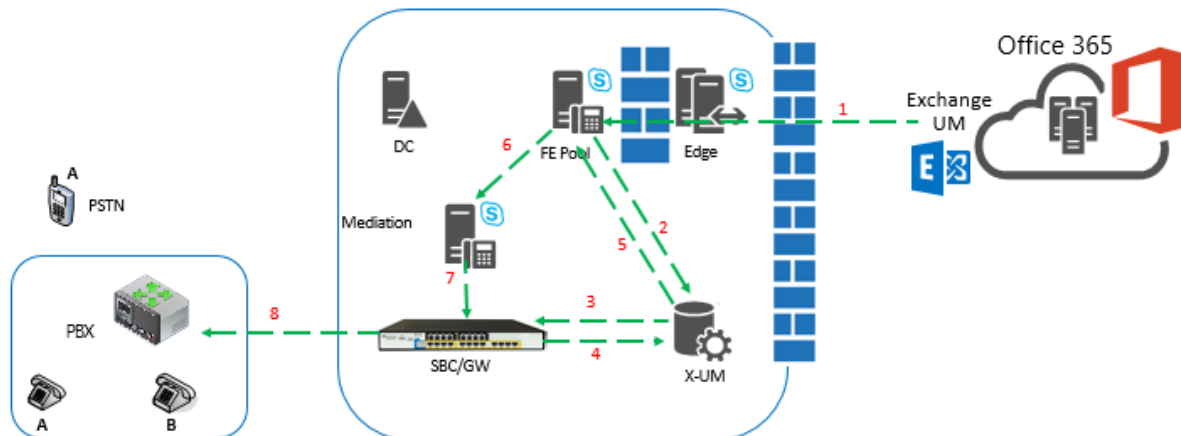
On Outlook, User A requests to play the message on his Mobile phone:

6. Exchange UM dials to user A mobile via Edge and FE.
7. FE dials to the Mediation server.

8. The Mediation server calls SBC.
9. SBC calls user extension on the PBX.
10. PBX calls user phone.

2.3.7 Outlook Voice Access Call Out – User Access to Mailbox via Telephone and Call out

Figure 2-7: User Access to Mailbox via Telephone and Call out



User A accesses the mailbox from internal phone or External according to flow: “**Outlook Voice Access– User access to mailbox via telephone**”

User A selects to dial to a contact:

1. Exchange UM sends REFER message.
2. FE send the REFER to X-UM.
3. X-UM sends a self REFER + REPLACES to SBC.
4. SBC sends new INVITE + REPLACES to X-UM.
5. X-UM sends the INVITE (to the contact) to the FE.
6. FE calls Mediation server for external numbers and to Lync clients (and X-UM too) for internal users.
7. Mediation sends the call to SBC.
8. SBC sends call to PBX and PBX calls out.



Note: If contact is a Lync user registered on X-UM, then XUM accepts the call and forwards it to the SBC, PBX and user phone.

2.4 Debugging tools

X-UM Connector debugging tools - see Chapter 14.

2.5 Re-image X-UM Standard

Re-image X-UM is done according to the CB365 re-image and installation procedure which does not install the VM for the X-UM Connector. Therefore you must add an extra clean VM for the X-UM Connector and bring it to the state as provide from production.

In the next main version, the CB365 wizard will install the X-UM connector and will set it correctly as is the case for all other CB365 VMs.

For more information, see Chapter 1415.

This page is intentionally left blank.

3 Default Configuration and Login Information

The default configuration of the X-UM Standard is detailed below.

3.1 X-UM Standard Server information

3.1.1 Login

- **Username:** cloudbond365\Administrator
- **Password:** R3m0t3Supp0rt

3.1.2 IP Address Information

- UC-DC 192.168.0.101
- UC-FE 192.168.0.102
- UC-EDGE 192.168.0.103 (internal)
- UC-EDGE 192.168.254.103 (external)
- UC-RP 192.168.0.104 (internal)
- UC-RP 192.168.254.104 (external)
- UC-XUM 192.168.0.105 (Not installed by default)
- All subnet masks 255.255.255.0

3.1.3 X-UM Standard Domain Information

- Internal FQDN cloudbond365.local
- NetBIOS domain cloudbond365

3.1.4 X-UM Standard Default Skype for Business Topology

- **Default SIP Domain**
 - cloudbond365.local
- **Simple URL's**
 - <https://meet.cloudbond365.local/dialin>
 - <https://meet.cloudbond365.local/meet>
- **FE Pool**
 - uc-fe.cloudbond365.local
- **External Web**
 - ewslync.cloudbond365.local
- **Edge Pool**
 - uc-edge.cloudbond365.local
 - Access Edge sip.cloudbond365.local:5061
 - Web Conferencing sip.cloudbond365.local:444
 - A/V Edge sip.cloudbond365.local:443

3.2 SBC Mediant 800 Information

3.2.1 Login

- **Username:** Admin
- **Password:** Admin

3.2.2 IP Address Information

- **Mediant 800 Gateway:** 192.168.0.2

4 Changing Default Hyper-V Settings & Importing X-UM Connector

This section includes the following:

- Stop the Reverse Proxy
- Change Front-end Memory Size
- Add the X-UM Connector Virtual Machine
- Re-Join the X-UM to the Domain

4.1 Stop the Reverse Proxy

X-UM Standard does not require Reverse Proxy. CloudBond is packaged with Reverse Proxy installed by default. To save resources, stop the Reverse Proxy server and disable it by doing the following:

➤ **To stop the Reverse Proxy:**

1. Open the Hyper-V Manager.
2. Shut down the Reverse Proxy virtual machine.
3. Delete the Reverse Proxy virtual machine.

The VHDX of the Reverse Proxy will not be deleted. If it is needed in the future we can create it from the VHDX.

4.2 Change Front-End Memory Size

The procedure below describes how to change the front-end memory size.

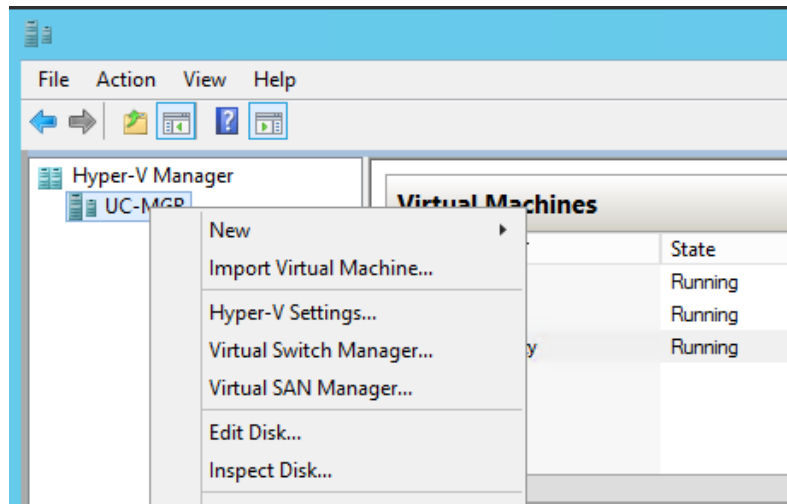
➤ **To change the front-end memory size:**

1. Open the Hyper-V Manager.
2. Stop the Front-End server. Change the memory size to 12 Gb.
3. Start the Front-End server.

4.3 Add the X-UM Connector Virtual Machine

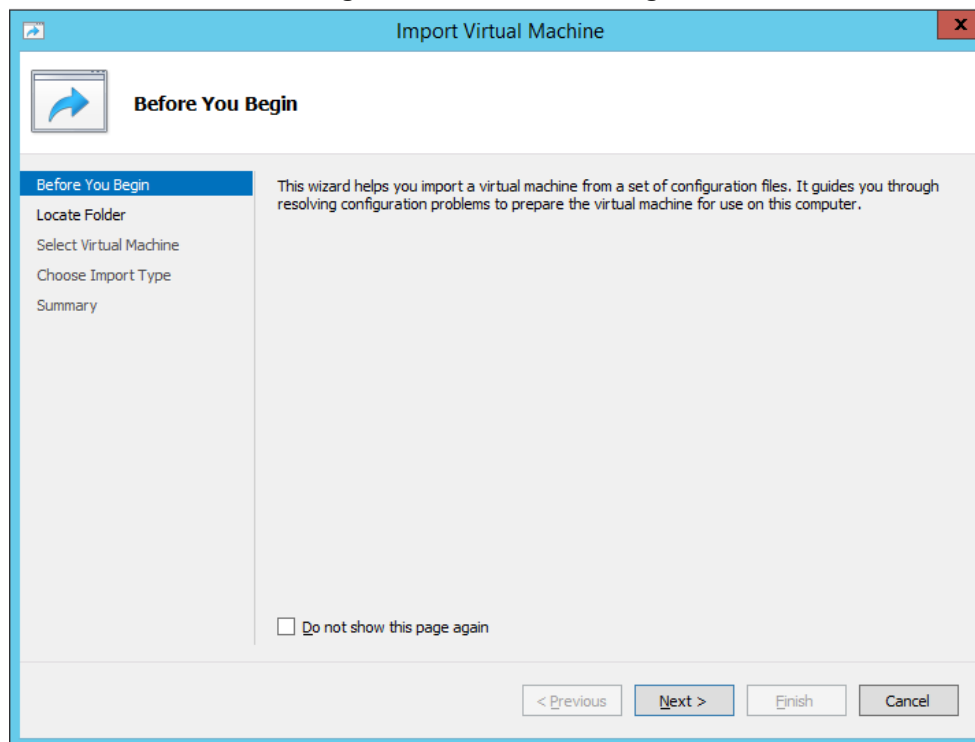
1. Open the **Hyper-V Manager**.
2. Right-click on **UC-MGR** (tree item); the following screen appears:

Figure 4-1: Hyper-V Manager



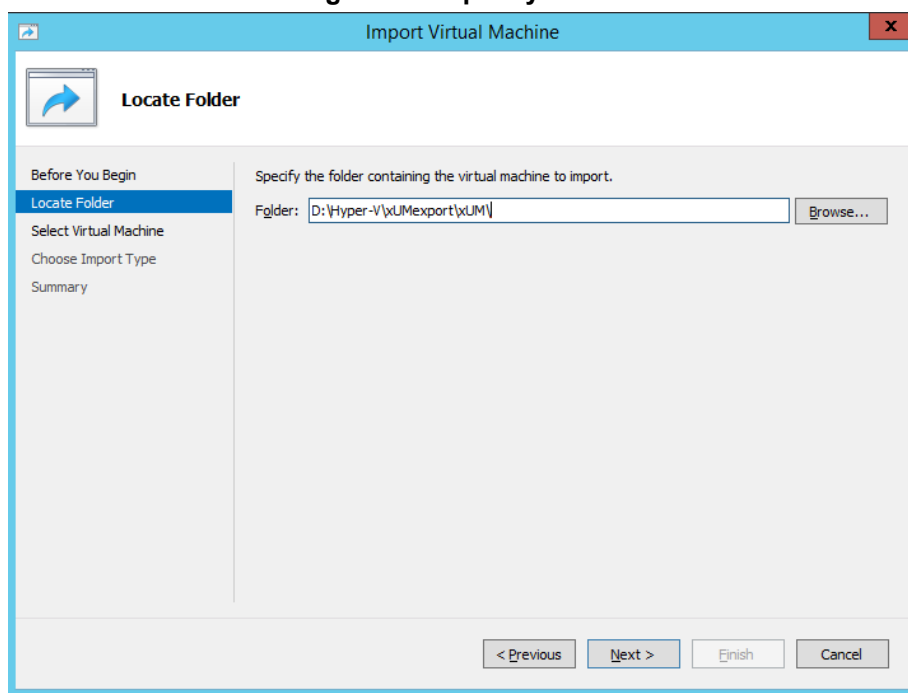
3. Click **Import Virtual Machine**; and then select **Virtual Machine**; the following screen appears:

Figure 4-2: Before You Begin



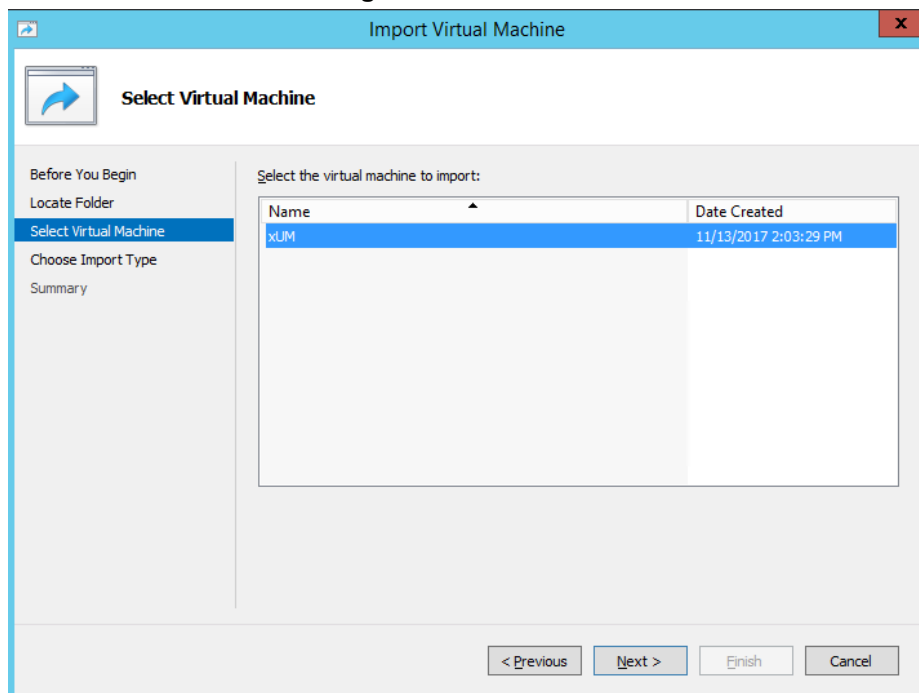
4. Click **Next**; the following screen appears:

Figure 4-3: Specify Folder



5. In the 'Folder' field, browse to **D:\Hyper-V\xUMexport\xUM**.
6. Click **Next**; the following screen appears:

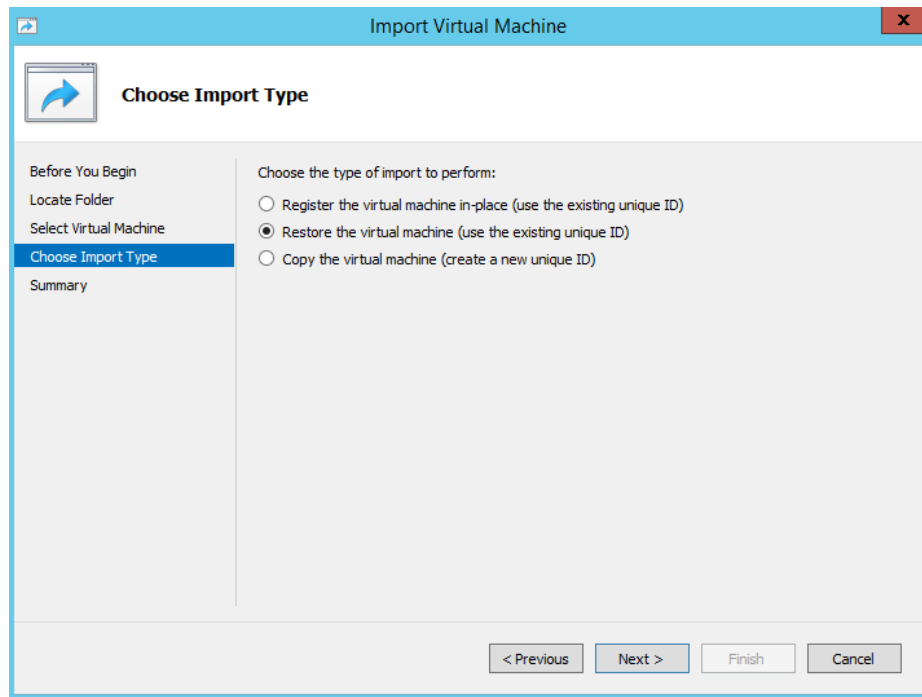
Figure 4-4: Select VM



7. Select the 'xUM' virtual machine.

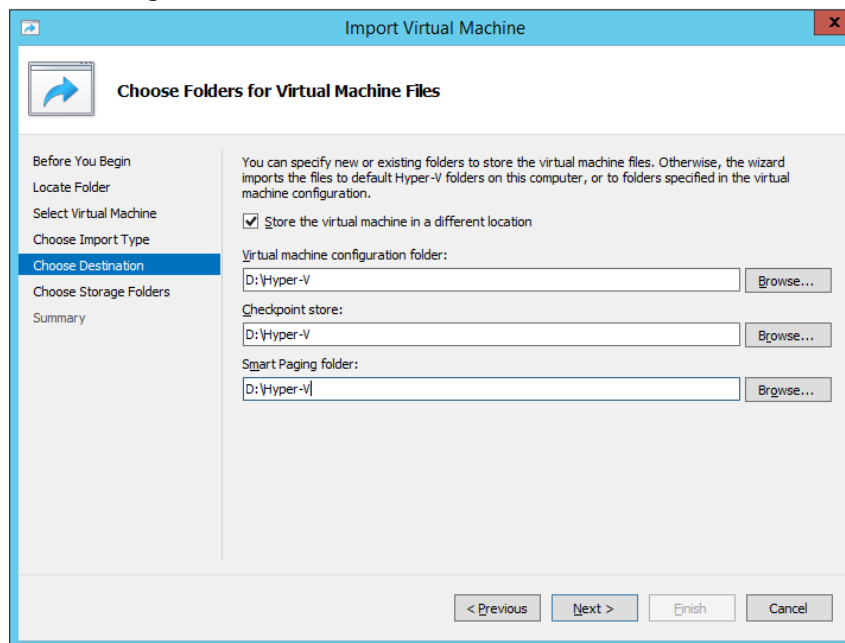
8. Click **Next**; the following screen appears:

Figure 4-5: Import Type

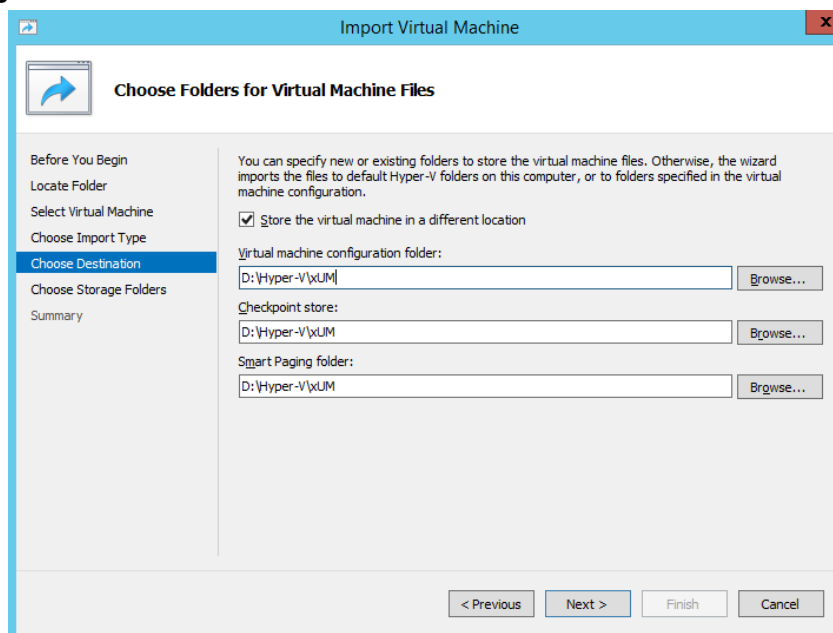


9. Select 'Restore the Virtual machine'.
10. Click **Next**; the following screen appears:

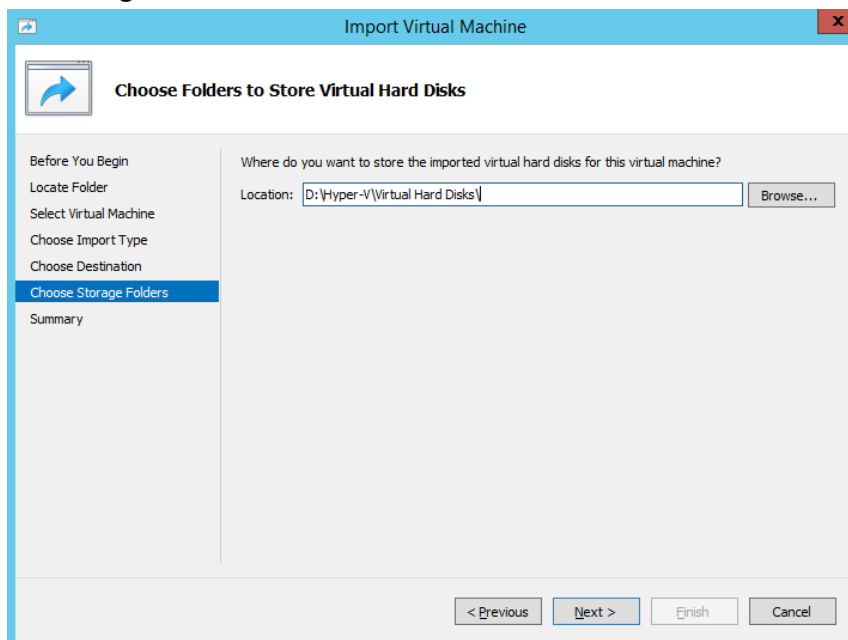
Figure 4-6: Choose Folders – Choose Destination



11. Check 'Store the virtual machine in different location'
12. In the 'Virtual machine configuration folder' field, browse to D:\Hyper-V\xUM.
13. In the 'Checkpoint store' field, browse to D:\Hyper-V\xUM.
14. In the 'Smart paging folder' field, browse to D:\Hyper-V\xUM.

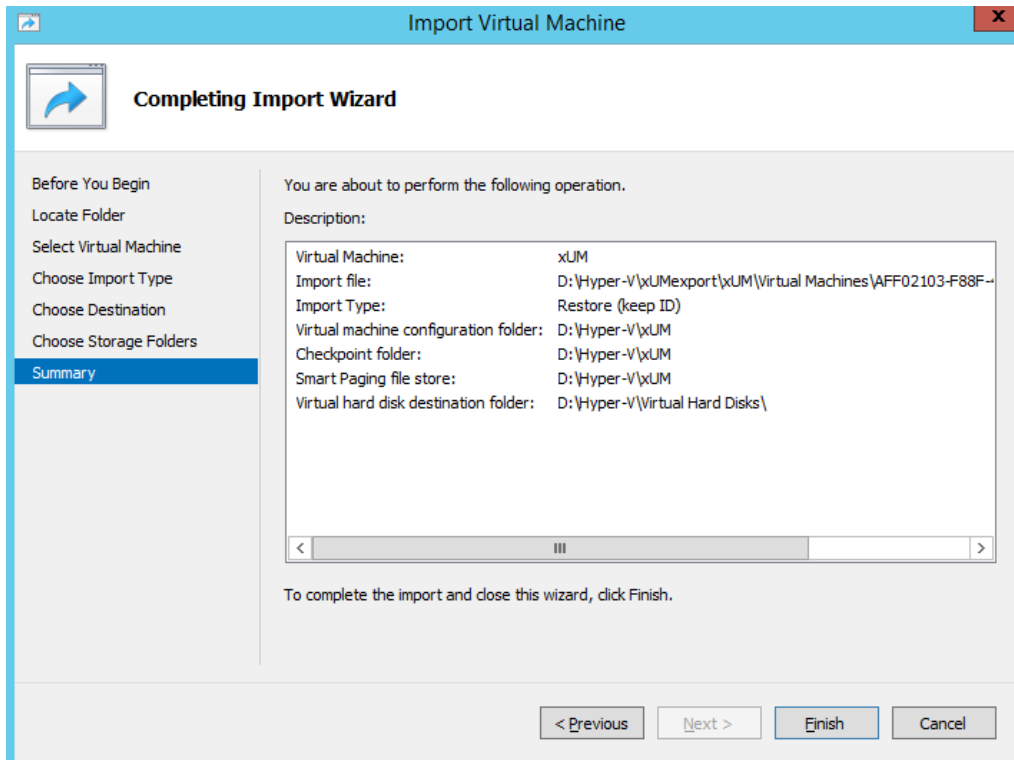
Figure 4-6: Choose Folders – Choose Destination – Virtual Machine Files

15. Click **Next**; the following screen appears:

Figure 4-6: Choose Folders to Store Virtual Hard Disk

16. In the Location' field, browse to **D:\Hyper-V\Virtual Hard Disks**.
17. Click **Next**; the following screen appears:

Figure 4-7: Complete Import Wizard

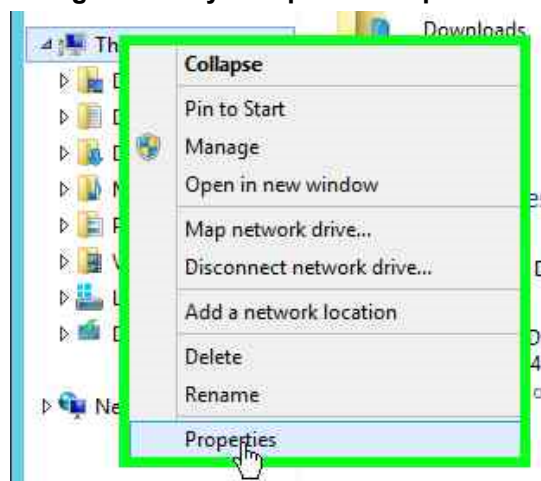


18. Click **Finish**; the import procedure will start. It can take approximately 25 minutes.
19. Start the xUM Virtual machine.

4.4 Re-Join the X-UM to the Domain

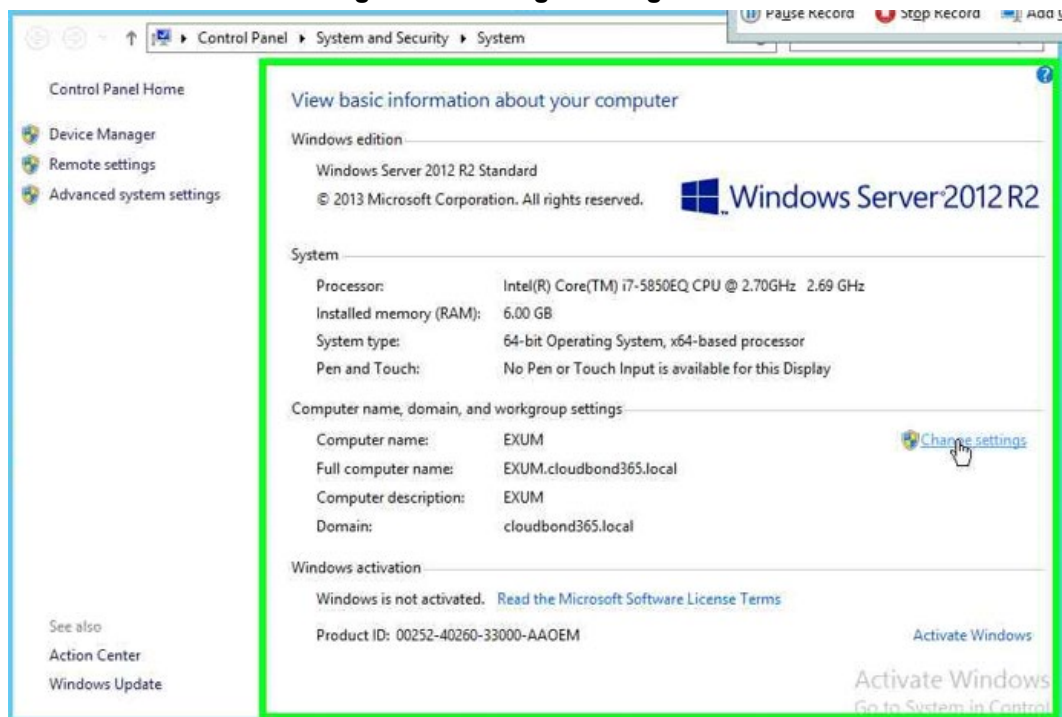
1. Login to the X-UM virtual machine.
2. From the Desktop, select the **My Computer** icon and right-click to view the settings.
3. Select **Properties**.

Figure 4-1: My Computer - Properties



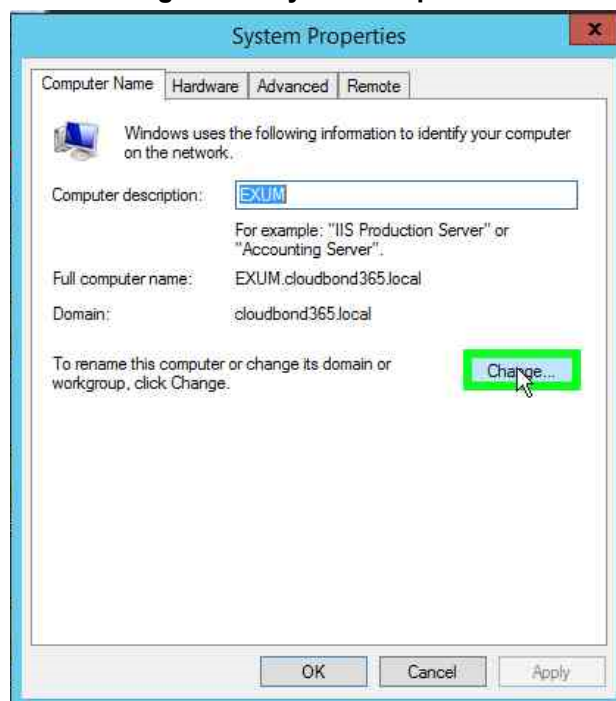
4. On the Windows Server 2012 R2 screen, click **Change settings**.

Figure 4-2: Change Settings Link



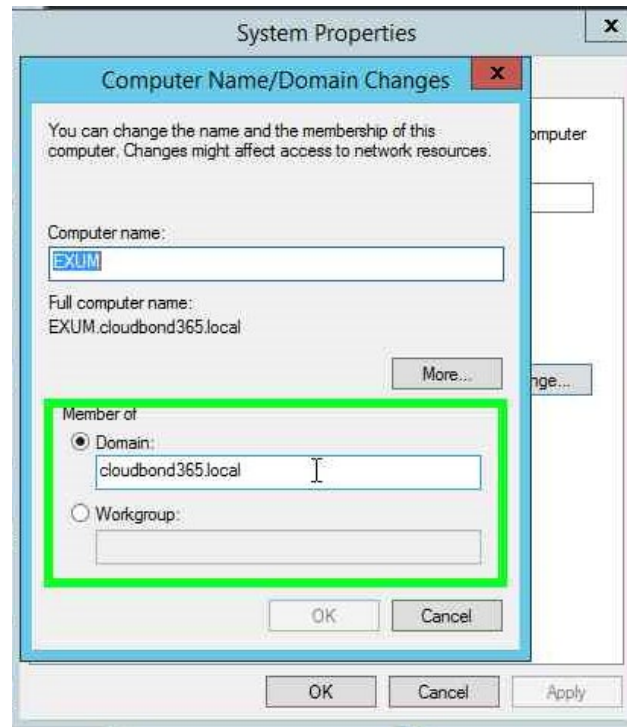
5. On the System Properties screen, click **Change**.

Figure 4-3: System Properties



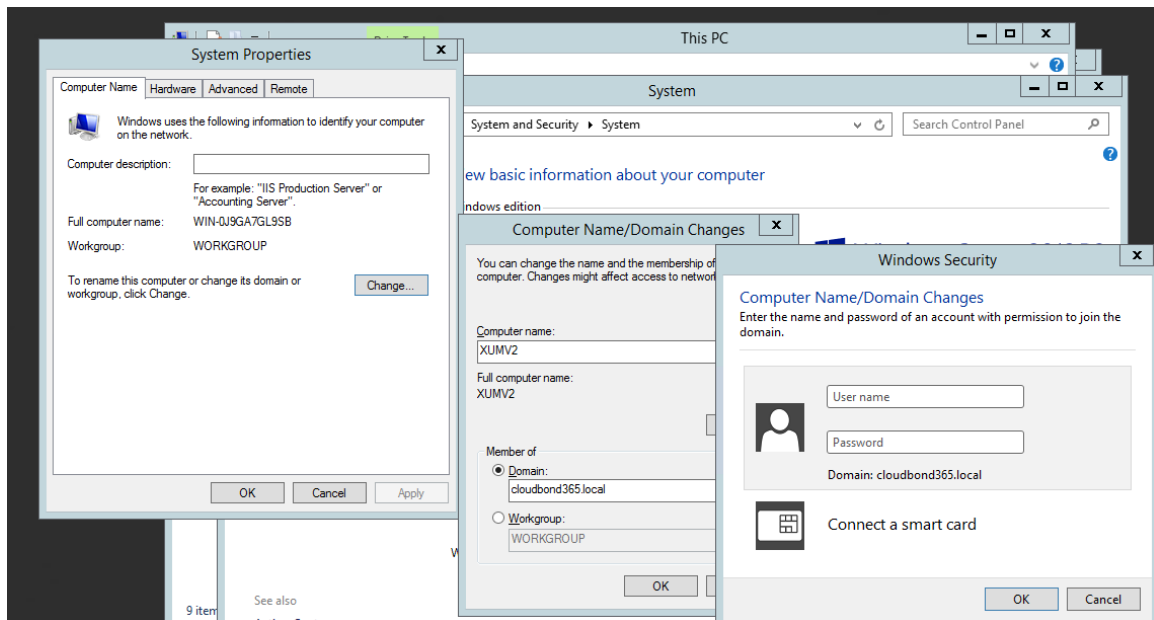
6. Change the **Domain** to be **cloudbond365**, and then click **OK**.

Figure 4-4: System Properties - Change



7. Insert the user name and password of CloudBond365 Administrator, and then click **OK**.

Figure 4-5: Windows Security



8. Restart the X-UM machine.

5 Assigning Manual IP Address

This section describes how to manually configure the IP addresses used by the X-UM Standard servers. Note the following:

- Information about manually configuring IP addresses for the X-UM Standard servers.
- This guide assume you are familiar with the Windows 2012 R2 Network configuration, modifying and deploying the Skype for Business topology, editing the hosts file, and verifying DNS entries etc.

A X-UM Standard System usually has various external optional components with which it communicates. These include Media Gateways, Session Border Controllers, Reverse Proxy Servers, Hardware Load balancers, IP PBX's etc. You may need to consult the individual documentation for such external devices to change their IP addresses.

5.1 Planning Your Network Changes

It is very important to plan your network IP addressing scheme before making changes to the default settings. It is very easy to render the X-UM Standard system inoperative by misconfiguring the underlying IP network.

Consult the CloudBond 365 Intake Form to record your IP Network configuration prior to making any network changes.

5.2 Making Changes to X-UM Standard

You may make changes to the X-UM Standard IP Network by either:

- Attaching a local Monitor, Keyboard, and Mouse to the X-UM Standard rear panel
- Starting an RDP Session to the X-UM Standard Controller. Each option has advantages and disadvantages.

5.2.1 Using Local Monitor, Keyboard, and Mouse

Using a local monitor, keyboard and mouse allows you to make changes to the X-UM Standard system without “losing connectivity” should you make an error in configuration. However, it does require physical access to the X-UM Standard, which may be difficult when installed in a server rack.

5.2.2 Use RDP Sessions

Using RDP sessions to connect to the X-UM Standard Controller is a convenient way of making configuration changes. However, care must be taken with the sequences of network changes. RDP relies on the very network you are changing for its connectivity, and so it is easy to “kill” RDP access through configuration errors.

5.3 Changing IP Addresses

Changes to IP addresses may be required to both X-UM Standard core server components, as well as hardware devices and servers external to the X-UM Standard software. You may also have to update the DNS server to reflect the changes.

X-UM Standard Core Components:

- Change the IP addresses for each individual server (Controller, Front-End, Edge, X-UM Connector)
- Confirm IP addresses in DNS server
- Change topology entries
- Change Static DNS records

Devices and Servers external to the X-UM Standard software are typically optional components, depending upon your chosen X-UM Standard product and individual customer configuration.

For example, X-UM Standard includes an AudioCodes Mediant 800 gateway device which will probably require an IP address change. X-UM Standard External Components include the following:

- Change any Media Gateway addresses, including Mediant 800 IP address
- Change Office Web Apps Server IP address

When changing external components, such as Media Gateways and SBC's, you may need to make corresponding changes in the Skype for Business topology, and also update any certificates if TLS communication is used.

5.3.1 Changing IP Addresses for Each Individual Server

Using RDP sessions to each server (or Hyper-V sessions from the X-UM Standard Controller) you may change the IP address settings in Windows 2012 R2 for all individual servers (as shown in the figure below for the DC).

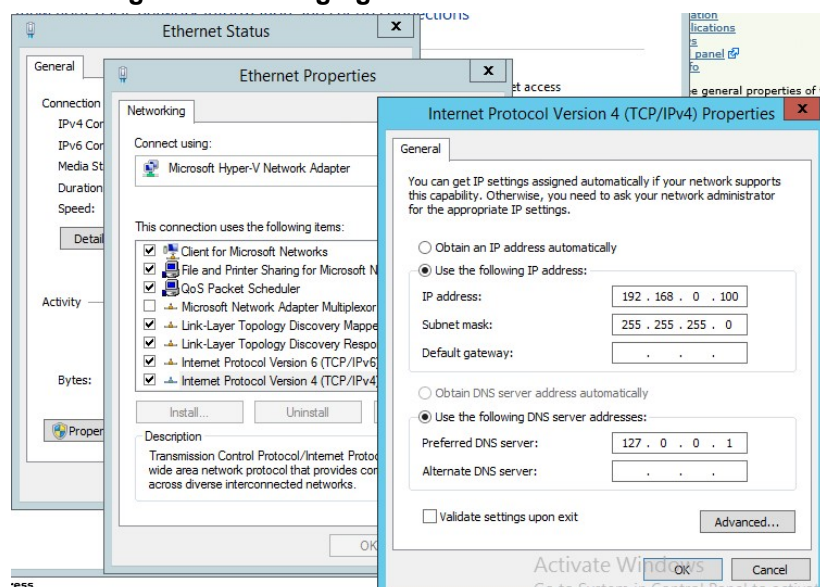


Note: The Edge server will have two interfaces, one for the internal IP and one for the external IP. The external DNS should point to a public DNS provider, such as your ISP. The internal DNS and gateway should be empty, as a Hosts file is used to lookup the internal server addresses.

➤ **To change the IP addresses for each server:**

1. In the Network and Sharing Center, click the **Ethernet** button; the Ethernet Status screen is displayed.
2. Select the IP interface and then click **Properties** to change the IP address settings as shown in the figures below.

Figure 5-1: Changing Individual Server Addresses





Warning: Do not use a primary DNS address of 127.0.0.1 on a Domain Controller. Performing such an action will break forest trusts and prevent normal activities between the customer domain and the X-UM Standard domain. Instead, use the actual Domain Controller IP address, such as 192.168.0.101.

5.3.2 Confirming IP Addresses on DNS Server

After changing the IP addresses in Windows 2012 R2, it is useful to confirm that the new IP addresses are correct. This can be done by performing simple PING tests from each server, and by checking the forward lookup zone within the DNS server on the X-UM Standard Controller. The PING test should be performed by the IP address as well as the DNS name.

➤ **To confirm IP addresses on the DNS Server:**

1. Open the Command Prompt and perform the PING tests.

Figure 5-2: PING Tests

```
Administrator: Command Prompt

C:\Users\Administrator>ping acs-uc-fe.acs-unified-communications.net

Pinging acs-uc-fe.acs-unified-communications.net [192.168.0.101] with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping acs-uc-edge.acs-unified-communications.net

Pinging acs-uc-edge.acs-unified-communications.net [192.168.0.103] with 32 bytes of data:
Reply from 192.168.0.103: bytes=32 time<1ms TTL=128
Reply from 192.168.0.103: bytes=32 time<1ms TTL=128
Reply from 192.168.0.103: bytes=32 time<1ms TTL=128
Reply from 192.168.0.103: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

2. Open the DNS Manager (**Server Manager > DNS** and then in the Toolbar, choose **Tools > DNS**).

Figure 5-3: Check DNS Updates

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[130], dc.cb106.com., host...	static
(same as parent folder)	Name Server (NS)	dc105.cb106.com.	static
(same as parent folder)	Name Server (NS)	dc.cb106.com.	static
(same as parent folder)	Host (A)	10.21.57.45	1/27/2017 2:00:00 PM
(same as parent folder)	Host (A)	10.21.57.55	1/27/2017 8:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:7a4c...	1/31/2017 8:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:0b9c6...	1/27/2017 7:00:00 PM
cb105	Host (A)	10.21.57.56	1/31/2017 8:00:00 PM
cb105	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:4537e...	1/31/2017 8:00:00 PM
CB107	Host (A)	10.21.57.52	1/31/2017 11:00:00 AM
dc	Host (A)	10.21.57.45	static
dc	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:0b9c6...	static
DC105	Host (A)	10.21.57.55	static
DC105	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:7a4c...	static
DC107	Host (A)	10.21.57.51	1/31/2017 12:00:00 PM
DC107	Host (A)	10.21.2.34	1/31/2017 12:00:00 PM
Edge	Host (A)	10.21.57.47	static
FE	Host (A)	10.21.57.46	1/27/2017 7:00:00 PM

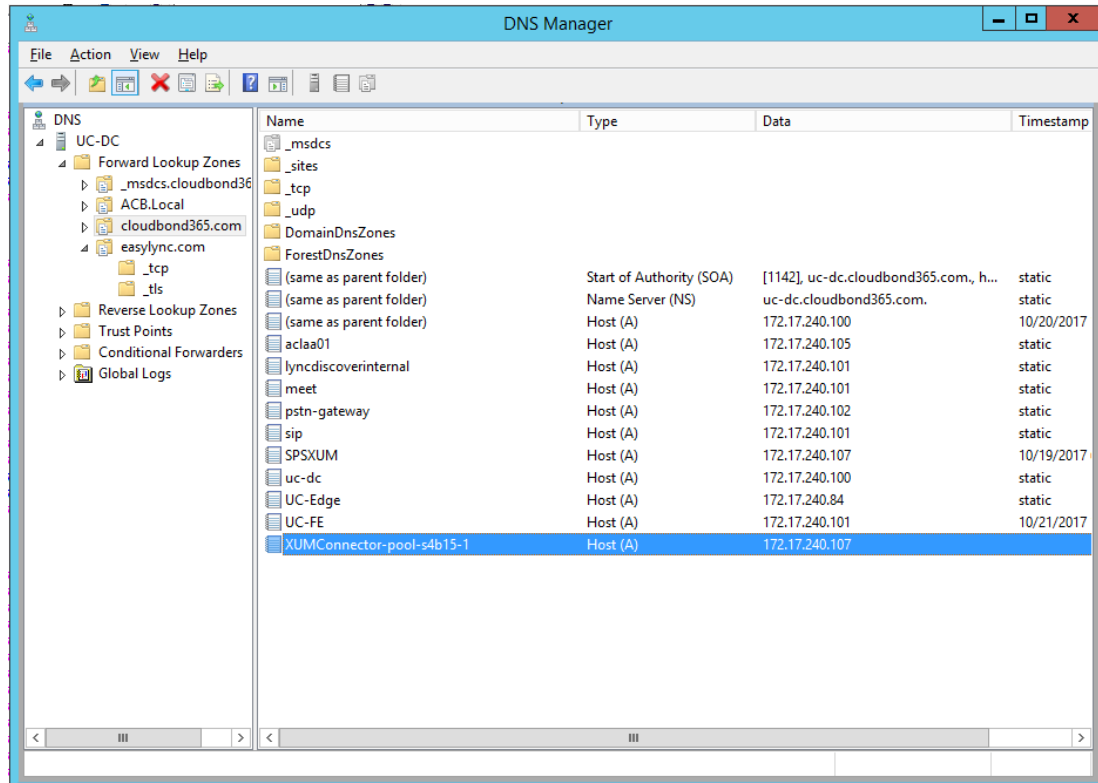


Note: The DNS entries may not update immediately in the DNS server.

5.3.3 Changing X-UM Connector Pool Entry

On the DNS server, change the X-UM Connector Pool Entry to point to the new IP of the X-UM Connector Virtual Machine.

Figure 5-3: Changing X-UM Pool Entry



5.3.4 Changing Topology Entries

On the X-UM Standard Controller server (UC-DC), start the Skype for Business Topology builder, then modify the following entries as required. After completing you topology changes, you will need to publish the topology. The following topics are described:

- Default sip domain
- Simple URL's
- Edge Settings
- Publish Topology



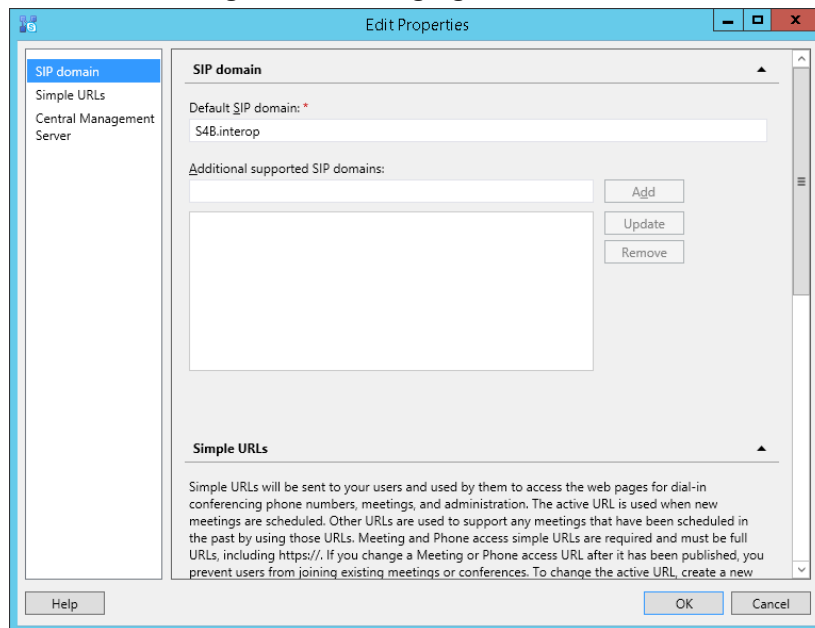
Note: Whilst changes to IP addresses are generally simple and require nothing further, changes to SIP Domains and Simple URL's are closely tied to Certificates within Skype for Business. Before changing SIP Domains and Simple URL's, see Chapter 6 for more information.

5.3.4.1 Changing Default SIP Domain

If you have changed the name of your SIP domain to match your existing email or active directory domain, you will need to modify the Default SIP domain entry, or add an addition supported domain within the Skype for Business topology. It is recommended to add additional supported SIP domains, rather than modify the default SIP domain.

- **To change SIP domains:**
- Open the Topology Builder, right-click the server (**Skype for Business Server 2015\Lync Server 2013**) and choose **Edit > Properties**.

Figure 5-4: Changing SIP Domains



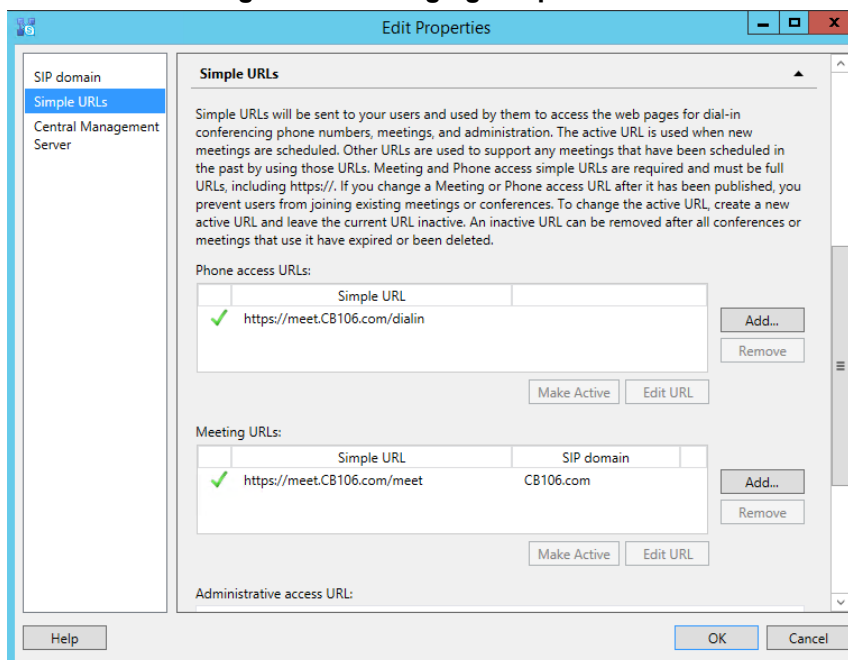
Note: Under some circumstances, such as when using Office 365 with Exchange Online as a voicemail server for PSTN calls, it is **necessary** to change the default SIP domain. Even in these cases, it is easier to add the new domain as an “Additional SIP domain”, then at a later time use the Skype for Business Management Shell to issue the following command:

```
Set-CsSipDomain -Identity contoso.com -IsDefault $True
```

5.3.4.2 Changing Simple URL's

You may need to change the Simple URL's.

- **To change simple URLs:**
- Open the Topology Builder, right-click the server (**Skype for Business Server 2015\Lync Server 2013**), choose **Edit > Properties** and then in the Navigation pane, select **Simple URLs**.

Figure 5-5: Changing Simple URL's

5.3.4.3 Changing Edge Settings

The Edge server settings within the topology contains IP address information which need to match any changes you have made.

➤ **To change the Edge Server settings:**

- Open the Topology Builder and then the Edge pools folder.

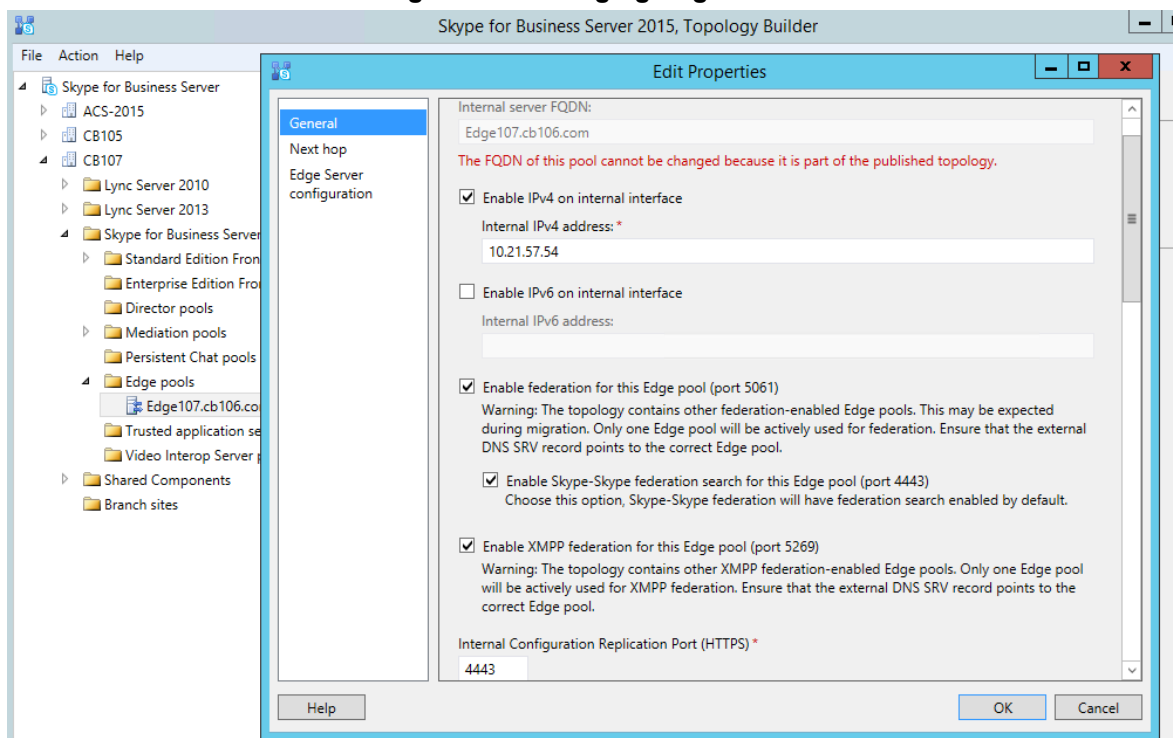
Figure 4-6: Changing Edge Server

Figure 5-7: Changing Edge Server

Edit Properties

General

Next hop

Edge Server configuration

External settings

Specify the external, fully qualified domain names (FQDNs) and ports for Access Edge, Web Conferencing Edge, and A/V Edge services. The combinations of FQDN and port must be unique.

☐ Enable separate FQDN and IP address for web conferencing and A/V

☒ Enable IPv4 on external interface

☐ Enable IPv6 on external interface

☐ A/V Edge service is NAT enabled

Access Edge service

FQDN: *
sip.contoso.com

Ports
: 5061 (TLS)

IPv4 address: *
192.168.254.103

IPv6 address:

Web Conferencing Edge service

FQDN:
sip.contoso.com

Ports
: 444 (TLS)

IPv4 address:
192.168.254.103

Help OK Cancel

In addition to the topology changes, the Edge server must know how to reach each internal subnet. This will be accomplished by using the “**route add <network address> mask <subnet mask> <gateway> metric 10 -p**” command in an elevated command prompt.

Example: To instruct the Edge server to use the 192.168.0.254 gateway for all traffic destined for the 192.168.0.0/24 network, use the following command:

```
"route add 192.168.0.0 mask 255.255.255.0 192.168.0.254 metric 10 -p".
```

Repeat this step for all network subnets that are internal and rely on the Edge server for media traversal.

5.3.5 Publishing the Topology Changes

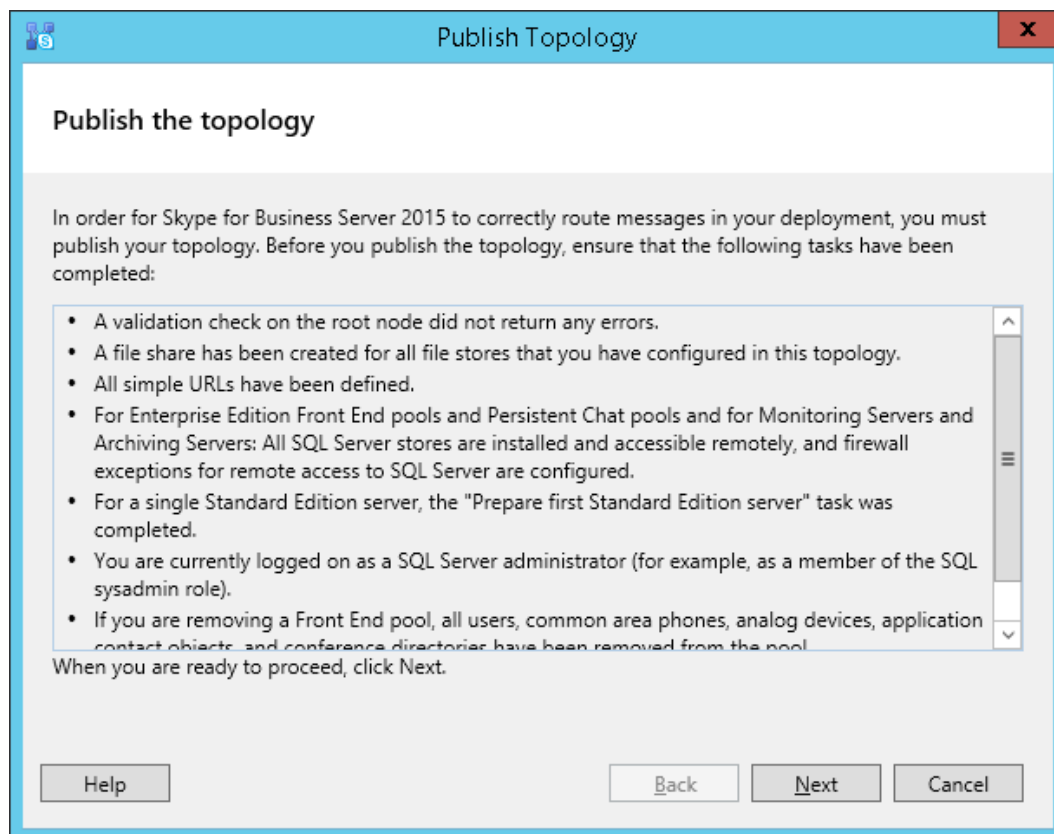
Once all topology changes are complete, publish the Skype for Business topology.

You will then need to use RDP etc. to connect to both the Front-end (FE) and Edge servers, and run the Skype for Business Deployment Wizard to update the changes.

➤ **To publish the topology changes:**

- In the Skype for Business 2015 Topology Builder menu, choose **Action > Publish Topology**.

Figure 5-1: Publish Topology



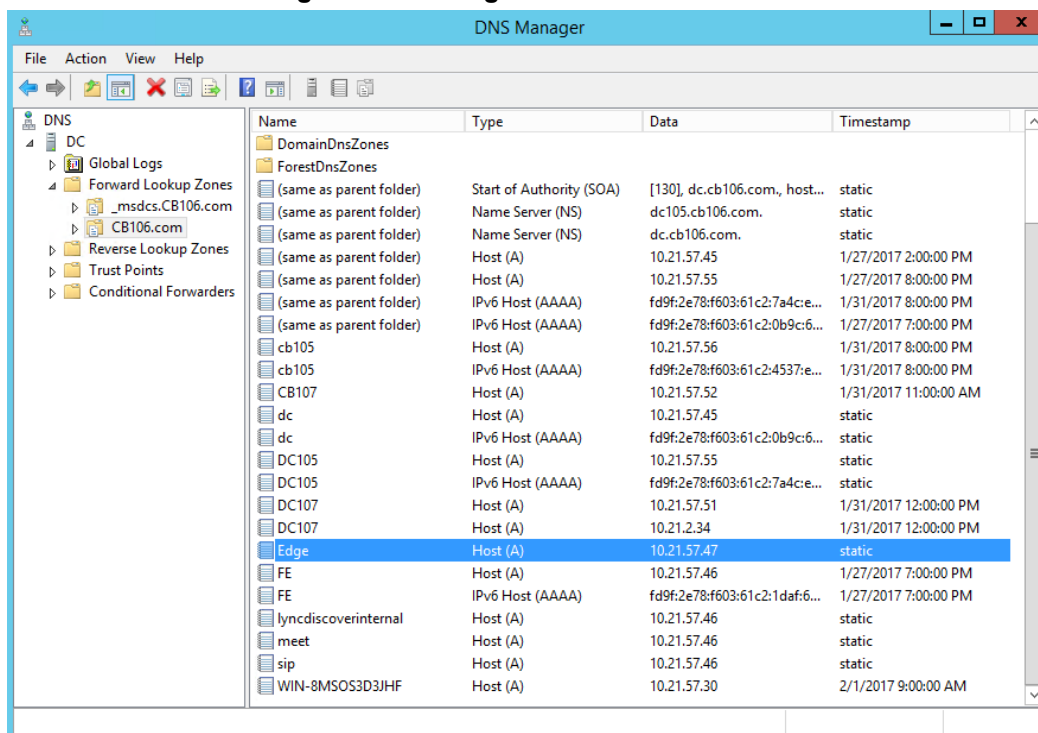
5.3.6 Changing Static DNS Records

The CloudBond 365 Edge server is not part of the CloudBond X-UM domain for security reasons. As such, it uses a static DNS table (Hosts file) to find the IP addresses of the CloudBond X-UM servers on the internal network. Use the DNS entries from the CloudBond X-UM Controller to manually update the Hosts file on the Edge server.

➤ **To change static DNS records:**

- Open the DNS Manager (**Server Manager > DNS** and then in the Toolbar, choose **Tools > DNS**).

Figure 5-2: Change Static IP DNS Entries



5.3.6.1 Modifying the Edge Server Hosts File

The Edge server is not a domain member, and has no reference to the internal DNS server. You will need to manually edit the c:\windows\system32\drivers\etc\hosts file, so the Edge server can find the internal server FQDN names.

➤ To modify the Edge Server Hosts file:

1. On the Edge server, open the Hosts file (C:\Windows\System32\drivers\etc).
2. Edit the file as required.

Figure 5-3: Locating the Hosts file

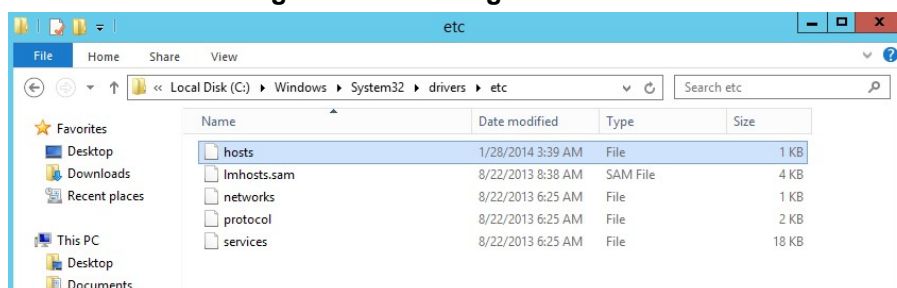
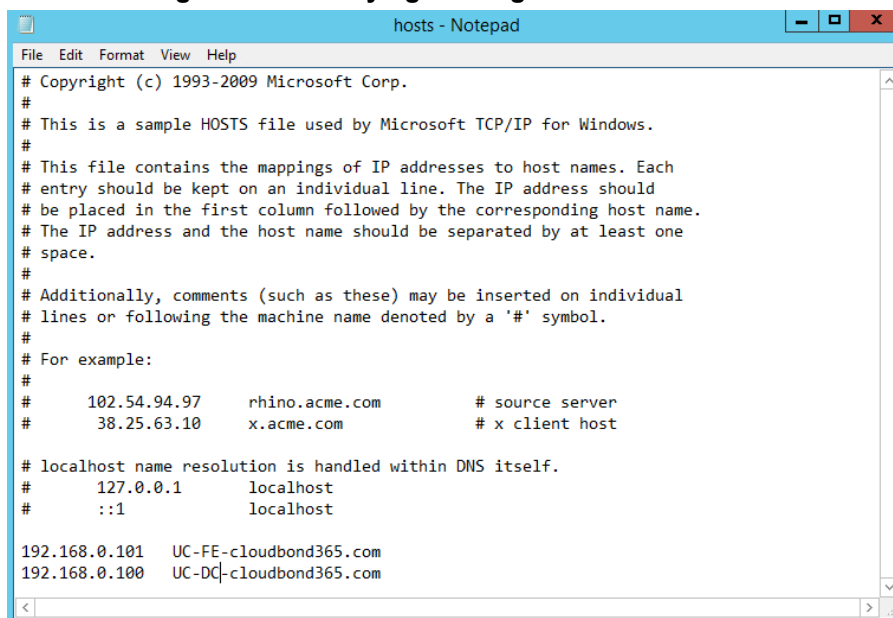


Figure 5-4: Modifying the Edge Server Hosts File

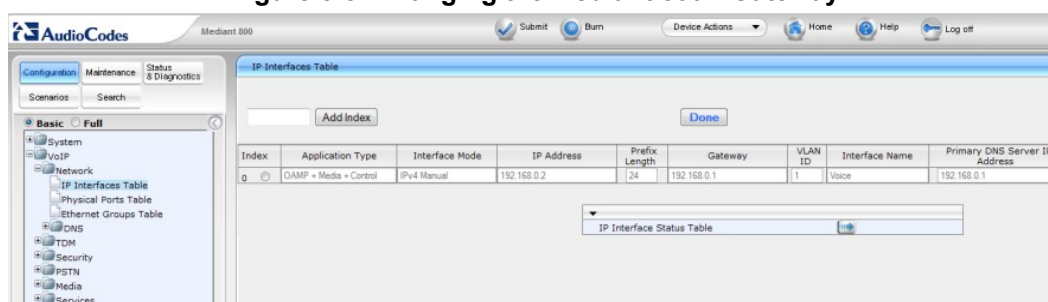
5.3.7 Changing the IP Address of AudioCodes Devices

For the system to function correctly, the Mediant 800B should be assigned with an address on the same internal network subnet as the CloudBond X-UM Controller.

5.3.7.1 Changing Mediant 800B IP Address

The CloudBond X-UM system uses an AudioCodes Mediant 800B appliance as a PSTN gateway device. The Mediant 800B device usually provides the physical network connection for the CloudBond X-UM Controller via the Mediant 800 front panel GE1 connector.

You can modify the default IP address assigned to the Mediant 800B (192.168.0.2) via its Web configuration pages. Please consult your AudioCodes trained expert for details.

Figure 5-5: Changing the Mediant 800B Gateway

This page is intentionally left blank.

6 Changing or Adding a SIP Domain

This chapter describes how to change or add a SIP domain to the X-UM Standard system. The SIP domain is very important for Skype for Business operations, as it provides the sign-on and various other addresses within a Skype for Business environment. As Skype for Business uses TLS as a secured protocol, many other items must match the SIP address.



Note: You must change or add a valid SIP domain for external access as the default SIP domain (yourdomain.com) and associated Simple URL's. For example, DNS references are not suitable for the public internet.

6.1 Skype for Business and the SIP Domain

Skype for Business supports a primary SIP domain, and additional SIP domains.

Microsoft recommends that the SIP domain should match a user's email domain. This simplifies many features of Skype for Business for the user, such as logging in using a Skype for Business Client, where the user logs in using a SIP domain.

Skype for Business clients with automatic configuration use the users sign-in domain component (i.e., the users SIP Domain) to locate Skype for Business Server resources via DNS.

6.1.1 DNS and Simple URLs

DNS records are used both internally and externally to Locate Skype for Business resources. Skype for Business Simple URL's are used for external login and conferencing features.

Whilst Skype for Business supports several configurations of Simple URL, the most common involve embedding the SIP domain within the Simple URL. Corresponding DNS records are required to support the Simple URLs.

6.1.2 DNS and Certificates

Because Skype for Business uses TLS as a transport protocol, this secure protocol requires SSL certificates, which must match the DNS resources to which they correspond. Commonly, the required SSL certificates thus include the SIP Domain.



Note: You can have additional SIP domains for internal use only. If these domains are not accessed externally, they will not require public certificate entries.

6.1.3 X-UM Standard and the SIP Domain

A X-UM Standard system has a default Primary SIP domain of cloudbond365.local. After deployment, the SIP domain must be added or changed to meet customer requirements for external access.



Warning: The default SIP domain (cloudbond365.local) of a X-UM Standard system cannot be used for external public access.

It is generally easier to add your email domain as an additional SIP Domain, rather than replace the Primary SIP Domain.

6.2 Changing X-UM Standard SIP Domain

Modifying the X-UM Standard SIP domain is not a simple process. Various skills with Microsoft Technologies are required to successfully execute this process. Microsoft tools involved include:

- Remote Desktop Client or Hyper-V Console
- Skype for Business Topology Builder
- Various DNS tools
- Certificate Requests
- CloudBond 365 SysAdmin

6.2.1 Process Overview

What needs to change when changing the SIP domain?

Firstly, SIP domains are defined in the Skype for Business Topology. We will need to use the Skype for Business Topology Builder tool on the X-UM Standard Controller server to either, change the primary SIP domain, add or remove additional SIP domains, or both.

Also defined in the Skype for Business Topology are the Simple URL's. Skype for Business uses these to locate resources for dialing conferencing, meetings, etc. These changes can be quite complex if you are changing the primary SIP domain.

The Topology also contains DNS names for the External Web Services (on the FE server), and DNS names for various services on the Edge server, which may need to be adjusted.

Once the Topology has been reconfigured, we need to publish the changes to all Skype for Business servers, so that the changes can be updated into the CMS databases. On X-UM Standard, this will include the UC-FE and UC-Edge servers.

After publishing a topology change, the Skype for Business Deployment Wizard must be re-run on all Skype for Business servers (UC-FE and UC-Edge). For a SIP domain change, this will update the IIS configuration to recognize requests for the new SIP Domain simple URL's. Changes to the SIP domains and Simple URL's have flow on requirements for DNS entries. We will need to update DNS entries for both internal and external DNS servers to match the new SIP domains. This includes many records, such as those used for Simple URL's, those used for Auto Configuration of Skype for Business Clients, and those used for Federation.

Changes to DNS entries require changes to SSL Certificates in order for the secured HTTPS and TLS protocol to work correctly. Updated Certificates need to be installed on both the X-UM Standard -FE and X-UM Standard -Edge servers. This may involve a public certificate from your provider.

You will also need to examine Reverse Proxy servers and Firewalls, to ensure any DNS or URL references are updated accordingly.

Lastly, you need to examine any existing Skype for Business objects, such as users, RGS objects etc. and modify them to match the new domains if required.

6.2.2 Connecting to X-UM Standard Controller using RDP

Connect to the X-UM Standard controller. As an alternative, Hyper-V Manager on the X-UM Standard Controller can be used to connect to the console of both the X-UM Standard Front-End and Edge servers (UC-FE and UC-Edge).

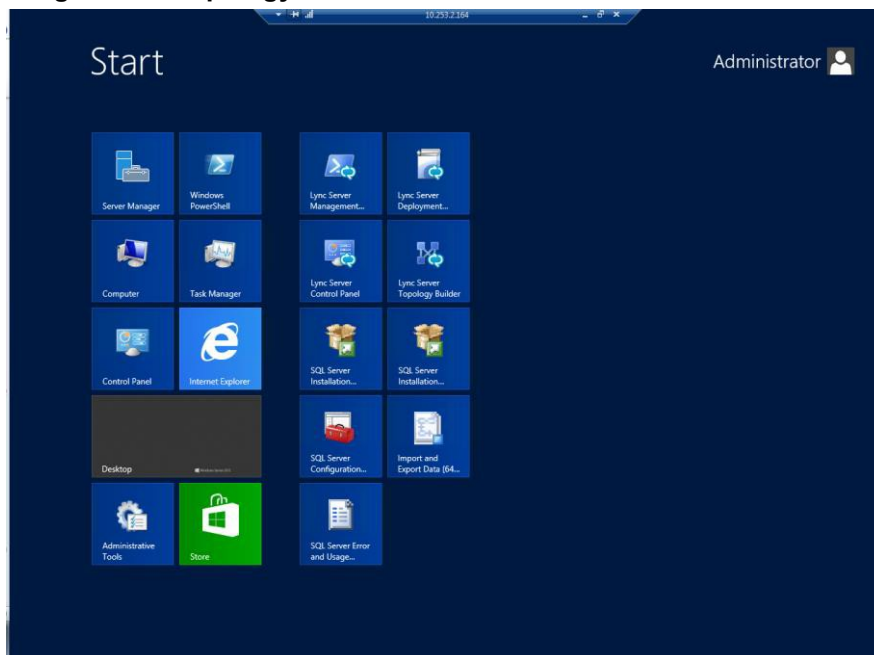
6.2.3 Using the Topology Builder

This section describes how to use the Topology Builder.

➤ **To use the Topology Builder:**

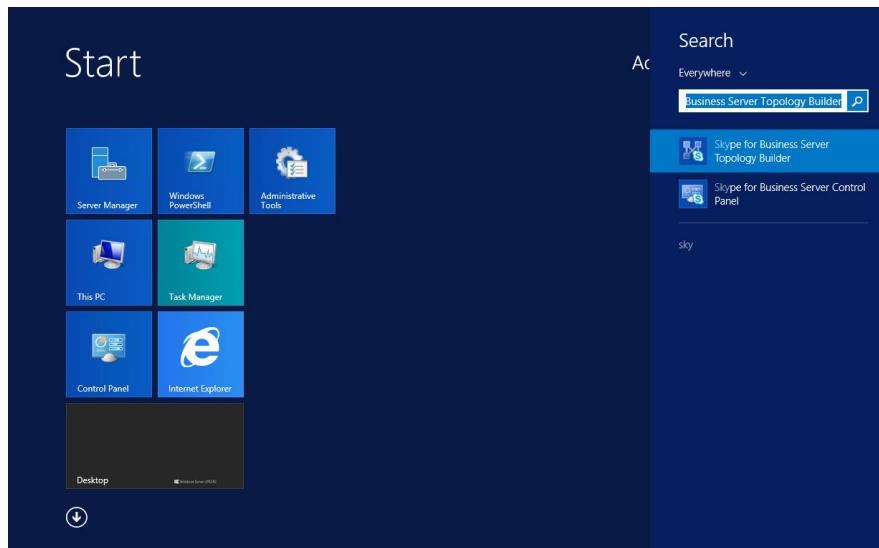
3. Open the Topology builder.

Figure 6-1: Topology Builder - From the X-UM Standard Controller



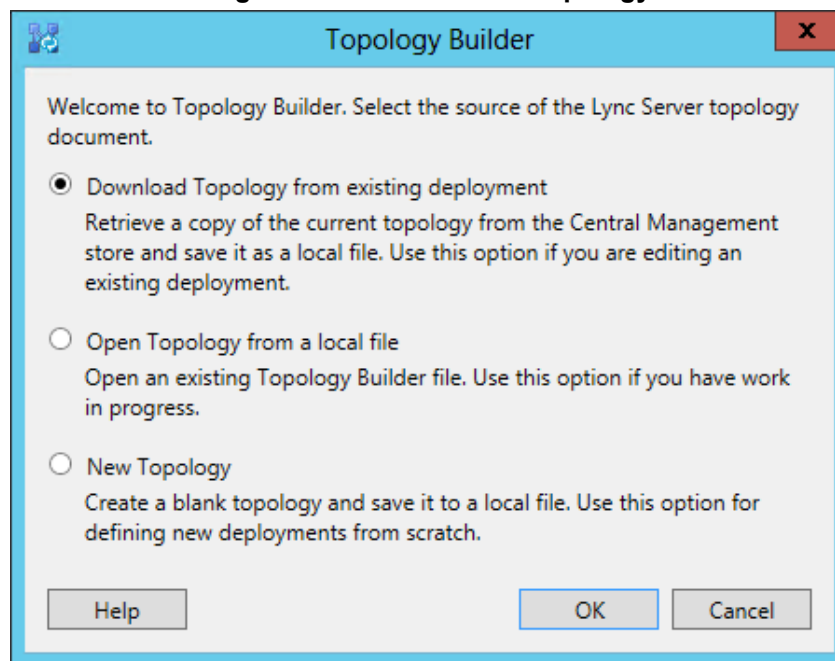
4. Use **Search** to open Skype for Business Utilities.

Figure 6-2: Using Search to Open Skype for Business Utilities



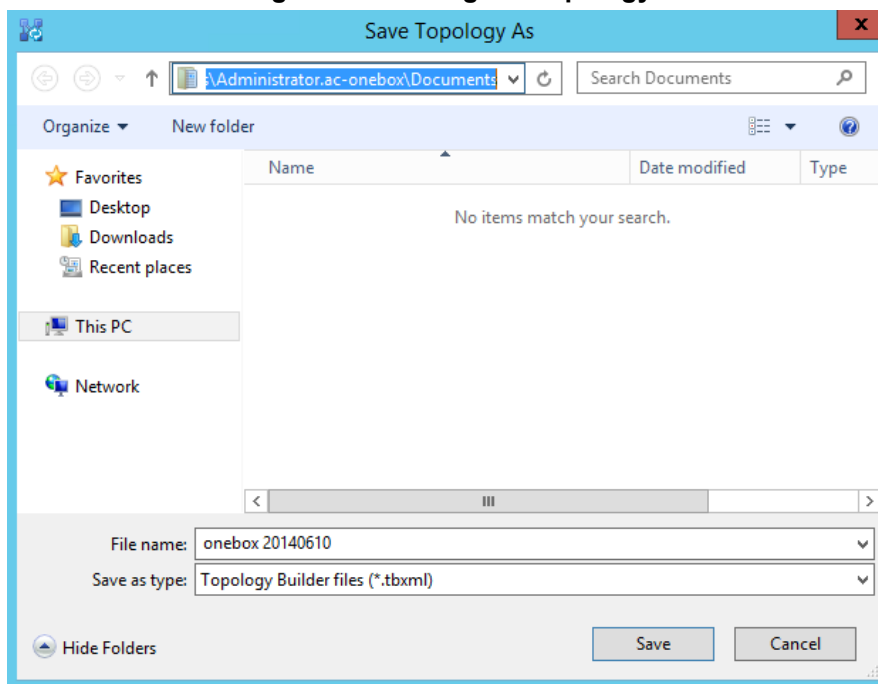
5. Download and save the current topology.

Figure 6-3: Source of the Topology



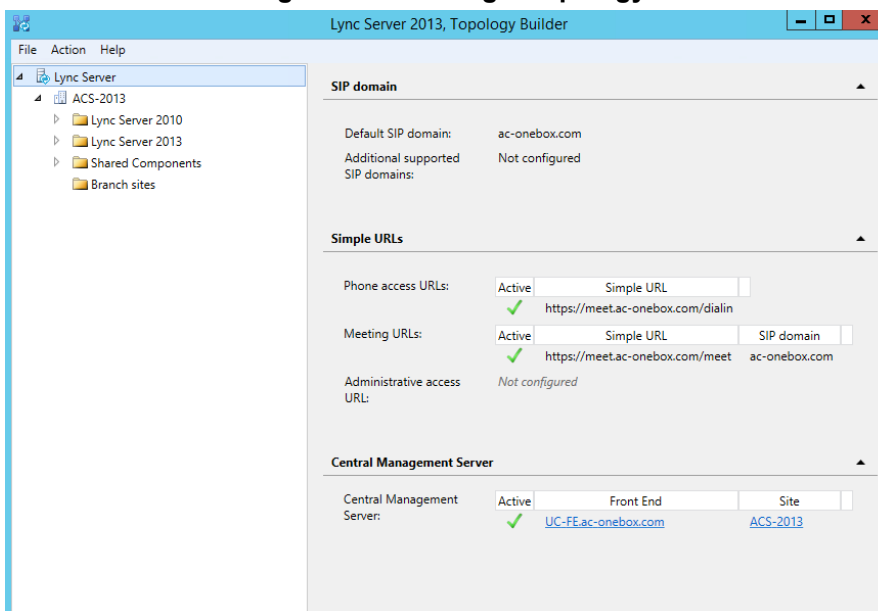
6. Save the topology.

Figure 6-4: Saving the Topology



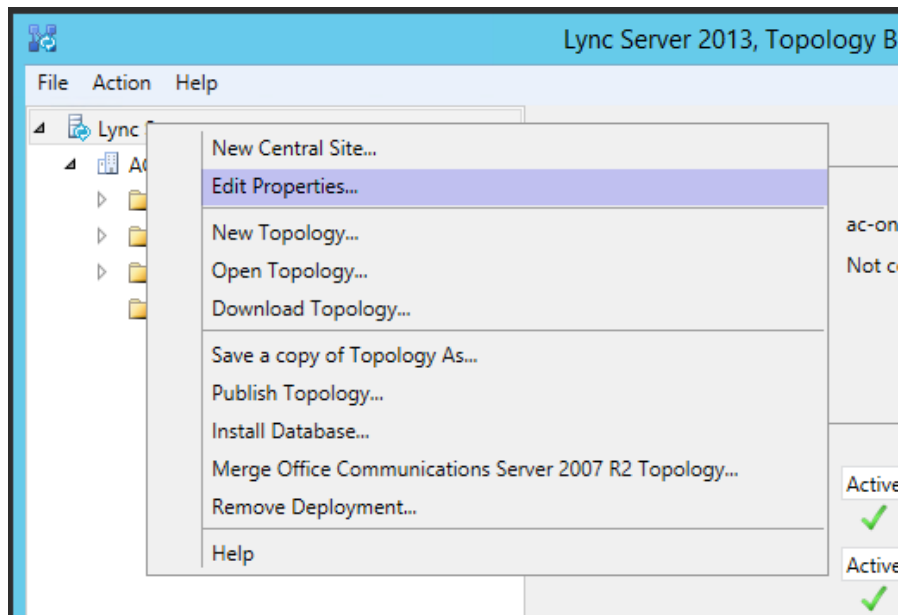
7. View the topology; SIP Domains and Simple URL's are properties of the whole server (**Skype for Business Server 2015\Lync Server 2013**).

Figure 6-5: Viewing a Topology



8. Right-click the server (**Skype for Business Server 2015/Lync Server 2013**), and select **Edit Properties**.

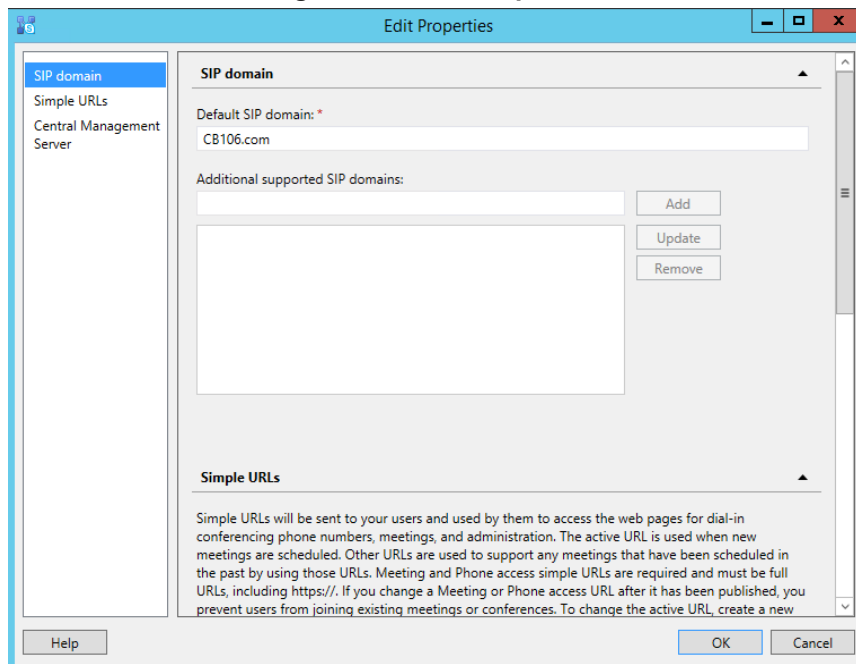
Figure 6-6: Edit Server Properties



6.2.3.1 Adding the New SIP Domain to the Topology

- To add a new SIP domain to the topology:
 - Enter a new SIP domain name in the **Additional supported SIP domains** field, and then click **Add**.

Figure 6-7: Edit Properties

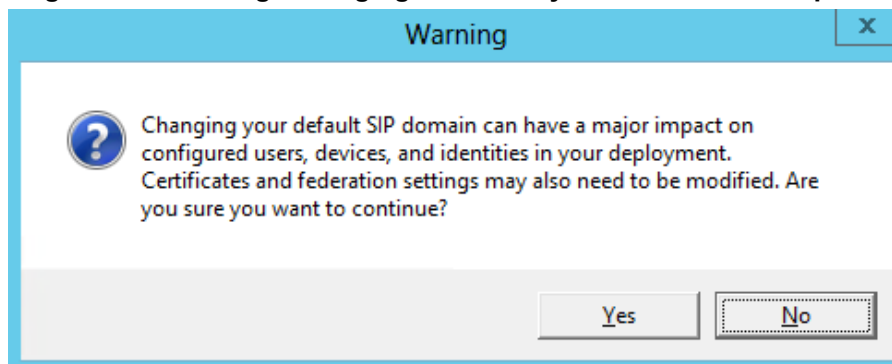


6.2.3.2 Changing the Default (Primary) SIP Domain

If you change the primary SIP domain, the following pop-up is displayed, to remind you of some of the implications of making the change. In general, it is usually easier to add an Additional SIP domain, rather than change the default SIP domain.

After changing the primary SIP domain, you **MUST** review both the Simple URL's and Edge Server properties to make appropriate changes.

Figure 6-8: Warning: Changing the Primary SIP Domain is Complex



Note: Simple URL's, Edge services, and their matching certificates are covered in Section 10 on page 147.



Note: It is also possible to change an existing **Additional SIP domain** to the "Default SIP domain", using the Skype for Business Management shell and the *set-csSipDomain* command.

e.g., `Set-CsSipDomain -Identity constoso.com -IsDefault $True`

6.2.3.3 Managing Simple URLs

The process below describes how to manage simple URLs.

➤ **To manage simple URLs:**

1. To change a URL, select the URL, and then click **Edit URL**.
2. To remove a URL, select the URL, and then click **Remove**.

Figure 6-9: Simple URL's Using Option 3

3. Add a **Phone access URL** for the new SIP domain (e.g., <https://meet.contoso.com/dialin>).
4. Mark it as **Active**, if appropriate.
5. Remove any phone access URL's no longer required (e.g., <https://meet.ac-onebox.com/dialin>).
6. Modify and/or add **Meeting URL's**.



Note: Further details on naming options for Simple URLs are covered in Chapter 10 on page 147.

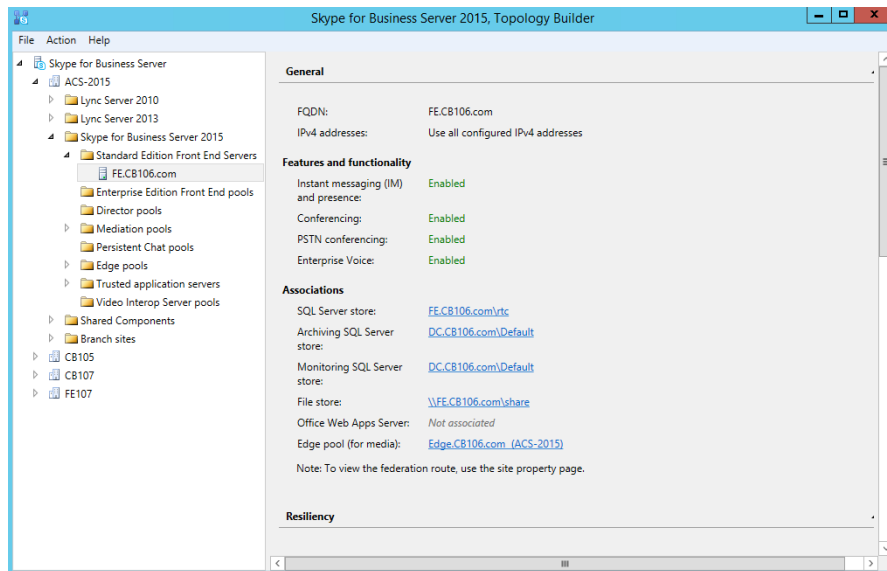
6.2.3.4 Editing External Web Services

The External Web Services FQDN is a property of the Skype for Business Standard Edition Front End server's pool.

➤ **To edit external Web services properties:**

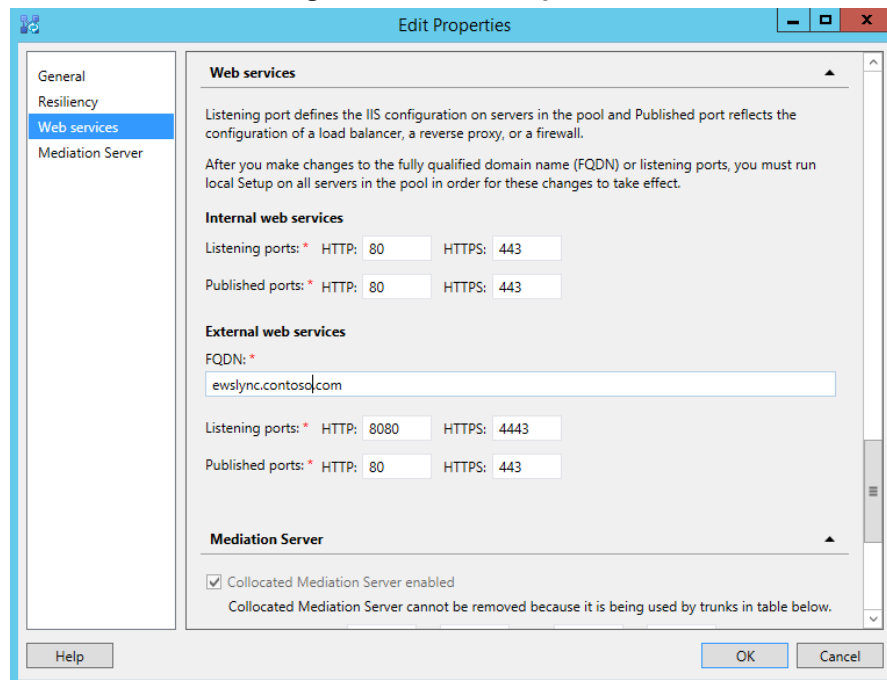
1. In the Topology Builder, navigate to the Skype for Business Standard Edition server, right-click, and then select **Edit Properties**.

Figure 6-10: Selecting the Standard Edition Front End Pool



2. The External Web Services URL must be unique from the Simple URLs.

Figure 6-11: Edit Properties



3. If required, modify the **External web services FQDN** to match the new SIP domain.

6.2.3.5 Editing Edge Services Properties

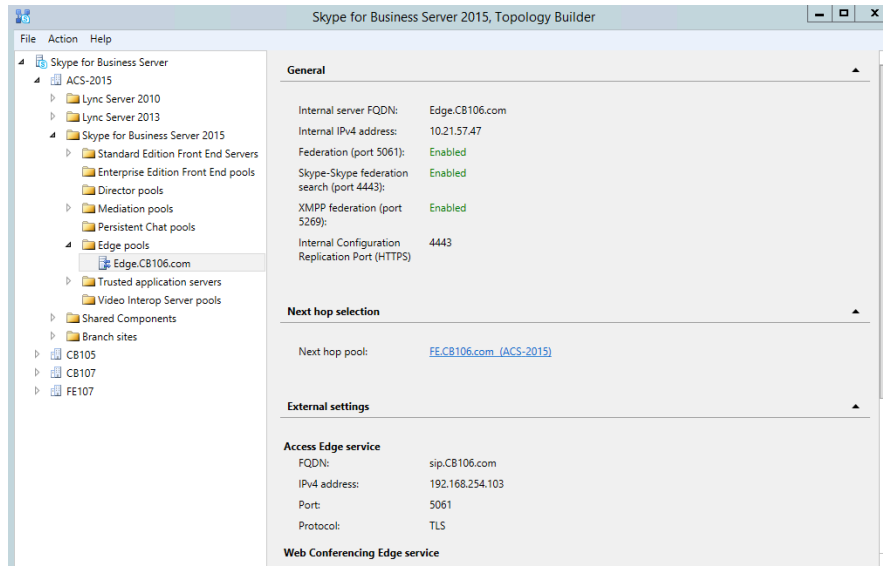
Edge External FQDN's allow users to access your Skype for Business system from outside your organization. This includes Access Edge for external users, Web Conferencing Edge for external conferences, and A/V Edge for voice and video calls.

The Edge Server configuration is a property of the Skype for Business Server Edge pools.

➤ **To edit Edge Services properties:**

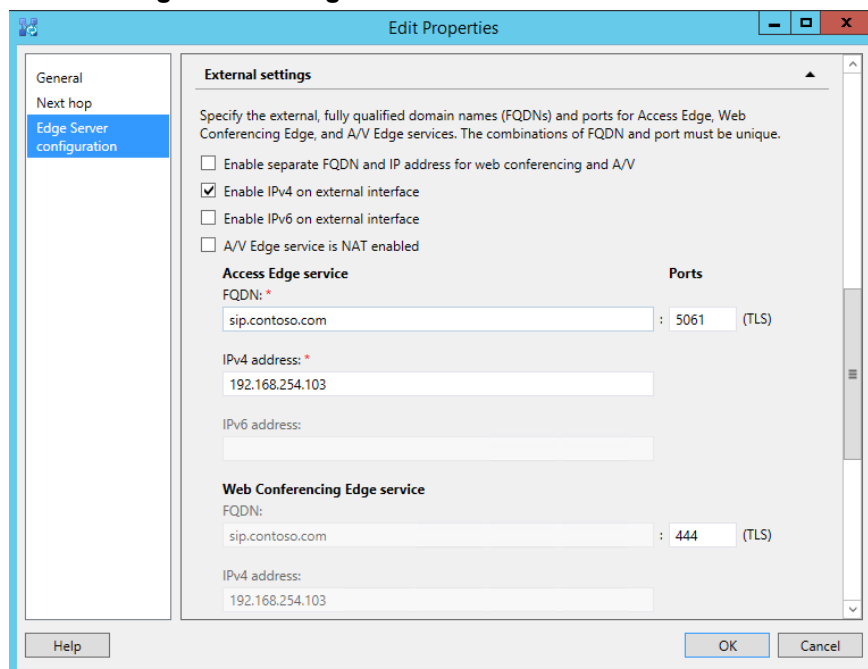
1. In the Topology Builder, navigate to the server (**Skype for Business Server 2015/Lync Server 2013**) > **Edge Pools**. Right-click, and select **Edit Properties**.

Figure 6-12: Selecting the Edge Server from the Edge Pool



2. Scroll down, or select **Edge Server Configuration** from the left pane.

Figure 6-13: Edge Server External Access FQDNs



3. Modify the service FQDNs' as required.

4. Click **OK**.



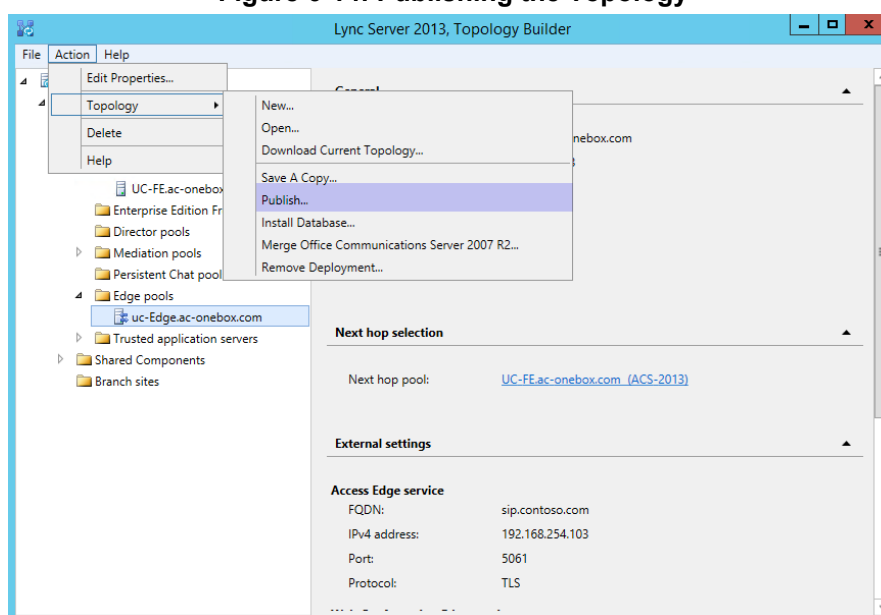
Note: The **Enable separate FQDN and IP Address for web conferencing and A/V** check box controls whether separate FQDN's may be entered for each service. The combination of FQDN and Port must be unique for each service.

6.2.3.6 Publishing Topology

- To publish the topology:

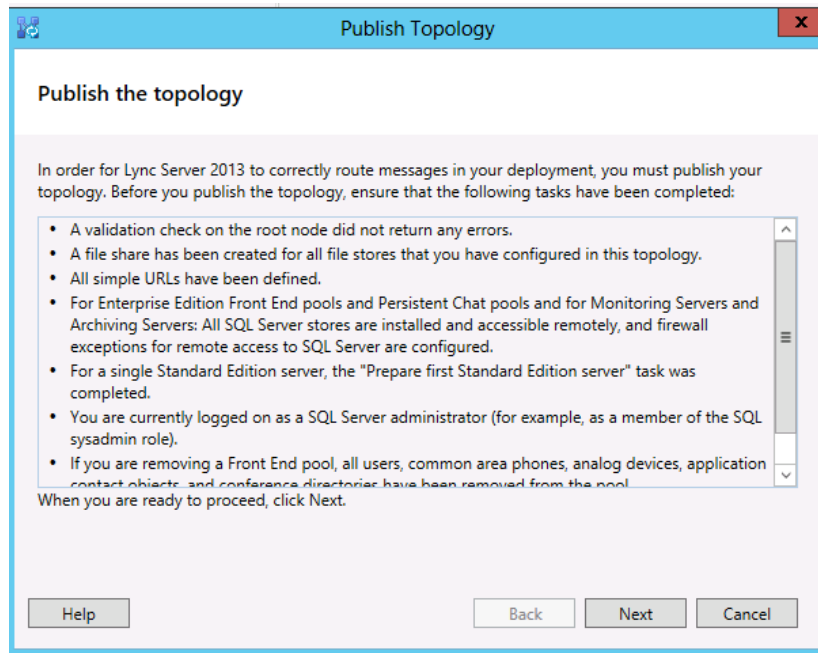
1. In the Topology Builder, make the required additions, e.g., additional SIP domains or voice gateways e, and the select **Publish Topology...** to continue the installation.

Figure 6-14: Publishing the Topology



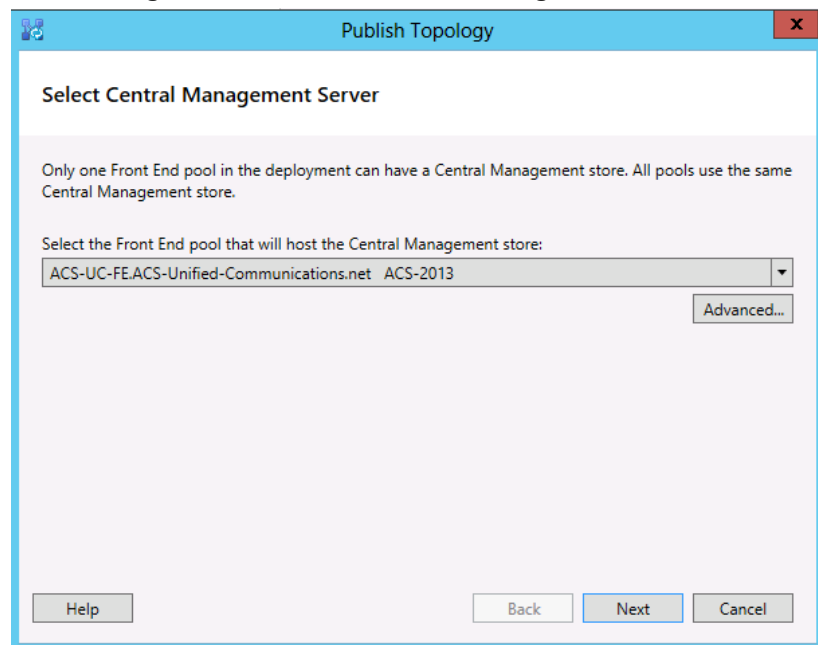
2. Continue the wizard by clicking **Next**.

Figure 1-15: Publishing the Topology

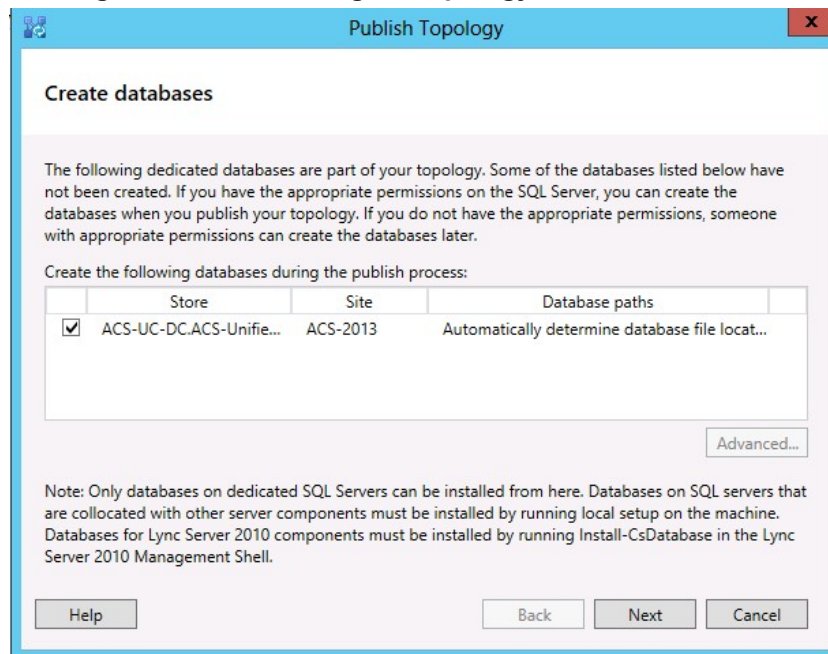


3. Click **Next**.

Figure 6-16: Select Central Management Server

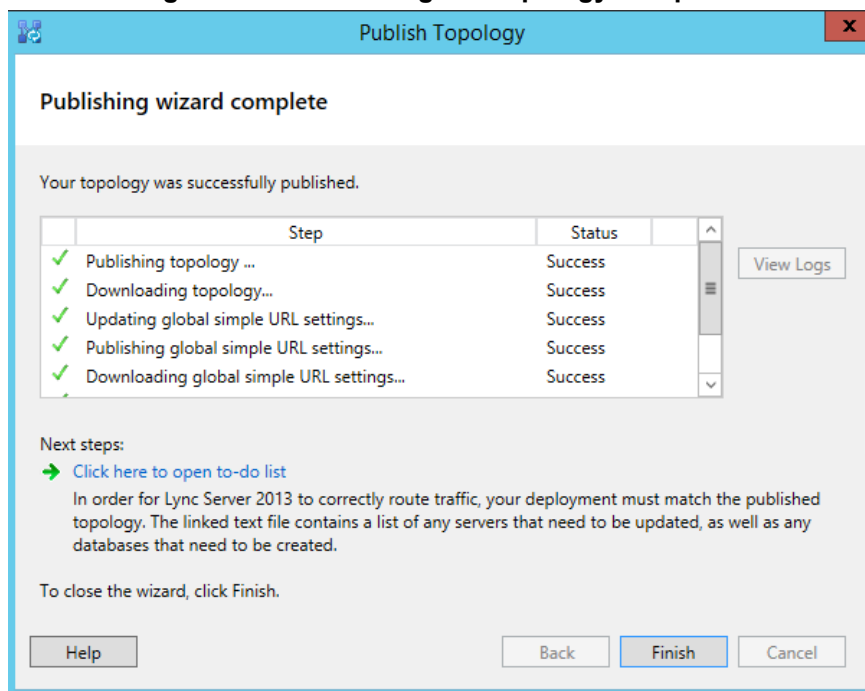


4. Click **Next**.

Figure 6-17: Publishing the topology – Create Databases

Note: These screens will not be displayed if the topology has been previously published.

5. Click **Finish**.

Figure 6-18: Publishing the Topology Completes

6.2.4 Running Deployment Wizard

The Deployment wizard implements any changes from the newly published Topology. The Deployment wizard must be run on both the X-UM Standard Front End and Edge servers.

Figure 6-19: Starting the Deployment Wizard

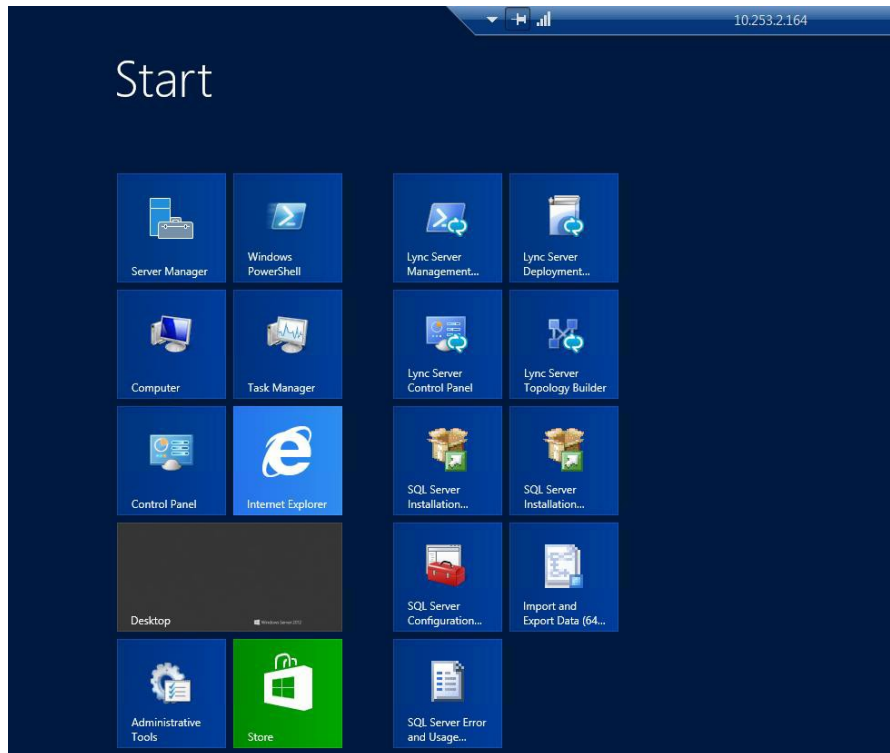
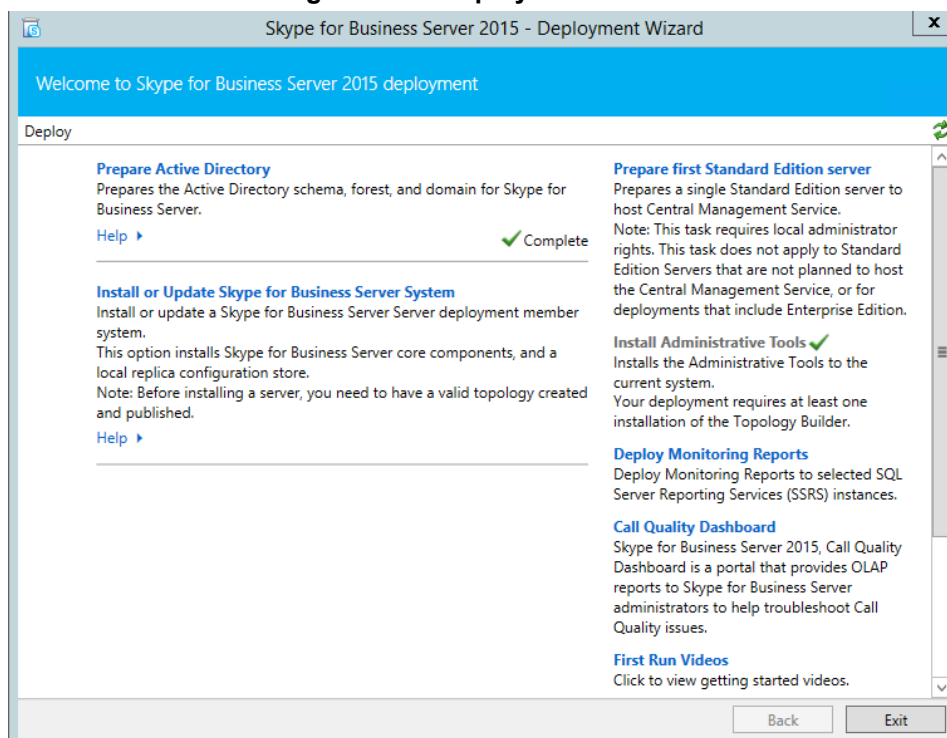


Figure 6-20: Deployment Wizard



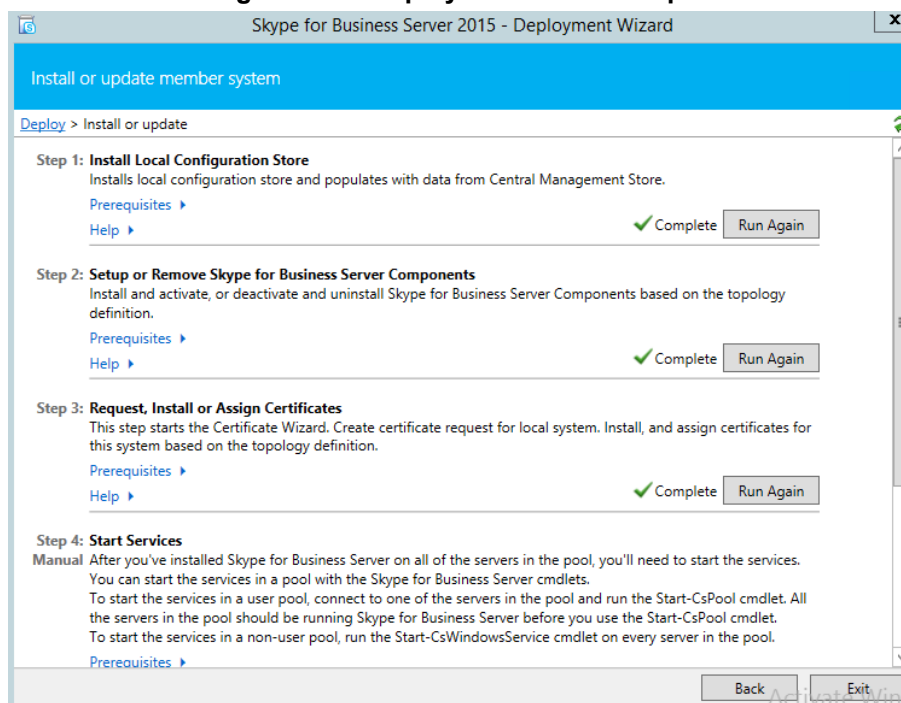
6.2.4.1 Installing or Updating Skype for Business Server System

The procedure below describes how to install or update Skype for Business server system.

➤ **To install or update Skype for Business server system**

1. Select **Setup or Remove Skype for Business Server Components**.

Figure 6-21: Deployment Wizard Steps



2. Click **Run Again**.

Figure 6-22: Setup Server Components

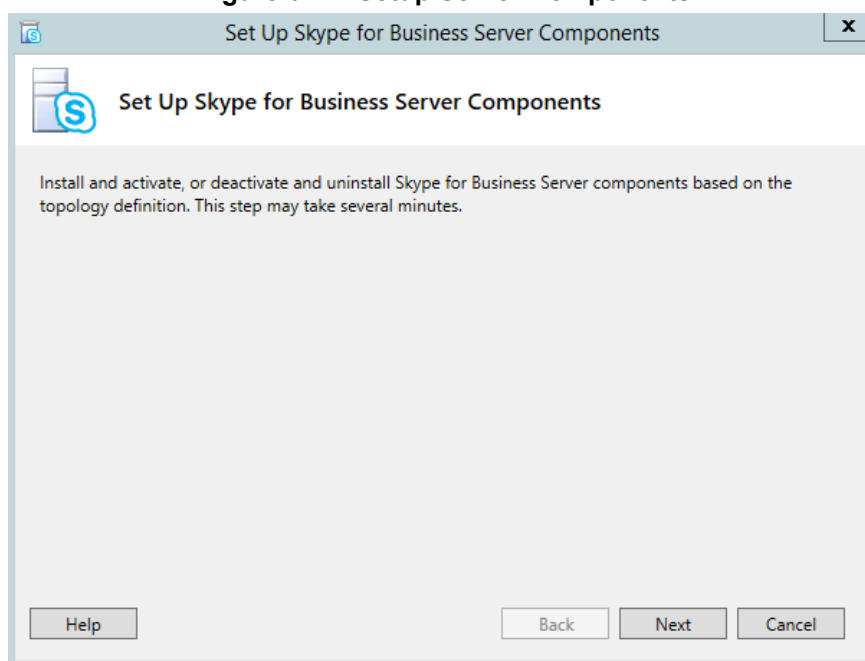
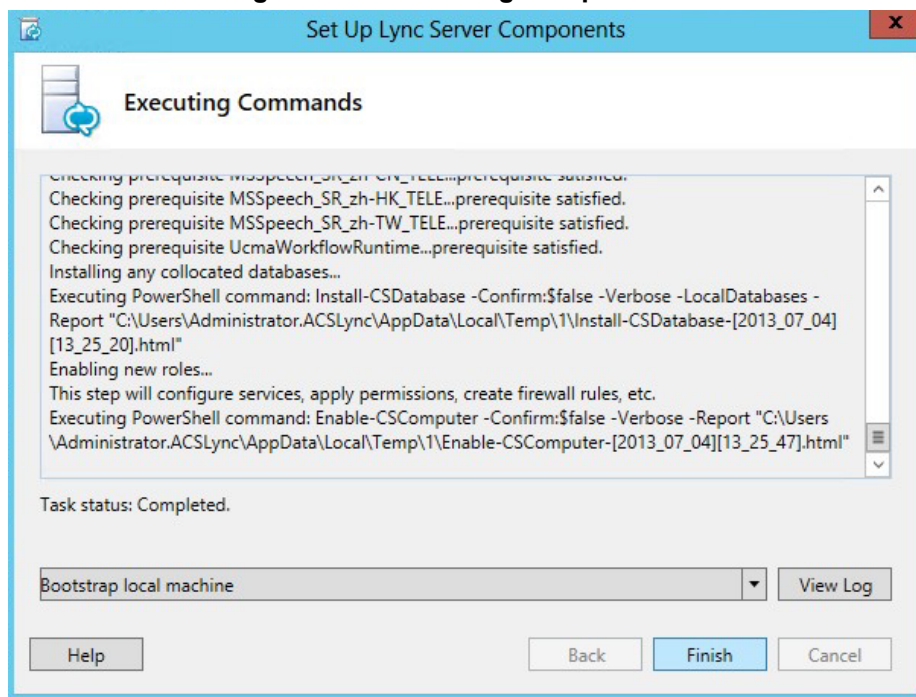


Figure 6-23: Executing Components



3. The Deployment wizard must be run on both the Front End server and the Edge Server.

6.2.5 DNS Entries

DNS entries are described in Section 6.2.5 on page 60.

New DNS entries will be required to match the topology changes you have made.

6.2.5.1 Skype for Business Internal Records

Internal records generally refer to the private IP address space.

- SRV: `_sipinternaltls._tcp.<FQDN>` over port 5061 to sip.<FQDN>
- SRV: `_sipinternal._tcp.<FQDN>` over port 5061 to sip.<FQDN>
- SRV: `_sip._tls.<FQDN>` over port 5061 to sip.<FQDN>
- A: `lyncdiscoverinternal.<FQDN>`
- A: `sip.<FQDN>`
- A: `meet.<FQDN>`

6.2.5.2 Skype for Business External Records

External records refer to public IP addresses.

- SRV: `_sipfederationtls._tcp.<FQDN>` over port 5061 to sip.<FQDN>
- SRV: `_sip._tls.<FQDN>` over port 5061 to sip.<FQDN>
- A: `sip.<FQDN>`
- A: `sipexternal.<FQDN>`
- A: `meet.<FQDN>`
- (in a default X-UM Standard installation, meet is used for both dialing and meet simple URL's)
- A: `ewslsync.<FQDN>`
- (is assigned to the default X-UM Standard Skype for Business external web services)

- CNAME: Skype for Businessdiscover.<FQDN> pointing to ewslync.<FQDN>

6.2.6 Certificates

Certificate requirements are covered in:

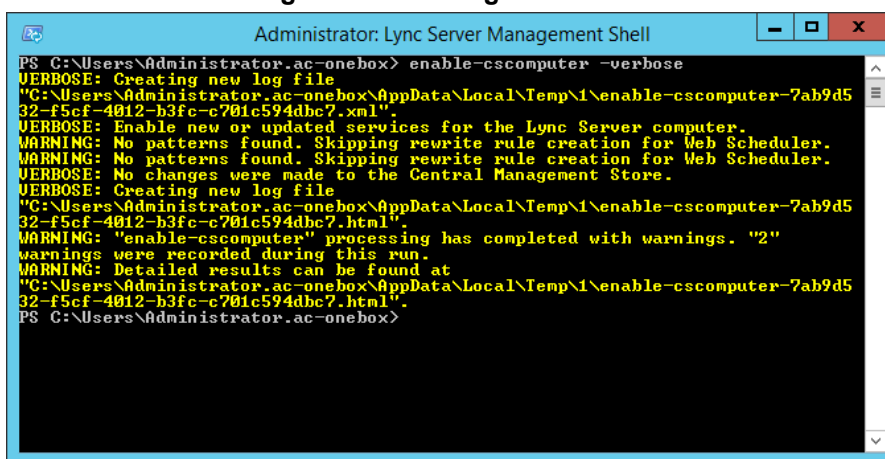
6.2.6.1 AudioCodes X-UM Standard Certificates Configuration Note

New certificates will need to be deployed to match the Topology changes you have made.

6.2.7 Enabling Configuration

After completing all the above steps, it is best to ensure the changed configuration is now active. To do so, run the “**Enable-CSComputer -Verbose**” command on both the UC-FE and UC-Edge servers.

Figure 6-24: Management Shell



```
PS C:\Users\Administrator.ac-onebox> enable-cscomputer -verbose
VERBOSE: Creating new log file
"C:\Users\Administrator.ac-onebox\AppData\Local\Temp\1\enable-cscomputer-7ab9d532-f5cf-4012-b3fc-c701c594dbc7.xml".
VERBOSE: Enable new or updated services for the Lync Server computer.
WARNING: No patterns found. Skipping rewrite rule creation for Web Scheduler.
WARNING: No patterns found. Skipping rewrite rule creation for Web Scheduler.
VERBOSE: No changes were made to the Central Management Store.
VERBOSE: Creating new log file
"C:\Users\Administrator.ac-onebox\AppData\Local\Temp\1\enable-cscomputer-7ab9d532-f5cf-4012-b3fc-c701c594dbc7.html".
WARNING: "enable-cscomputer" processing has completed with warnings. "2"
warnings were recorded during this run.
WARNING: Detailed results can be found at
"C:\Users\Administrator.ac-onebox\AppData\Local\Temp\1\enable-cscomputer-7ab9d532-f5cf-4012-b3fc-c701c594dbc7.html".
PS C:\Users\Administrator.ac-onebox>
```

This page is intentionally left blank.

7 Connecting Edge Server to a Full DMZ Deployment

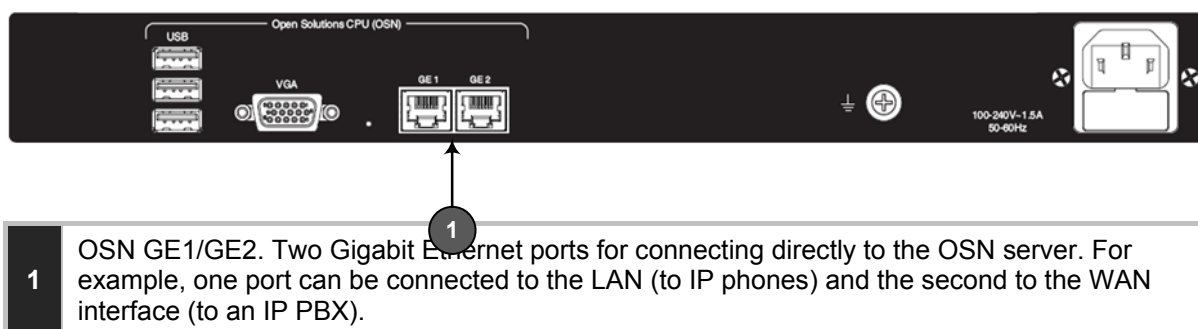
This chapter shows how to connect the X-UM Standard Edge Server to a full DMZ deployment.

7.1 Connecting the Edge Server

This chapter shows how to connect the X-UM Standard Edge Server to a full DMZ deployment.

The X-UM Standard Edge Server by default connects to the external world via a separated Ethernet connection, located on the rear panel of the X-UM Standard, shown in the figure below.

Figure 7-1: Two Gigabit Ethernet Ports on the X-UM Standard Rear Panel



The internal Edge Server 'leg' is connected internally to the Skype for Business Server pool. Deployment scenarios exist, however, in which customers want to take the Edge Server internal connection via a firewall as well, and utilize the second rear panel Ethernet port, shown in the figure below.

Figure 7-2: Utilizing the Second Ethernet Port on the X-UM Standard Rear Panel

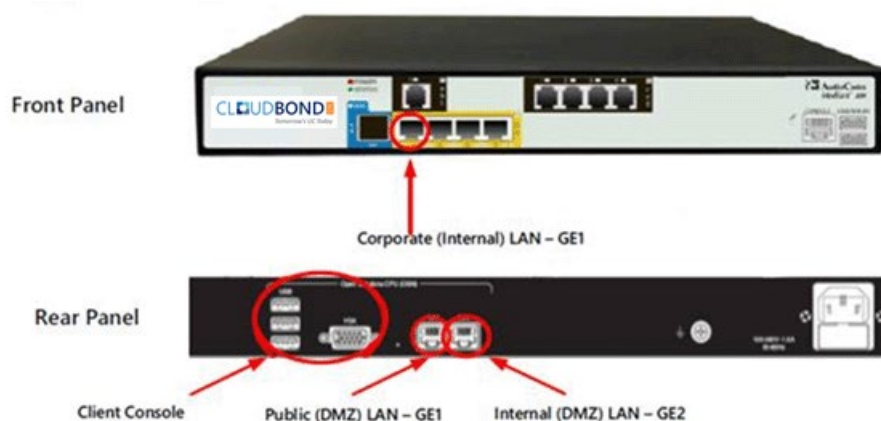
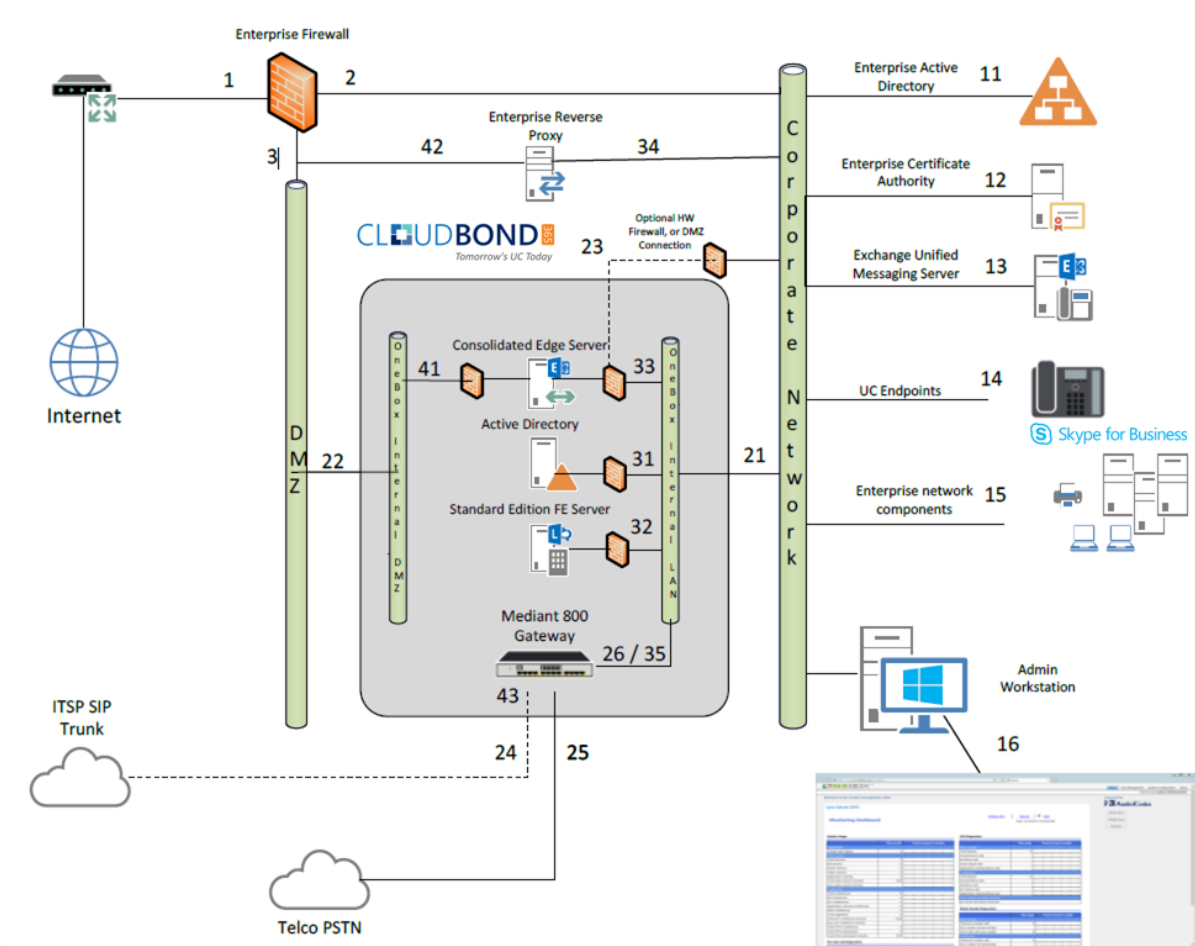


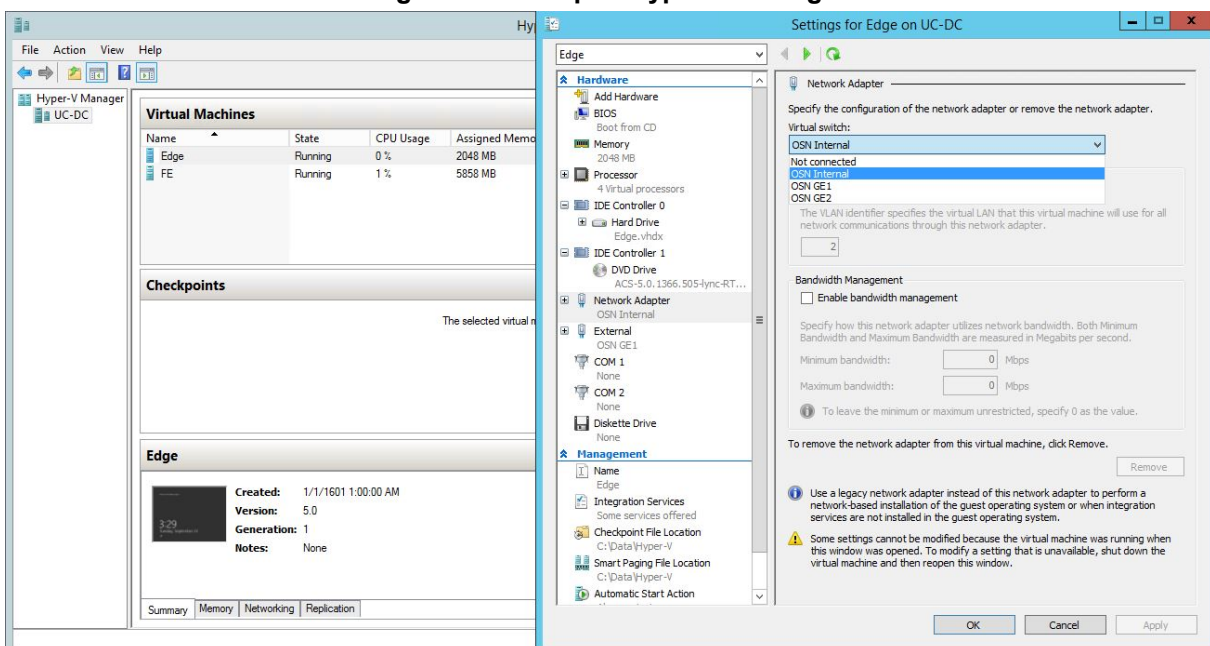
Figure 7-3: Edge Server - Two Legs



➤ **To set up the X-UM Standard for a deployment like this:**

1. Connect to X-UM Standard through a locally connected keyboard, mouse and monitor, or through a remote desktop connection to the X-UM Standard controller.
The default remote connection information is:
 - IP address: 192.168.0.101
 - Username: CloudBond365\administrator
 - Password: R3m0t3Supp0rt
2. Start the Hyper-V Manager application, located on the base Operating System.
3. Open the Edge Server settings through the Action menu, and then select the Network Adapter named **OSN Internal**.
4. Change the virtual switch from **OSN Internal** to **OSN GE2**, and then adapt the VLAN ID accordingly, if necessary.

Figure 7-4: Setup in Hyper-V Manager



5. Click **OK** and apply the changes.



Note: It's unnecessary to restart the Edge Server since this procedure is basically the same as patching a network cable.

This page is intentionally left blank.

8 Describing Deployment Requirements

This section describes the deployment of X-UM Standard within an existing corporate domain network. This guide provides information to technicians on how to perform on-site installation of CloudBond X-UM. The guide provides:

- Guidelines for preparing the customer enterprise network
- CloudBond X-UM Configuration procedure
- Basic system and site configuration information
- Concepts and procedures for Microsoft Exchange UM Integration
- Maintenance procedures for the server and the client applications

8.1 Before Deploying CloudBond X-UM

Before deploying CloudBond X-UM make sure:

- You have all deployment-related information
- Enterprise customer staff can be available if necessary, to perform specific tasks within the existing corporate enterprise network
- You have completed the *CloudBond 365 Intake Form* which contains information related to CloudBond 365 such as server names, IP addresses, and certificate information
- You are familiar with the following Domain Controller information:
 - DHCP
 - DNS
 - Microsoft Exchange details

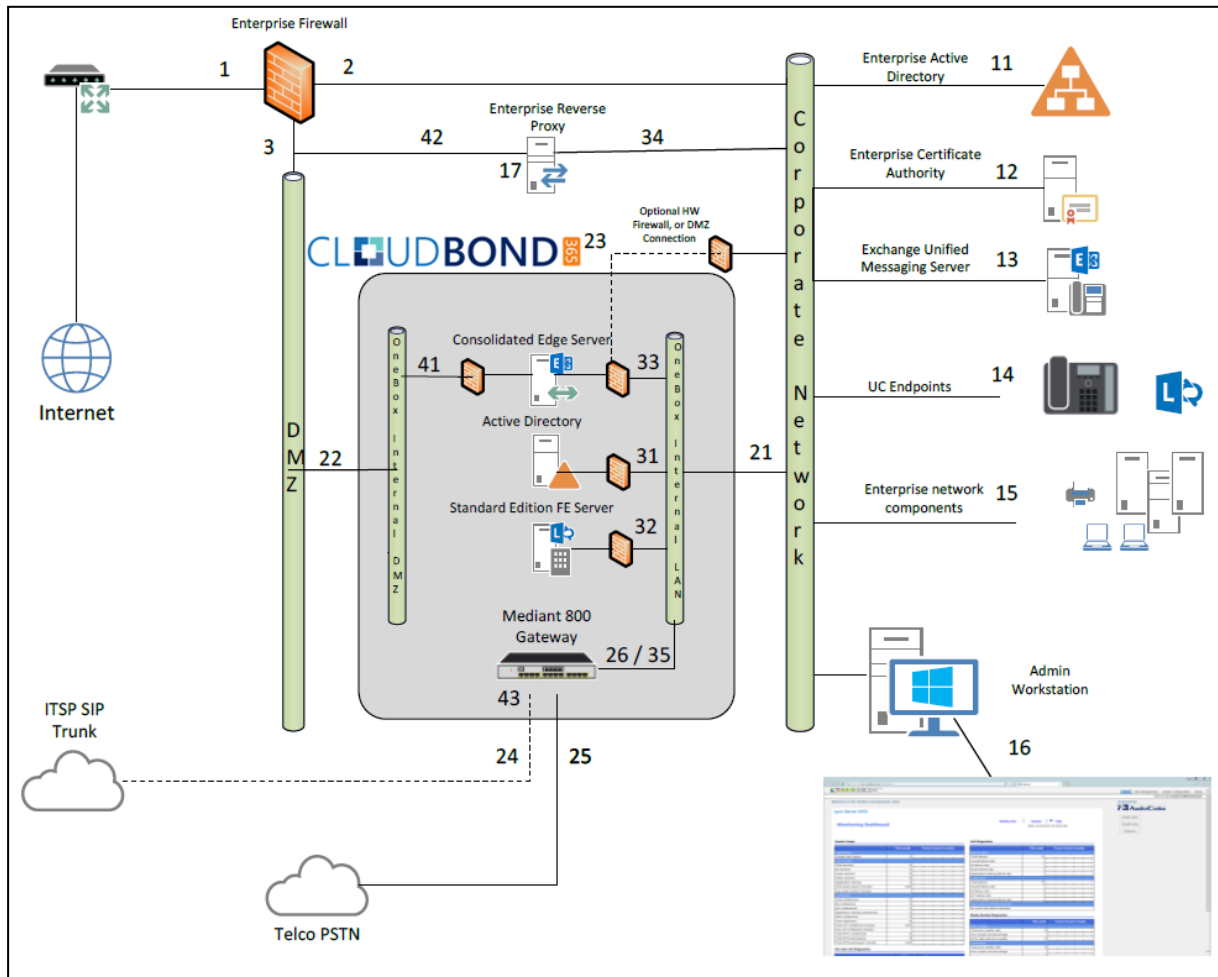
8.1.1 Public Key Infrastructure

Microsoft Skype for Business uses a Public Key Infrastructure (certificates) to enable secure MTLS and TLS communication between servers and clients. To communicate with Microsoft® Office 365 Exchange UM, you will need to deploy public certificates.

8.1.2 IP Addresses

CloudBond X-UM is connected to the enterprise network using at least five internal IP addresses. On the Internet side, one (optionally a NAT address) public IP address is required, AudioCodes SBC, may require additional external IP addresses. shows the location of CloudBond X-UM in the network. For more information on the required ports and firewall configuration, see Section 8.4 on page 89.

Figure 8-1: X-UM Located in the Network



All IP addresses will be set to default on a new CloudBond X-UM system. You may need to change IP addresses if the defaults are unsuitable.

The corporate Domain Controller should be able to ping all four CloudBond X-UM servers (Controller, Front End, Edge, X-UM Connector) by IP address. This is a reasonable test to perform for correct network connectivity. To change IP addresses, see Section 5.3 on page 33.

8.1.3 DNS

DNS records play a very important part in the correct functioning of Microsoft Skype for Business and the CloudBond X-UM. DNS Records are required to do the following:

- Establish a two way trust between the enterprise domain and the CloudBond 365 resource forest
- Allow Skype for Business clients to locate Skype for Business services and to automatically log on
- Allow Skype for Business services to be accessed externally.

You may need to create several DNS zones within the enterprise DNS server, and the public DNS provider, or add individual DNS records to both.

Typically, the following is required:

- On the enterprise DNS server, a stub zone matching the CloudBond 365 resource domain Fully Qualified Domain Name (FQDN) (cloudbond365.local). This stub zone is used to establish the forest level trust between the enterprise domain and the CloudBond 365 domain.
- On the CloudBond 365 Controller server, a stub zone matching the corporate enterprise DNS zone. This stub zone is used to establish the forest level trust between the enterprise domain and the CloudBond 365 domain.
- On the CloudBond 365 Controller server, a primary or stub zone matching the FQDN of the every SIP domain specified for the CloudBond 365 topology. These DNS zones contain the internal DNS records which permit automatic logon of the Skype for Business UCMA applications to the Skype for Business Front End server.
- On the public DNS server, a zone matching the FQDN of the SIP domain specified for CloudBond 365. If any additional SIP domains are supported, they may need additional DNS zones. These DNS zones contain the external DNS records which permit automatic logon of Skype for Business clients for external access, federation records, etc. These records typically resolve to the CloudBond 365 Edge.



Note: To be able to make changes to the enterprise DNS servers or to set up a bidirectional forest trust, you must be a member of the Domain Admins group (in the forest root domain) or the enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority. This means that if you don't have these permissions in the enterprise environment, a customer enterprise administrator should be available to assist.

See Section 8.1.3 on page 68 for more details on Skype for Business DNS records.



Note: You must change or add a valid SIP domain for external access as the default SIP domain (yourdomain.com) and associated Simple URLs, DNS references, etc., are unsuitable for the public internet. Public DNS records must match the amended SIP domain.

8.1.4 Forest and Domain Levels

Though CloudBond 365 runs in its own Active Directory forest, minimum requirements exist for the customer Active Directory environment.

This section details the requirements and some background information on how to reach this minimum level.



Note: Microsoft Windows Small Business Server Edition does not support forest trusts, so the Skype for Business client will have its own login information since SBS users cannot be synchronized with the Skype for Business appliance. The remainder of this document assumes that an SBS network is *not* installed.

Domain and forest functional levels provides the means by which you can enable additional domain-wide and forest-wide Active Directory features, remove outdated backward compatibility within your environment, and improve Active Directory performance and security.

Microsoft Skype for Business requires both the domain and forest functional levels to be Windows Server 2003 or above. When the Windows Server 2003 functional level is enabled in your environment, additional Active Directory domain-wide and forest-wide features are automatically enabled.

Windows Server 2003 functional level can only be enabled in your environment when all domain controllers are running Windows Server 2003 or higher.

8.2 Integrating CloudBond X-UM

This procedures below describe the integration of CloudBond X-UM in the Enterprise.

8.2.1 Connecting CloudBond X-UM to the Enterprise Domain

➤ **To allow CloudBond X-UM to integrate with the enterprise's Active Directory:**

1. Verify the time and time zone settings for each CloudBond X-UM server.
2. Verify the DNS settings on the NIC adapters.
3. Verify the enterprise domain and forest levels.
4. Set up cross-forest DNS stub zones.
5. Set up a bidirectional forest trust.
6. Import the enterprise forest root certificate chain into CloudBond 365 as a trusted issuer.
7. Re-issue the certificate requests from both the appliance frontend and internal edge server (if required).
8. Create necessary DNS entries.

The following sections cover these steps.

8.2.2 Verifying the Time and Time Zone Settings for CloudBond X-UM Servers

For Skype for Business to function correctly, establishing an accurate time is essential. Typically this does not become apparent until the first client or remote computer attempts to connect to Skype for Business, or until the first import of users from the enterprise domain. To prevent unnecessary confusion later on, make sure all CloudBond X-UM servers and hardware components are set to the same time zone, and same time.

CloudBond X-UM typically defaults to **GMT +1:00 hour**. All servers (Controller, Front End, Edge, X-UM Connector and Mediant 800 will need to be synchronized accordingly.

8.2.3 Verifying DNS Settings on NIC Adapters

When setting the IP address, Network Mask, Gateway, and DNS server settings on a NIC adapter, the Primary DNS entry will often default to 127.0.0.1 (Localhost or Loopback address) on DNS servers and Domain Controllers. This is typically set by Microsoft software.

Though this typically does not present problems, it's a known issue when establishing Forest Trusts and other DNS-based Active Directory activities.

To avoid any issues, make sure the Primary DNS setting on NICs on both the Corporate Domain Controller and CloudBond 365 Controller are set to the IP address of the box rather than to 127.0.0.1. Failure to change these DNS entries will result in a Forest Trust that appears to be configured correctly; however does not function.

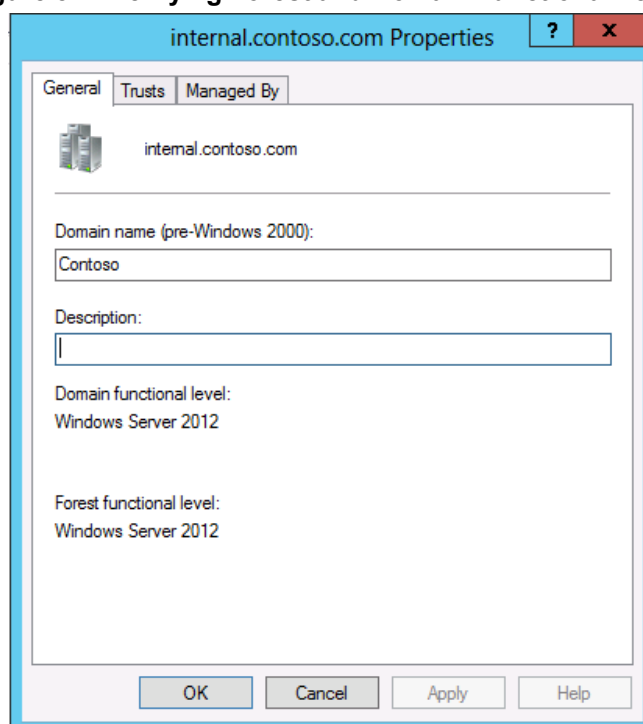
8.2.4 Verifying the Enterprise Domain and Forest Levels

The Active Directory Domains and Trusts console is used to view the existing domain and forest functional levels as well as for raising the levels.

➤ **To verify the Enterprise Domain and Forest Levels:**

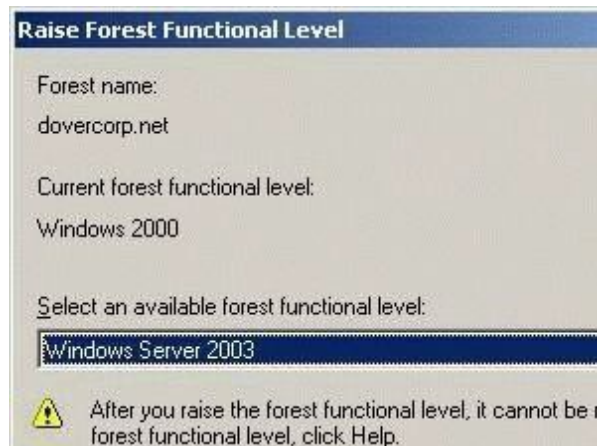
1. On the Enterprise Domain Controller, open the Active Directory Domains and Trusts console.
2. Right-click the domain and select **Properties**; both the domain and forest functional level are displayed.
3. Make sure both domain and forest functional levels are 2003 or higher.

Figure 8-2: Verifying Forest and Domain Functional Levels



Note: Before raising the domain or forest functional level, consult with the domain administrator.

Figure 8-3: Raising Forest Functional Level



- **To raise the domain functional level for a domain:**
 1. Open the Active Directory Domains And Trusts console.
 2. Right-click the domain whose functional level you wish to raise, and select **Raise Domain Functional Level** from the shortcut menu; the Raise Domain Functional Level dialog opens.
 3. From the 'Select an Available Domain Functional Level' list, choose the domain functional level for the domain.
 4. Click **Raise** and then click **OK**.
- **To raise the forest functional level for a forest:**
 1. Open the **Active Directory Domains and Trusts** console.
 2. Right-click **Active Directory Domains and Trusts** in the console tree, and select **Raise Forest Functional Level** from the shortcut menu; the Raise Domain Functional Level dialog opens.
 3. Click **Raise** and then click **OK**.

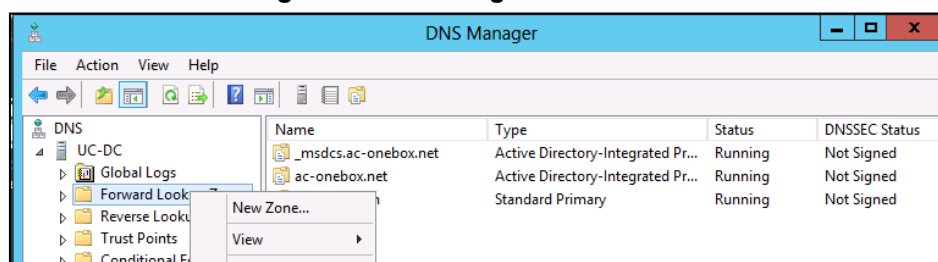
8.2.5 Setting up Cross Forest DNS Stub Zones

The CloudBond 365 Active Directory connector relies on a bidirectional forest trust between CloudBond 365's Active Directory and enterprise Active Directory.

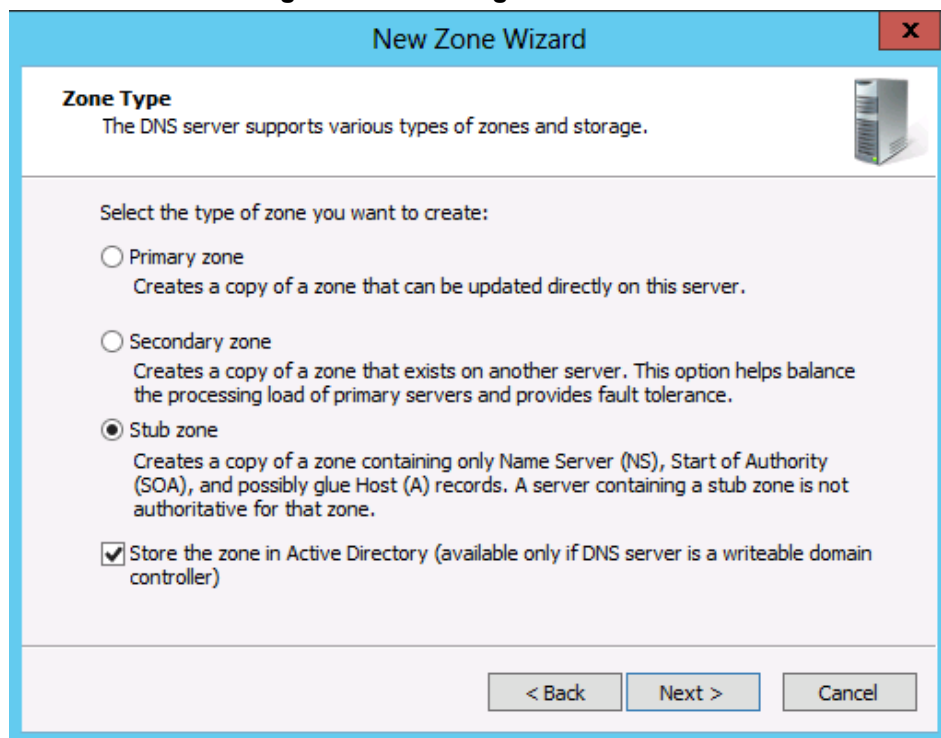
Before a forest trust can be created, both forest domain controllers should be able to find each other. For this cross domain lookup, Stub forward lookup zones need to be created on both the CloudBond 365 DNS and enterprise DNS servers.

- **To create a Stub forward lookup zone on the CloudBond 365 Controller:**
 1. Open the DNS management console and right-click **Forward Lookup Zones** to start the New Zone Wizard.

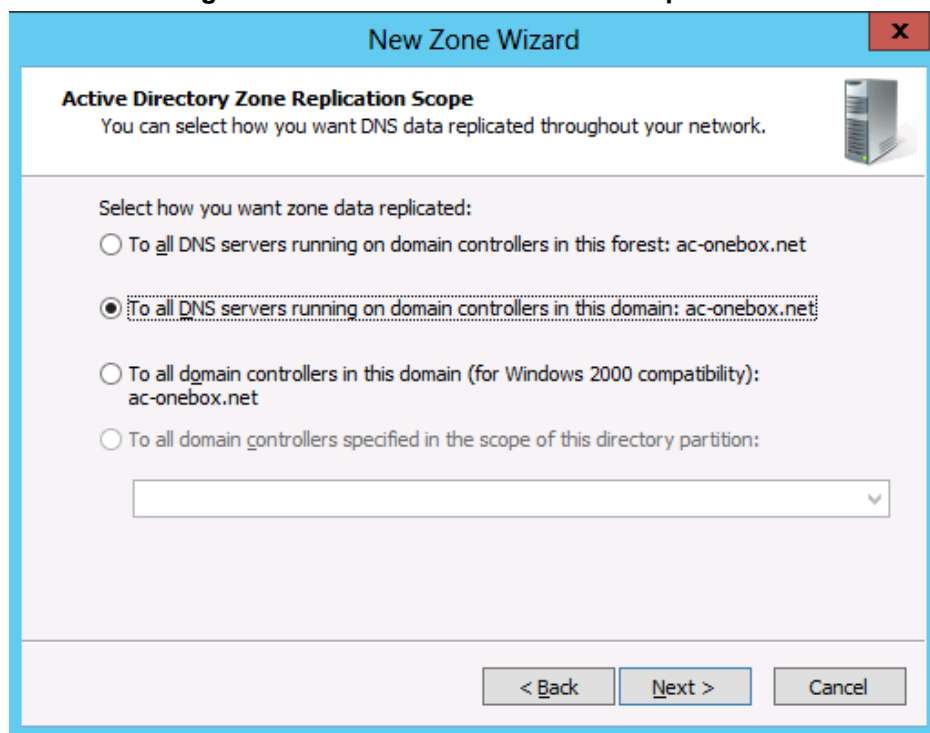
Figure 8-4: Creating DNS Stub Zone



2. Click **Next** to start the wizard and select **Stub zone**. Store the zone in Active Directory by enabling the checkmark.

Figure 8-5: Creating DNS Stub Zone

3. Set replication to all servers within the domain.

Figure 8-6: DNS New Zone Wizard – Replication

4. Specify the Fully Qualified Domain Name (FQDN) for the enterprise domain that is going to be trusted.

Figure 8-7: DNS Stub Zone – FQDN

Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:
internal.contoso.com

< Back Next > Cancel

5. Specify the IP addresses or FQDNs for the enterprise DNS server(s).

Figure 8-8: DNS Stub Zone - Master DNS Server

Master DNS Servers
The stub zone is loaded from one or more master servers.

Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.

Master Servers:

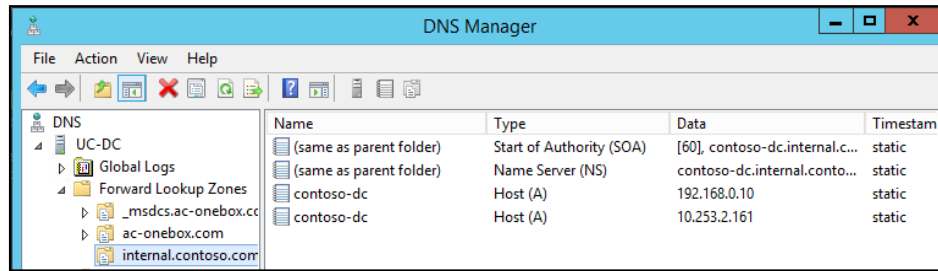
IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
192.168.0.10	Contoso-DC	OK

☐ Use the above servers to create a local list of master servers

< Back Next > Cancel

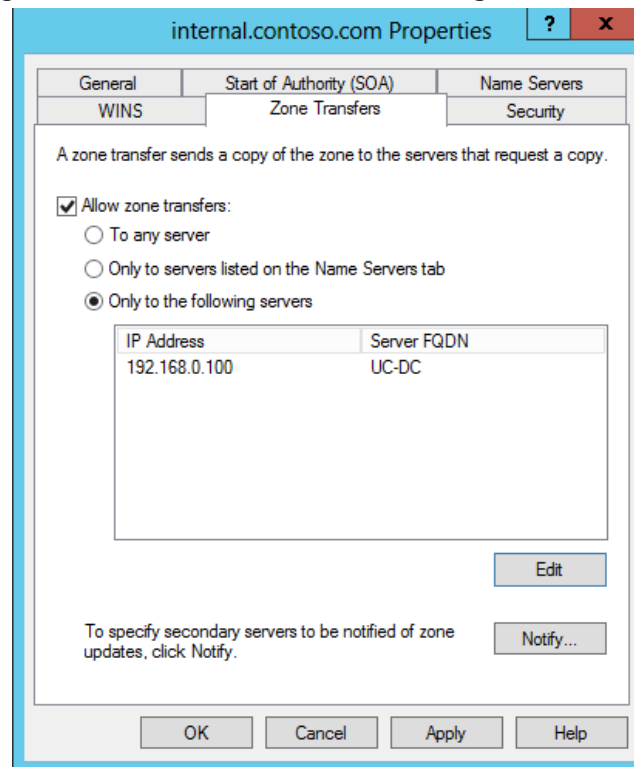
6. Complete the wizard and make sure the name servers from the enterprise forest are populated in the right pane under the zone just created

Figure 8-9: Results of Creating DNS Stub Zone



7. Populating the data from the Master DNS can take a few minutes. If, after a reasonable time, the name servers are not populated, open the enterprise forest DNS management console and right-click the enterprise FQDN forward lookup zone properties (in the example above: internal.contoso.com).
8. Check the settings on the Zone Transfers Tab and if 'Only to Servers listed on the Name Servers Tab' is selected, make sure the CloudBond 365 Controller IP address is listed there.

Figure 8-10: DNS Stub Zone - Restricting Zone Transfers



9. Perform the same steps on a DNS server in the enterprise forest, where the forward lookup stub zone should point to the CloudBond 365 FQDN instead (cloudbond365.local).
10. If the enterprise environment has multiple DNS servers that are not Active Directory integrated, there will be no default replication between them. Make sure all enterprise DNS servers are aware of the new Stub zone just created.
11. Repeat steps 1-10 for all other (child-) domains that require a trust with the CloudBond 365 domain.



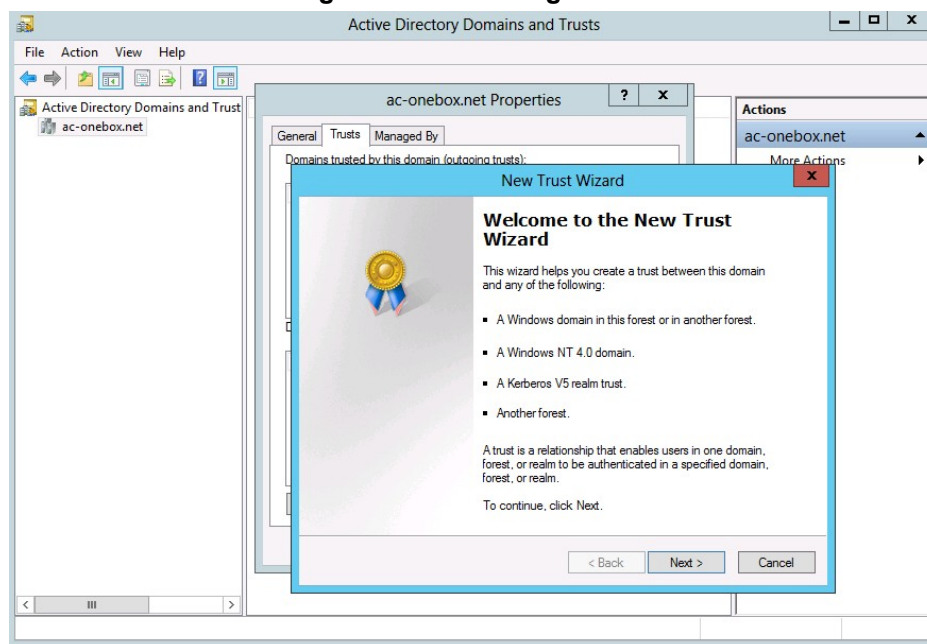
Note: Make sure 127.0.0.1 is not in use as the Primary DNS entry on the NIC of both CloudBond 365 controller and corporate Domain Controller. If you don't, the result may be a Forest Trust which appears correct but fails to work.

After the DNS cross Forest Name resolution is set up, a bidirectional forest trust can be created.

➤ **To set up a Forest Trust:**

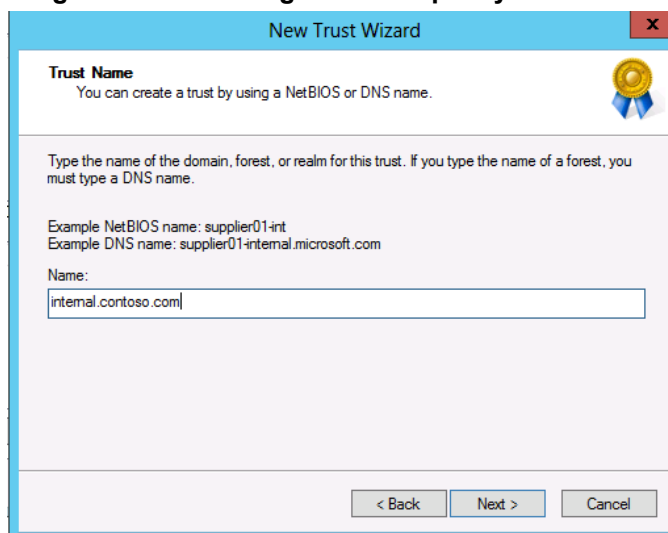
1. On the CloudBond 365 Controller, go to Active Directory Domains and Trusts and right-click the CloudBond 365 domain (cloudbond365.local) to select properties.
2. Go to the **Trusts** tab and select **New Trust**.

Figure 8-11: Creating a Trust

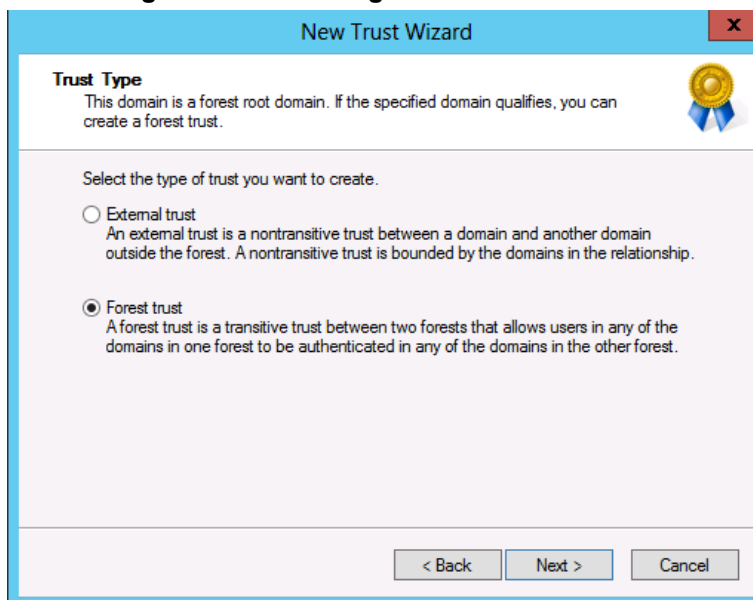


3. Specify the DNS name for the enterprise network (in the example here, **internal.contoso.com**).

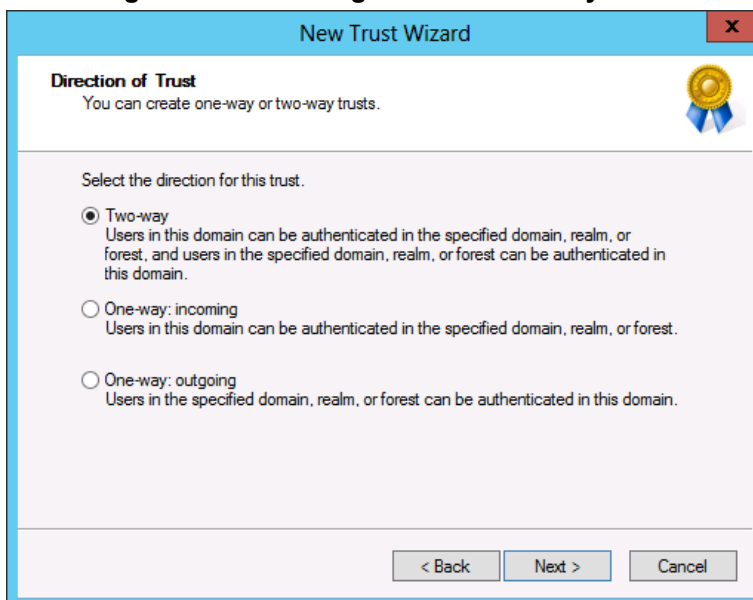
Figure 8-12: Creating a Trust - Specify the Domain



4. Select **Forest trust**.

Figure 8-13: Creating a Trust - Forest Trust

5. Specify an account with sufficient rights in the enterprise forest.
6. Select **Two-way**.

Figure 8-14: Creating a Trust - Two Way Trust

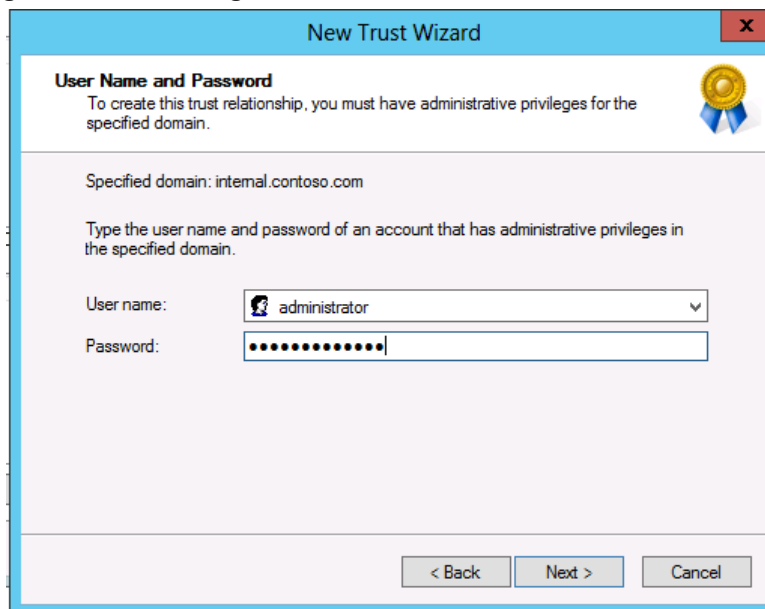
7. Use the wizard to create the trust in both locations (CloudBond 365 Forest and Enterprise Forest).

Figure 8-15: Creating a Trust - Create Both Sides of the Trust

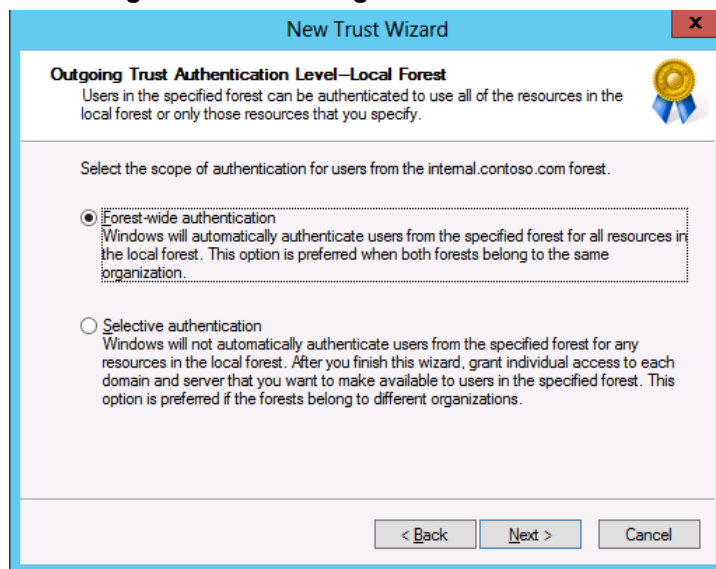
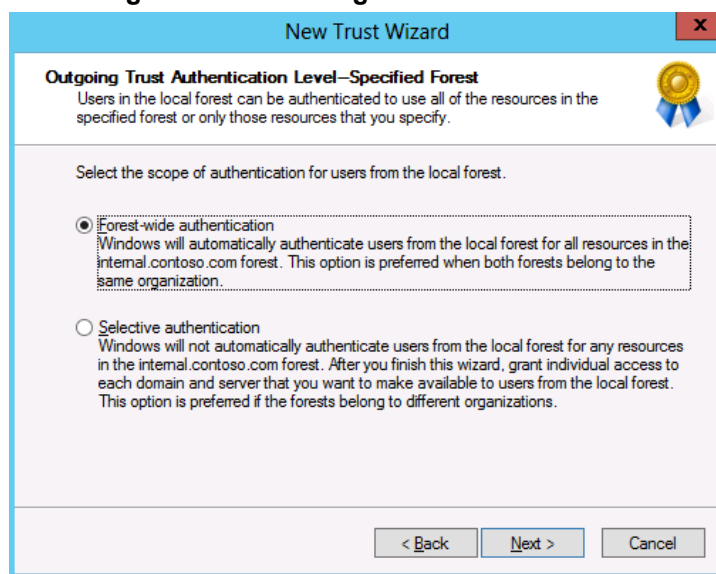


8. Specify the enterprise credentials with rights to create the “remote” trust

Figure 8-16: Creating a Trust - Enter Credentials for the Other Side



9. Select Forest-wide authentication for both:
 - Outgoing Trust Authentication Level – Local Forest
 - Outgoing Trust Authentication Level – Specified Forest

Figure 8-17: Creating a Trust - Forest Wide**Figure 8-18: Creating a Trust - Forest Wide**

10. Finish the wizard by clicking **Next** on the completion page.
11. After successful creation, click **Next** to confirm the outgoing and incoming trusts.

Figure 8-19: Confirming the Trust

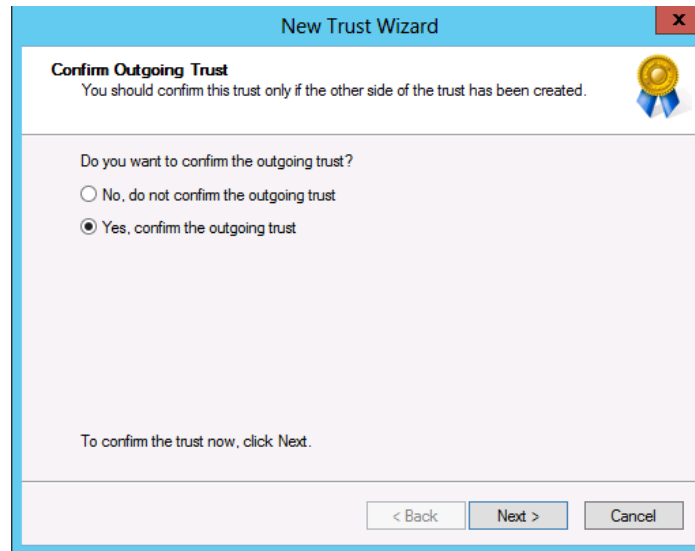
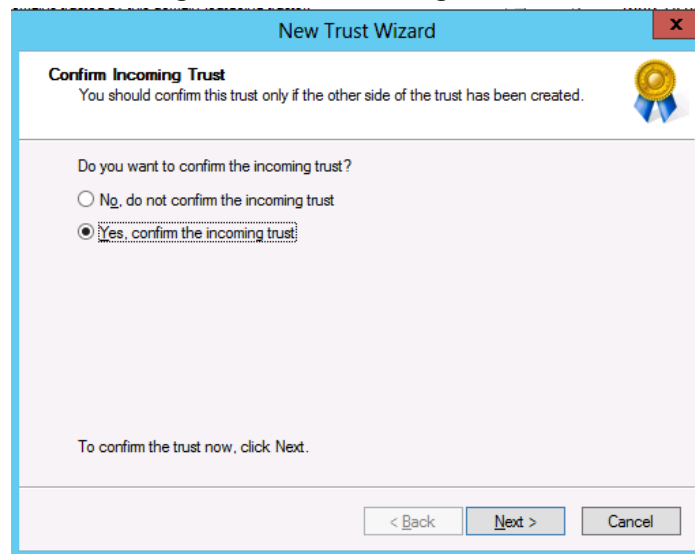
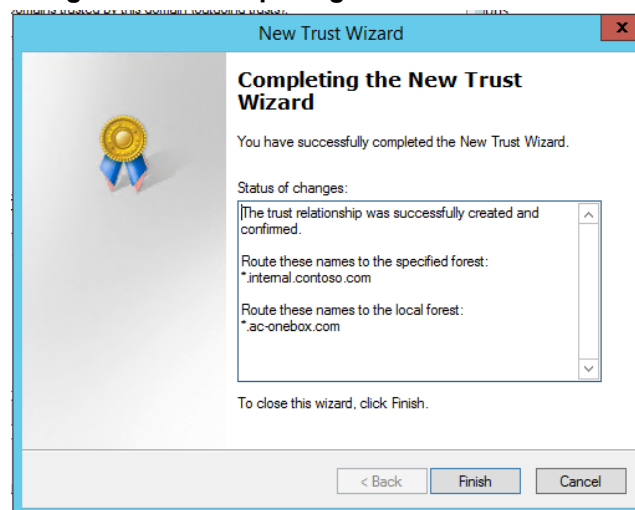


Figure 8-20: Confirming the Trust



12. A successful Trust Creation page should appear.

Figure 8-21: Completing the New Trust Wizard



8.2.6 Active Directory Synchronization

For complete integration of CloudBond 365 Skype for Business with Microsoft Exchange, CloudBond 365 must be able to update the user's ProxyAddress property with the CloudBond 365 Skype for Business SIP Address for objects within the corporate Active Directory. This updating is performed during the CloudBond 365 AD Connector Synchronization process (AcsUserReplication.exe), which runs as a Scheduled Task on the CloudBond 365 Controller.

For the ProxyAddress property to be updated with the correct SIP Address, the CloudBond 365 Administrator account (default cloudbond365/Administrator) must be given write permissions to update the objects within the source container (where your users objects are) of the corporate Domain Controller.

If Office 365 integration is enabled using Microsoft's DirSync or AADSync tool, the following five Active Directory attributes will also need to be populated towards the corporate Active Directory environment by the AcsUserReplication task:

- msRTCSIPUserEnabled
- msRTCSIPOptionFlags
- msRTCSIPDeploymentLocator
- msRTCSIPLine
- msRTCSIPPrimaryUserAddress



Warning: The AcsUserReplication scheduled task should only run on one management server in a multi-server environment. If multiple management servers are installed for redundancy, the scheduled tasks on the redundant servers should be disabled and only enabled if the primary server goes down, thereby preventing stale objects from being created in the Active Directory.

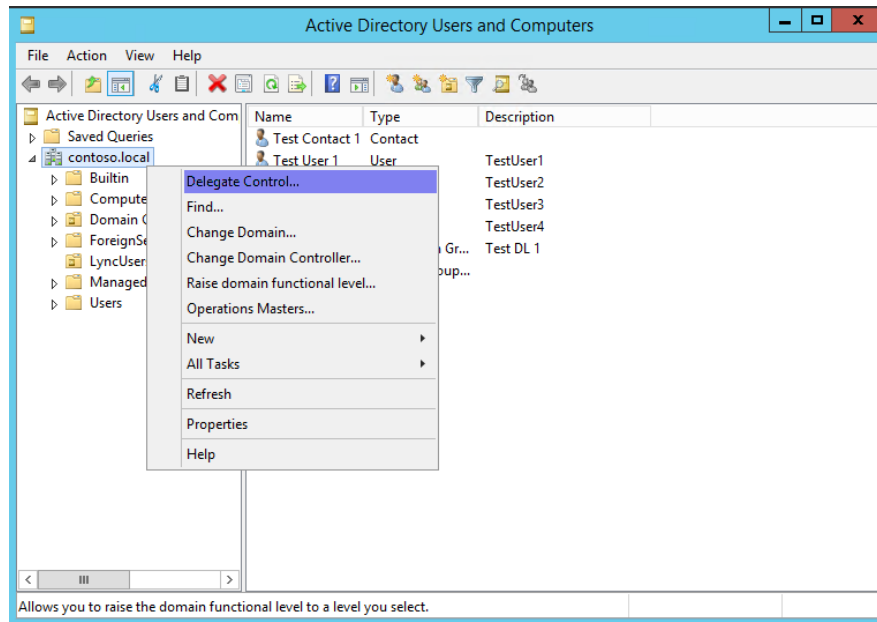
8.2.7 Delegate Control

Prepare the User Forest Active Directory for write access from the Resource forest (cloudbond365) administrator account.

➤ **To delegate control:**

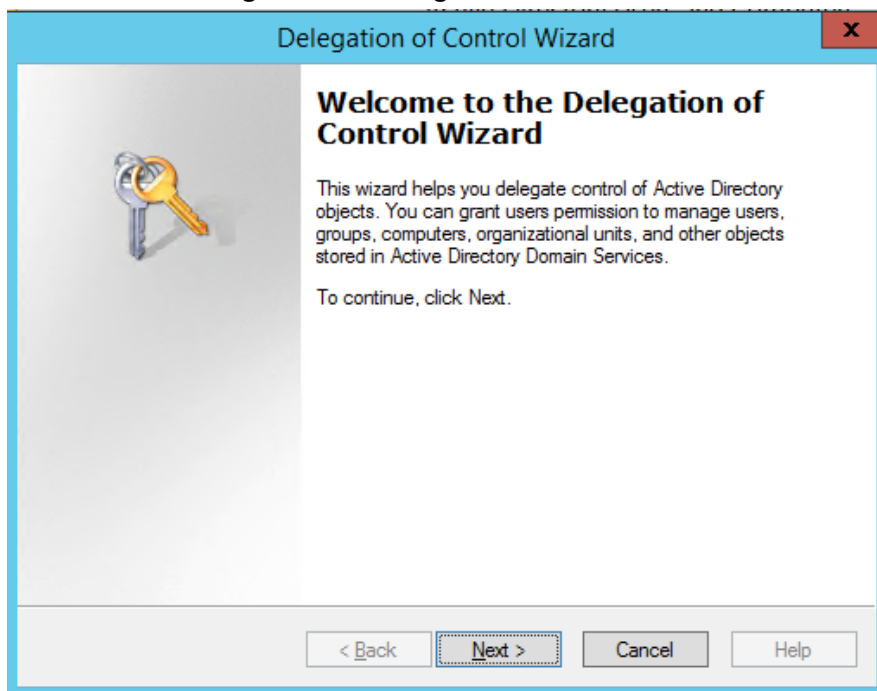
1. On the corporate customer's Domain Controller, open the Active Directory Users and Computers tool.
2. Right-click the top level domain, and select **Delegate Control...**:

Figure 8-22: Delegate Control

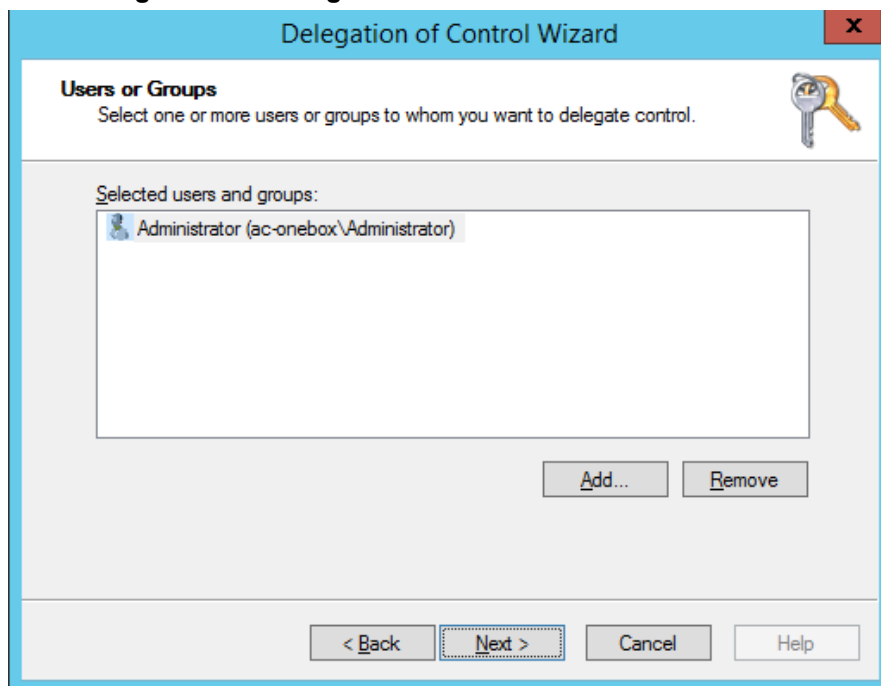


3. Click **Next**.

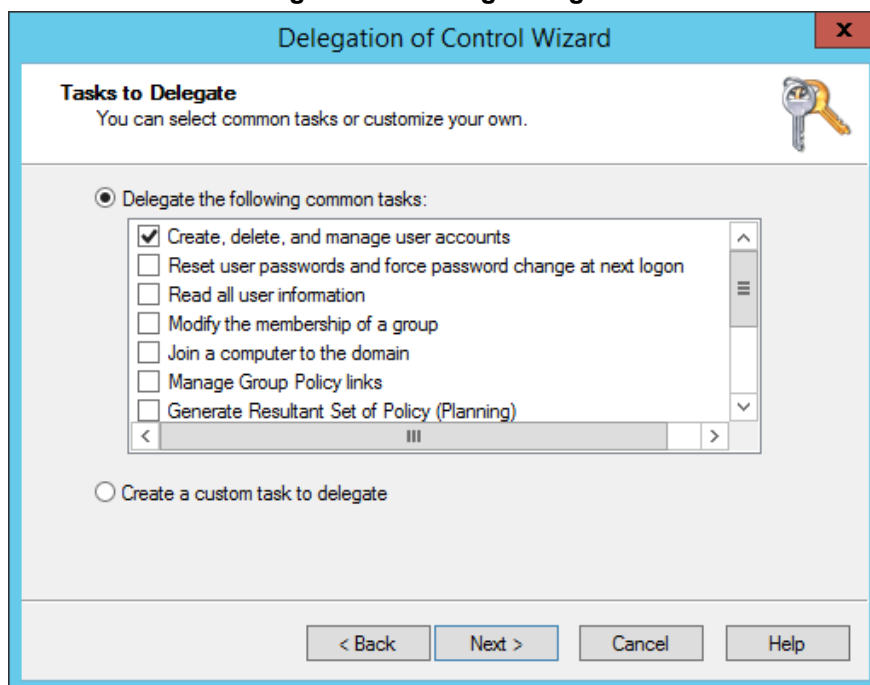
Figure 8-23: Delegate Control Wizard



4. Click **Add**.

Figure 8-24: Delegate to CloudBond 365 Administrator

5. Select the 'Create, delete, and manage user accounts' check box, and then click **Next**.

Figure 8-25: Delegate Rights

6. Click **Finish**.

Figure 8-26: Complete the Wizard



Note: Administrator accounts within the Organizational Unit (OU) will not follow the delegation. Microsoft best practice is not to use administrator accounts for regular use. If an Administrator account needs to be enabled, the security settings need to be applied using DSACLs on the AdminSDHolder container.

For more information, see:

[https://technet.microsoft.com/en-us/library/cc772662\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772662(v=ws.10).aspx)

8.2.8 Certificates

Private certificates were issued by the Certificate Authority (CA) installed on the CloudBond 365 controller. To fully access CloudBond 365 from a corporate network, you need to issue new certificates.

External certificate must be set to be able to connect to Microsoft® Office 365 Exchange UM via the Edge.

For more information, see Section 10 on page 147.

8.3 Skype for Business DNS Records

For Microsoft Skype for Business to function correctly, some special DNS records must be created in the public or in the private name space. Skype for Business clients use various DNS records in various sequences to automatically locate Skype for Business services and log in.



Note: Although user clients are not used in CloudBond X-UM, we still perform "full" DNS settings, the same as is done when clients are used.

When you need to provide an external Web access IP address, use the Edge external IP address or another IP.

One possible DNS configuration is what Microsoft describes as “split brained” DNS. In this configuration:

- Separate DNS servers are used for internal and external records.
- Both internal and external DNS servers are authoritative for the same DNS domain.
- The internal or enterprise DNS server contains only the internal DNS records.
- The external or public DNS server contains only the external DNS records, which are publicly available.

Other DNS configurations are possible.

8.3.1 Skype for Business Internal Records

Internal records generally refer to the private IP address space

- SRV: `_sipinternaltls._tcp.<FQDN>` over port 5061 to `sip.<FQDN>`
- SRV: `_sipinternal._tcp.<FQDN>` over port 5061 to `sip.<FQDN>`
- SRV: `_sip._tls.<FQDN>` over port 5061 to `sip.<FQDN>`
- A: `lyncdiscoverinternal.<FQDN>`
- A: `sip.<FQDN>`

If you change the Simple URLs, you may also need:

- A: `meet.<FQDN>` (in a default CloudBond 365 installation, `meet` is used for both dialing and `meet simple` URLs)

8.3.2 Skype for Business External Records

External records refer to public IP addresses

- SRV: `_sipfederationtls._tcp.<FQDN>` over port 5061 to `sip.<FQDN>`
- SRV: `_sip._tls.<FQDN>` over port 5061 to `sip.<FQDN>`
- A: `sip.<FQDN>`
- A: `sipexternal.<FQDN>`
- A: `meet.<FQDN>` (in a default CloudBond 365 installation, `meet` is used for both dialing and `meet simple` URLs)
- A: `ewslync.<FQDN>` (is assigned to the default CloudBond 365 Skype for Business external web services)
- CNAME: `Lyncdiscover.<FQDN>` pointing to `ewslync.<FQDN>`

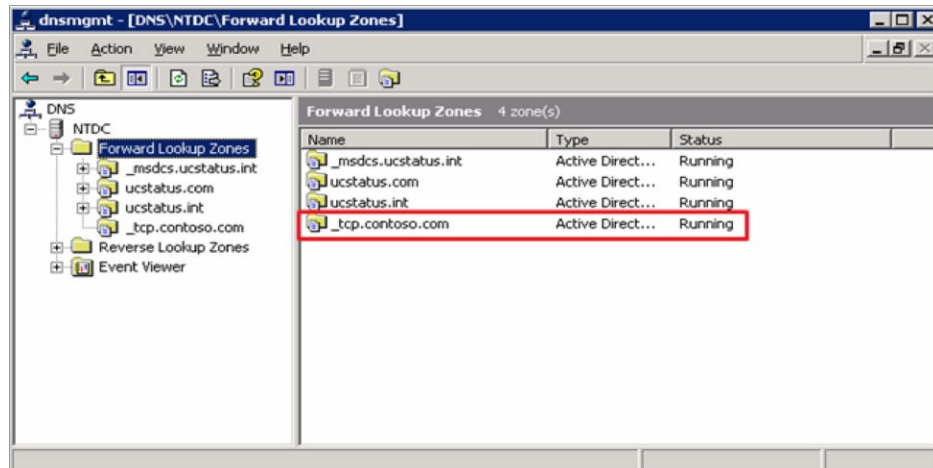
8.3.3 Skype for Business DNS Records without the Entire DNS Zone

When customers are unable to or unwilling to create a DNS Zone of the Public namespace internally in their AD environment, you need to get automatic configuration to function.

➤ **To get automatic configuration to function:**

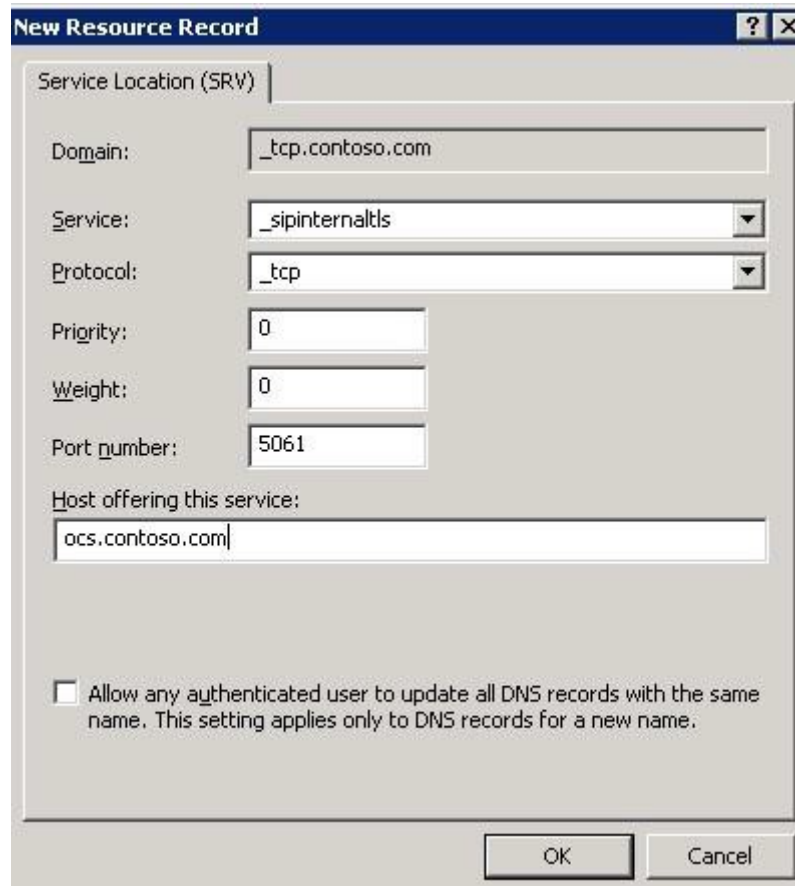
1. Create a new DNS zone that mimics the SRV Record Domain. The figure below shows an example of a completed domain .

Figure 8-27: Forward Lookup Zones



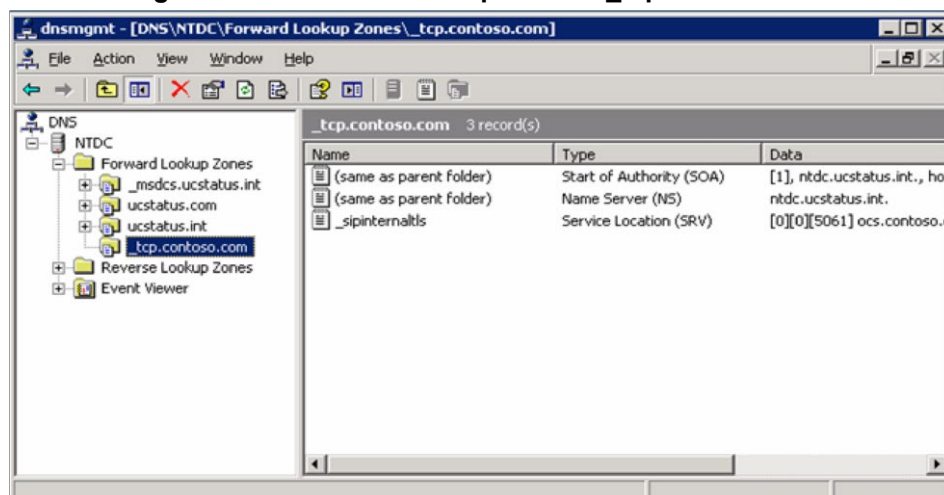
2. After the SRV Domain has been created, create the *_sipinternaltls* SRV Record in the domain. Since the zone was created with *_tcp* when the record was created, it will create it in the root of this zone.

Figure 8-28: New Resource Record



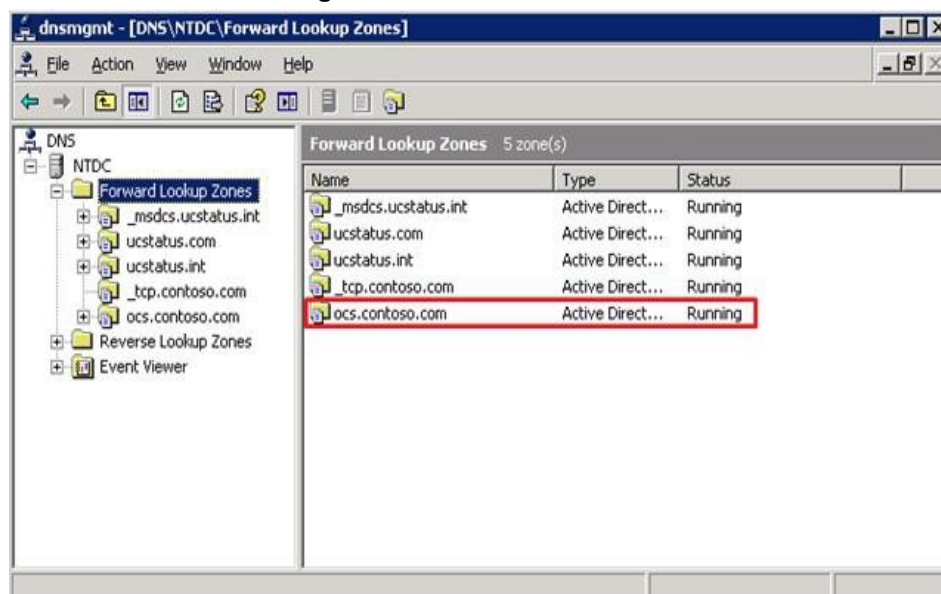
3. View **record_sipinternaltls._tcp.contoso.com** created in the root of the **_tcp.contoso.com** zone.

Figure 8-29: Forward Lookup Zones - _tcp.contoso.com



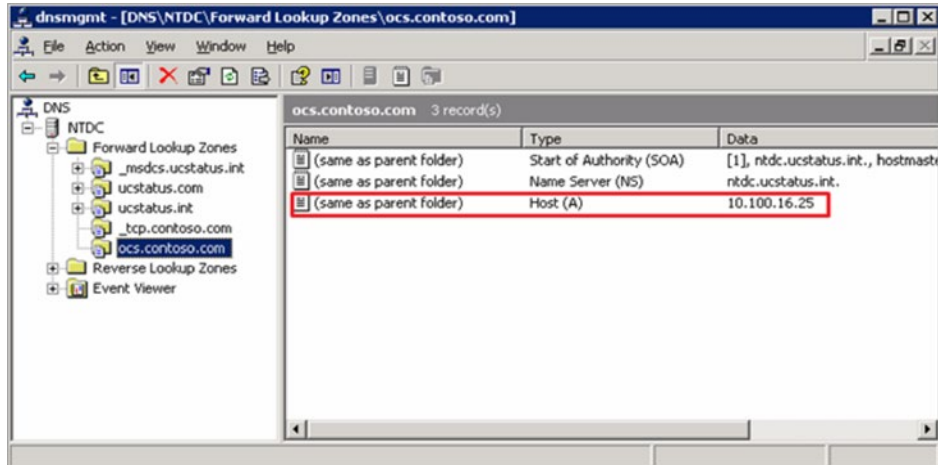
4. Create the host record you used when creating the SRV Record. In this scenario, **ocs.contoso.com** was used. This A-record cannot be created in the SRV Zone that was created earlier. If the host record was created in this zone, it would become **ocs._tcp.contoso.com** which is not where the SRV record that was created points to. Instead, create a new zone with the name of the host record.

Figure 8-30: ocs.contoso.com



5. In this zone, create a blank host record that points to the CloudBond 365 Server. This will use the Parent (Zone Name) for this record.

Figure 8-31: ocs.contoso.com – 3 records



Warning: The above configuration, created with the management console, does not function if you have non-Windows clients. To be able to use non-Windows clients, use the **dnscmd** command line tool instead.

8.3.3.1 DNS Records for Non-Windows Clients

For **Contoso**, the required commands are:

```

dnscmd . /zoneadd _sipinternaltls._tcp.contoso.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.contoso.com. @ SRV 0 0 5061 sip.contoso.com.
dnscmd . /zoneadd sip.contoso.com. /dsprimary
dnscmd . /recordadd sip.contoso.com. @ A 172.16.45.12
  
```

Make changes appropriate to your environment. If you're not running the command on your Windows DNS server, replace the first dot with your server name. You may also prefer a different zone type to **dsprimary**. If so, change the **zoneadd** commands appropriately.

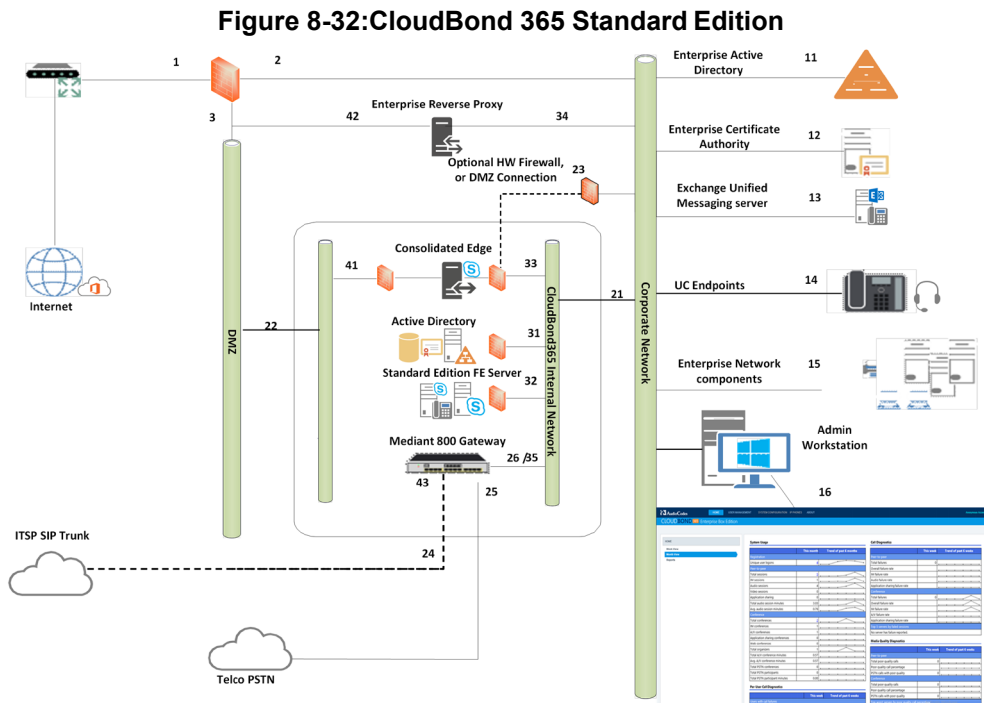
8.4 Firewall Port Requirements

This chapter describes the port requirements for placing the CloudBond X-UM system behind a firewall. This guide provides the following:

- Overview of CloudBond 365 Deployment
- Perimeter Network port requirements for Consolidated Edge
- Port Requirements if internal firewalls are deployed

8.4.1 CloudBond 365 Deployment Overview

A network diagram for CloudBond 365 Standard Plus Edition deployed in an enterprise network is shown below:



8.4.1.1 References

The items below correspond to the entries on the Network diagrams.

8.4.1.1.1 Existing Corporate Firewall

Each customer will have their own existing Internet access, firewall, and network configuration. Each will vary in capacity, features and capabilities.

The Enterprise Firewall and networks shown in the diagram are examples only. Each CloudBond X-UM installation will need to be adapted to suit the customer environment.

6. The public Internet side of the corporate firewall:
 - This IP address may be required if NATing is used to access the Edge server.
 - If NATing is used, Public DNS records for SIP will point here
 - If the Firewall is also a Reverse Proxy server, other DNS records may point here
7. The private internal corporate LAN:
 - This IP address may be used as a gateway address for internal servers to access the Internet. e.g., Windows Updates
8. The DMZ or other network for servers with external access:
 - This IP address will be used as a gateway address for externally accessible servers, such as Edge and Reverse Proxy.

8.4.1.1.2 Existing Internal Corporate Servers

11. Enterprise Active Directory
 - Used for Forest trust and user replication. May also host corporate DHCP and DNS servers
12. Enterprise Certificate Authority
 - Used to issue internal private certificates for communication with Skype for Business servers
13. Exchange Unified Messaging Server
 - Used for enterprise Voicemail features of Skype for Business
14. UC Endpoints
 - Skype for Business clients. May be either Skype for Business phone edition or Skype for Business Client Software



Note: Skype for Business mobile clients are used externally to the corporate network.

15. Enterprise Network Component
16. Admin Workstation
 - Typical Administrators workstation, used to access CloudBond Management Suite application and also RDP to Skype for Business servers for maintenance activities

8.4.1.1.3 CloudBond 365 Physical Connections

CloudBond X-UM have “spare” network adapters (25) which can optionally be used to separate network traffic and enhance network security where required.

21. Corporate LAN Connection (trusted network)
 - Front GE1 connector
22. DMZ Connector (untrusted public network)
 - Rear GE1 connector

- 23. Optional Edge firewall connector
 - Rear GE2 connector
- 24. Optional SBC ITSP Connection
 - Front GE3 connector or WAN connector
- 25. PSTN Connection (typically ISDN BRI or PRI)
- 26. Media Gateway internal IP Address
 - Typically the management connection address (OAMP)
 - May also be media address for IP Calls e.g. OAMP + Media + Control
 - Default CloudBond 365 Standard edition is 192.168.0.2

8.4.1.1.4 CloudBond 365 Internal Connections

The CloudBond 365 Systems have an internal trusted network and an external untrusted network (DMZ)

8.4.1.1.4.1 Internal Trusted Networks

It is safe to connect this network directly to the Corporate LAN. All CloudBond 365 components with connections to this network are meant to act as internal servers.

Whilst a firewall may be placed between this network and the Corporate LAN, doing so complicates the deployment and requires significant firewall configuration.

You may use the “spare” network adapters to provide traffic separation; however, doing so requires additional manual configuration of the CloudBond 365 component affected.

- 31. CloudBond 365 Controller IP address (UC-DC):
 - Used for maintenance and access to CloudBond Management Suite application
 - Used for Forest trust with Enterprise DC.
 - SfB reporting and monitoring server DB
 - Default 192.168.0.101
- 32. Skype for Business Standard Edition Front End Server (UC-FE):
 - Used for all Skype for Business processing
 - SfB Mediation server
 - Default 192.168.0.102
 - Entry in internal DNS typically sip.contoso.com and meet.contoso.com
- 33. Skype for Business Consolidated Edge Server (UC-Edge)
 - Used for Skype for Business external communications, including external users, federation, etc.
 - Default 192.168.0.103
 - To enhance security, an additional rear Ethernet connector and internal hardware firewall can be used to separate this server from the corporate network. See 23.
- 34. AudioCodes SBC:
 - Available as SBC component of Mediant 800 gateway
 - Default address 192.168.0.2
- 35. X-UM Connector (X-UM)
- 36. Used for SIP and RTP between SBC and Skype for Business Standard Edition Front End Server (UC-FE).
 - Default 192.168.0.105

8.4.1.1.4.2 External Untrusted Networks

This network may be connected directly to the Corporate DMZ. All CloudBond 365 components connected to this network have their own firewalls enabled, and are designed for connection to untrusted networks.

You may use the “spare” network adapters to provide traffic separation, but doing so requires additional manual configuration of the CloudBond 365 component affected.

41. Edge external connection:

- Used for external user access, federation, etc.
- May use NATing of Enterprise Firewall
- Default address 192.168.254.103
- Entry required in Public DNS and Certificates. Typically sip.contoso.com, plus SRV DNS records.

43. SBC External Address:

- Used as SIP Trunk endpoint from ITSP

8.4.1.1.4.3 One Voice Operations Center Management Network

The One Voice Operations Center Management Networks applies only when your CloudBond 365 is to be managed by the AudioCodes Element Management System (One Voice Operations Center), for example, for remote monitoring or for One Voice Operations Center license pool management).

The CloudBond 365 management server should have access to the One Voice Operations Center server usually located on the Service Provider's premises or for large companies in the company's data center.

8.4.1.1.4.4 Internet Access

In general, each of the CloudBond X-UM server components may need some level of internet access, as would normally be available Enterprise network users. Access is required for activities such as:

- Windows Activation
- Windows Updates
- General Web browsing such as Microsoft Skype for Business reference documentation
- Downloading specific fixes and Skype for Business phone edition updates from Microsoft web sites.

In addition, the CloudBond 365 Controller (DC) will need internet access to retrieve user information from Office365, via port 443.

8.4.2 Perimeter Network Port Requirements

The most important components that are almost always separated by hardware firewall devices is the Skype for Business Edge server component. The firewall ports required to be opened are discussed in this topic.

8.4.2.1 Edge Server

The CloudBond 365 Edge server passes traffic between the external network (internet) and the CloudBond 365 Front End and Mediation servers. This traffic includes SIP Access, Web Conferencing, and A/V service, amongst other features. It is largely control and media based traffic.

8.4.2.1.1 Determining External A/V Firewall and Port Requirements

The firewall port requirements for external (and internal) SIP and conferencing (PowerPoint presentations, white boarding and polling) interfaces are consistent, regardless of the version your federation partner is running. The same is not true for the Audio/Video Edge external interface.

In most cases, the A/V Edge service requires that external firewall rules allow RTP/TCP and RTP/UDP traffic in the 50,000 through 59,999 port range to flow in one or both directions. For example, opening this port range is required to support certain federation scenarios.

When reading the tables, *(in)* refers to traffic sent from a less trusted network to a more trusted network, such as Internet-to-perimeter or perimeter-to-corporate. For example, traffic from the Internet to the Edge external interface or from the Edge internal interface to the next hop pool. *(out)* refers to traffic sent from a more trusted network to a less trusted network, such as corporate-to-perimeter or perimeter-to-Internet. For example, traffic from a corporate pool to the Edge internal interface or from the Edge external interface to the Internet. *(in/out)* refers to traffic that traverses in both directions.

8.4.2.1.1.1 Inbound/Outbound Edge Traffic

Figure 8-33: Edge Server

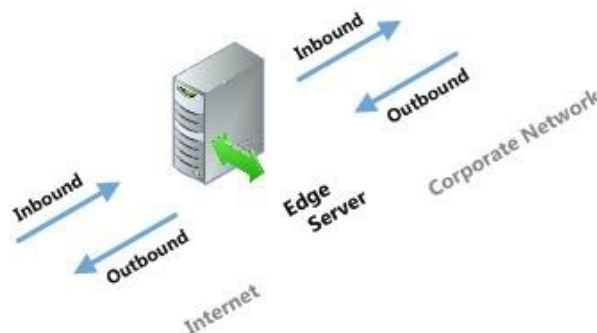
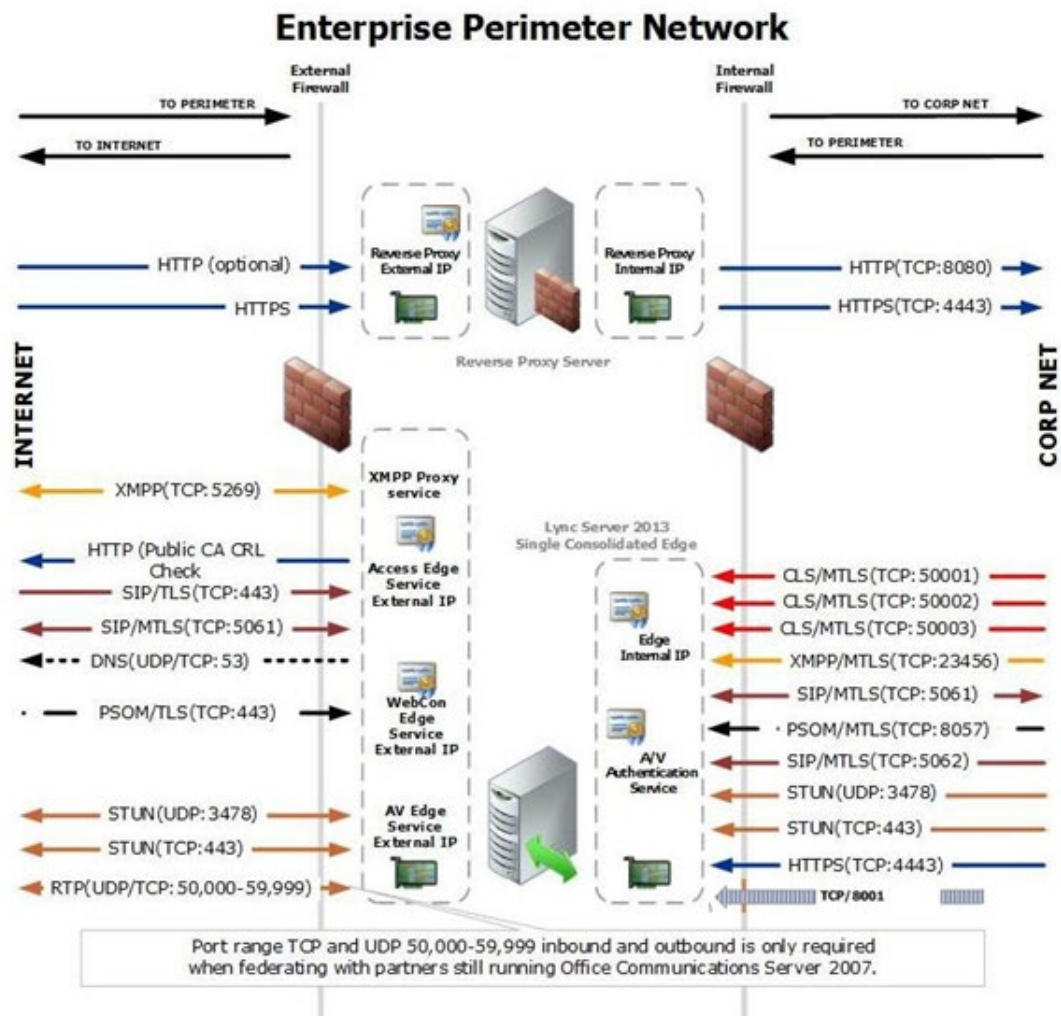


Figure 8-34: Enterprise Perimeter Network



8.4.2.1.2 Firewall Summary for Single/Scaled Consolidated Edge:External Interface #41

Protocol/Port which are Grayed are needed for specific Skype service that is not needed for basic CloudBond X-UM functionality (no clients, no conference services...)

Table 8-1: Edge Server

Protocol/Port	Used for
XMPP/TCP/5269 (in/out)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
HTTP 80 (out)	Checking certificate revocation lists
DNS 53 (out)	External DNS queries
SIP/TLS/MTLS/5061 (in/out)	Client to server SIP traffic for remote user access Federation and connectivity with a hosted Exchange service
PSOM/TLS/444 (in)	Remote user access to conferences for anonymous and federated users
RTP/TCP/50K range (in)	Media exchange and Windows Live Messenger if public IM connectivity is enabled. Required for Office Communications Server 2007 R2 interoperability
RTP/TCP/50K range (out)Media exchange	Media exchange
RTP/UDP/50K range (out)	Media exchange or A/V with Windows Live Messenger Required for Office Communications Server 2007 interoperability
STUN/MSTURN/UDP/3478 (in/out)	External user access to A/V sessions (UDP)
STUN/MSTURN/TCP/443 (in)	External user access to A/V sessions and media (TCP)

8.4.2.1.3 Firewall Details for Single/Scaled Consolidated Edge:Internal Interface #33

Protocol/Port which are Grayed are needed for specific Skype service that is not needed for basic Cloudbond X-UM functionality (no clients, no conference services...)

Table 8-2: Edge Server

Protocol/Port	Used for
XMPP/MTLS/TCP (out)	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/5061 (in/out)	SIP traffic
PSOM/MTLS/8057 (out)	Web conferencing traffic from pool to Edge Server
SIP/MTLS/5062 (out)	Authentication of A/V users (A/V authentication service)
STUN/MSTURN/UDP/3478 (out)	Preferred path for media transfer between internal and external users (UDP)
STUN/MSTURN/TCP/443 (out)	Alternate path for media transfer between internal and external users (TCP)
HTTPS 4443 (out)	Pushing Central Management store updates to Edge Servers
TCP 8001 (out)	CloudBond 365 Edge worker process
MTLS/TCP/50001 (out)	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection.
MTLS/TCP/50002 (out)	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection.
MTLS/TCP/50003 (out)	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection.



Note: We recommend that you open only the ports required to support the functionality for which you are providing external access.



Warning: For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the Access Edge service is involved in instant messaging (IM), presence, web conferencing, and audio/video (A/V).

8.4.2.2 Management Server

These firewall settings are required only if your CloudBond 365 is to be managed and monitored by the AudioCodes One Voice Operations Center. These changes need to be applied to the Hyper-V Host.

8.4.2.2.1 Firewall Details for Hyper-V Host Server: Internal Interface #21

Table 8-3: Hyper-V Host Server

Protocol/Port	Used to
HTTPS 443 (out)	Connect to the One Voice Operations Center Server to retrieve updates from the License Pool Manager, for example, to retrieve the latest license.
SNMP (UDP) 162 (out)	Connect to the One Voice Operations Center Server to send alarms raised on the SBC/gateway platform and on the CloudBond 365 Microsoft Windows 2012 R2 platform.
SNMP (UDP) 1161 (out)	Connect to the One Voice Operations Center Server to send Keep-alive traps that are used for the One Voice Operations Center to add CloudBond devices to the One Voice Operations Center, and for the CloudBond 365 keep-alive status.

8.4.3 Other Port Requirements

This paragraph describes the port requirements for internal server to server and client to server communications.

In most cases, the IP addresses of the CloudBond 365 system domain controller and Front-End server reside on the corporate subnet and are not separated by a hardware firewall device. If this is also the case in your network, the remainder of this document can be skipped and is not needed for your deployment.

8.4.3.1 Network Ports Used by Trusts

Due to the fact that trusts must be deployed across various network boundaries, they might have to span one or more firewalls. When this is the case, you can either tunnel trust traffic across a firewall or open specific ports in the firewall to allow the traffic to pass through.

The following table defines the server listening ports used by network trusts. The server listening ports correspond to the numbers 11, 21 and 31 for the Domain Controllers / DNS servers in the diagram above and are considered to be inbound for all servers.

8.4.3.1.1 Required Active Directory Trust Listening Ports: Interfaces #11, #21, #31

The following ports should be open to allow communication between the CloudBond 365 Domain Controller (33 or 23) and the Corporate Domain controller (11).

Table 8-3: AD Trust

Server Port	Service
123/UDP	W32Time
135/TCP	RPC-EPMAP
138/UDP	NetBIOS
49152 -65535/TCP	RPC
389/TCP/UDP	LDAP
636/TCP	LDAP SSL
3268/TCP	LDAP GC
3269/TCP	LDAP GC SSL
53/TCP/UDP	DNS
135, 49152 -65535/TCP	RPC DNS
88/TCP/UDP	Kerberos
445/NP-TCP/NP-UDP	SAM/LSA

8.4.3.1.2 RPC

(*)With Registry Editor, you can modify the following parameters for RPC. The RPC Port key values discussed below are all located in the following key in the registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet\ Key Data Type

8.4.3.1.2.1 Ports REG_MULTI_SZ

This specifies a set of IP port ranges consisting of either all the ports available from the Internet or all the ports not available from the Internet. Each string represents a single port or an inclusive set of ports. For example, a single port may be represented by 5984, and a set of ports may be represented by 5000-5100. If any entries are outside the range of 0 to 65535, or if any string cannot be interpreted, the RPC runtime treats the entire configuration as invalid.

8.4.3.1.2.2 PortsInternetAvailable REG_SZ

This uses Y or N (not case-sensitive).

If Y, the ports listed in the Ports key are all the Internet-available ports on that computer. If N, the ports listed in the Ports key are all those ports that are not Internet-available.

8.4.3.1.2.3 UseInternetPorts REG_SZ

This uses Y or N (not case-sensitive). It specifies the system default policy.

If Y, the processes using the default will be assigned ports from the set of Internet-available ports, as defined previously.

If N, the processes using the default will be assigned ports from the set of Intranet-only ports.

Example:

1. Add the Internet key under: HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc
2. Under the Internet key, add the values "Ports" (MULTI_SZ), "PortsInternetAvailable" (REG_SZ), and "UseInternetPorts" (REG_SZ).

In this example ports 5000 through 5100 inclusive have been arbitrarily selected to help illustrate how the new registry key can be configured. For example, the new registry key appears as follows:

■	Ports:	REG_MULTI_SZ:	5000-5100
■	PortsInternetAvailable:	REG_SZ:	Y
■	UseInternetPorts:	REG_SZ:	Y

3. Restart the server. All applications that use RPC dynamic port allocation use ports 5000 through 5100, inclusive. In most environments, a minimum of 100 ports should be opened, because several system services rely on these RPC ports to communicate with each other.

You should open up a range of ports above port 5000. Port numbers below 5000 may already be in use by other applications and could cause conflicts with your DCOM application(s). Furthermore, previous experience shows that a minimum of 100 ports should be opened, because several system services rely on these RPC ports to communicate with each other.

8.4.3.2 Ports and Protocols Used by the Skype for Business Internal Servers

This section summarizes the listening ports and protocols used by the Skype for Business Server components with listening interface 5 in the before mentioned diagram (which diagram?).



Warning: Windows Firewall must be running before you start the Skype for Business Server.

8.4.3.2.1 Required CloudBond 365 Server listening Ports on Interface Number #21

Table 8-4: Skype for Business Servers

Server Ports	Service name	Notes
80/TCP *	IIS service	Used for accessing the CloudBond 365 sysadmin interface
135/TCP	Skype for Business Server Front- End service	Used for DCOM based operations such as Moving Users, User Replicator Synchronization, and Address Book Synchronization.
443/TCP	Skype for Business Server Web Compatibility service	Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components).

Server Ports	Service name	Notes
444/TCP	Skype for Business Server Front- End service	Used for HTTPS communication between the Focus (the Skype for Business Server component that manages conference state) and the individual servers. This port is also used for TCP communication between Front End Servers and Survivable Branch Appliances.
445/TCP	Skype for Business Server Master Replicator Agent service	Used to push configuration data from the Central Management store to servers running Skype for Business Server.
448/TCP	Skype for Business Server Bandwidth Policy Service	Used for call admission control by the Skype for Business Server Bandwidth Policy Service.
1434/UDP	SQL Browser	SQL Browser for local replicated copy of Central Management store data in local SQL Server instance
3389/TCP *	TermService	Used for accessing the server through an RDP client.
4443/TCP	Skype for Business Server Web Compatibility service	Used for communication from Front End Servers to the web farm FQDNs (the URLs used by the External IIS web components).
5060/TCP	Skype for Business Server Mediation service	Used for incoming SIP requests from the PSTN gateway to the Mediation Server
5061/TCP	Skype for Business Server Front- End service	Used by Standard Edition servers and Front End pools for all internal SIP communications between servers (MTLS), for SIP communications between Server and Client (TLS) and for SIP communications between Front End Servers and Mediation Servers (MTLS). Also used for communications with Monitoring Server.
5062/TCP	Skype for Business Server IM Conferencing service	Used for incoming SIP requests for instant messaging (IM) conferencing.
5063/TCP	Skype for Business Server Audio/Video Conferencing service	Used for incoming SIP requests for audio/video (A/V) conferencing.
5064/TCP	Skype for Business Server Conferencing Attendant service (dial-in conferencing)	Used for incoming SIP requests for dial-in conferencing.

Server Ports	Service name	Notes
5065/TCP	Skype for Business Server Application Sharing service	Used for incoming SIP listening requests for application sharing.
5066/TCP	Not applicable	Used for outbound Enhanced 9-1-1 (E9-1-1) gateway.
5067/TCP	Skype for Business Server Mediation service	Used for incoming TLS SIP requests from the PSTN gateway to the Mediation Server.
5070/TCP	Skype for Business Server Mediation service	Used by the Mediation Server for incoming requests from the Front End Server to the Mediation Server.
5071/TCP	Skype for Business Server Response Group service	Used for incoming SIP requests for the Response Group application.
5072/TCP	Skype for Business Server Conferencing Attendant service (dial-in conferencing)	Used for incoming SIP requests for Microsoft Skype for Business 2010 Attendant (dial in conferencing).
5073/TCP	Skype for Business Server Conferencing Announcement service	Used for incoming SIP requests for the Skype for Business Server Conferencing Announcement service (i.e., for dial-in conferencing).
5075/TCP	Skype for Business Server Call Park service	Used for incoming SIP requests for the Call Park application.
5076/TCP	Skype for Business Server Audio Test service	Used for incoming SIP requests for the Audio Test service.
5080/TCP	Skype for Business Server Bandwidth Policy Service	Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic.
5081/TCP	Skype for Business Server Mediation service	Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.
5082/TCP	Skype for Business Server Mediation service	Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.
8057/TCP	Skype for Business Server Web Conferencing service	Used to listen for Persistent Shared Object Model (PSOM) connections from client.

Server Ports	Service name	Notes
8058/TCP	Skype for Business Server Web Conferencing Compatibility service	Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Communicator.
8404/TCP	Skype for Business Server Response Group service	Used for incoming SIP requests for the Response Group application.
8861/TCP	EMS Agent	Used for report components alarms from the EMS Monitor Agents to the EMS main agent.
8863/TCP	EMS Agent (One Voice Operations Center)	Used by the EMS main agent to retrieve the status from the EMS Monitor Agents.
49152-65335/TCP	Skype for Business Server Application Sharing service	Media port range used for application sharing. This range can be restricted with the Set-CSWebServer <FQDN of Web Server> -AppSharingPortCount <at least 100> -AppSharingPortStart <port start> cmdlet
49152-57500/TCP/UDP	Various	Media port range used for audio conferencing on all internal servers. Used by all servers that terminate audio: Front End Servers (for Skype for Business Server Conferencing Attendant service, Skype for Business Server Conferencing Announcement service, and Skype for Business Server Audio/Video Conferencing service), and Mediation Server. This range can be restricted with the Set-CSWebServer <FQDN of Web Server> -AudioPortCount <at least 100> -AudioPortStart <port start> cmdlet
57501-65335/TCP/UDP	Skype for Business Server Audio/Video Conferencing service	Media port range used for video conferencing. This range can be restricted with the Set-CSWebServer <FQDN of Web Server> -VideoPortCount <at least 100> -VideoPortStart <port start> cmdlet



Note: *Those ports are only required to be open from management workstations (identified by number 16 in the diagram).



Note: Some remote call control scenarios require a TCP connection between the Front End Server or Director and the PBX. Although Lync 2010 no longer uses TCP port 5060, during remote call control deployment you create a trusted server configuration, which associates the RCC Line Server FQDN with the TCP port that the Front End Server or Director will use to connect to the PBX system. For details, see the CsTrustedApplicationComputer cmdlet in the Skype for Business Server Management Shell documentation.

8.4.3.2.2 Ports and Protocols Used By Skype for Business Clients (Diagram # 14)

Table 8-35: Skype for Business Clients

Port	Notes
67/68/DHCP	Used by Skype for Business Server to find the Registrar FQDN (that is, if DNS SRV fails and manual settings are not configured).
443/TCP (TLS)	Used for client-to-server SIP traffic for external user access.
443/TCP (PSOM/TLS)	Used for external user access to web conferencing sessions.
443/TCP (STUN/MSTURN)	Used for external user access to A/V sessions and media (TCP)
3478/UDP (STUN/MSTURN)	Used for external user access to A/V sessions and media (TCP)
5061/TCP (MTLS)	Used for client-to-server SIP traffic for external user access.
6891-6901/TCP	Used for file transfer between Lync 2010 clients and previous clients (clients of Microsoft Office Communications Server 2007 R2, Microsoft Office Communications Server 2007, and Live Communications Server 2005).
1024-65535* TCP/UDP	Audio port range (minimum of 20 ports required)
1024-65535* TCP/UDP	Video port range (minimum of 20 ports required).
1024-65535 * TCP	Peer-to-peer file transfer (for conferencing file transfer, clients use PSOM).
1024-65535* TCP	Application sharing.
67/68* DHCP	Used by the listed devices ⁱ to find the Skype for Business Server certificate, provisioning FQDN, and Registrar FQDN.



Note: *To configure specific ports for these media types, use the `CsConferencingConfiguration` cmdlet (ClientMediaPortRangeEnabled, ClientMediaPort, and ClientMediaPortRange parameters).



Note: Skype for Business Server clients automatically creates the required operating-system firewall exceptions on the client computer.



Note: The ports that are used for external user access are required for any scenario in which the client must traverse the organization's firewall (for example, any external communications or meetings hosted by other organizations).

8.4.4 Windows Update and SysAdmin Update Port Requirements

To be able to download updates for the Microsoft software, the TCP port 8530 needs to be opened to the Internet from interfaces 31, 32, 33 via 21,2 and 1. In addition to Microsoft updates, AudioCodes also provides an update service for the Sysadmin interface. To be able to receive updates on Sysadmin, TCP port 8350 needs to be opened to the internet as well.

8.4.4.1 Port Requirements for Integration with Exchange 2010 SP1 Unified Messaging

Microsoft Exchange Server 2010 Unified Messaging (UM) requires that several TCP and User Datagram Protocol (UDP) ports be used to establish communication between servers running Exchange 2010 and other devices. By allowing access through these IP ports, you enable Unified Messaging to function correctly. This topic discusses the TCP and UDP ports used in Exchange 2010 Unified Messaging.

8.4.4.1.1 Unified Messaging Protocols and Services

Exchange 2010 Unified Messaging features and services rely on static and dynamic TCP and UDP ports to ensure correct operation of the computer running the Unified Messaging server role. When Exchange 2010 is installed, static Windows Firewall rules are added for Exchange. If you change the TCP ports that are used by the Unified Messaging server role, you may also need to reconfigure the Windows Firewall rules to allow Unified Messaging to work correctly.



Warning: On Exchange 2010 Unified Messaging servers, Exchange setup creates the **SESWorker (TCP-In)** and **SESWorker (GFW) (TCP-In)** rules which allow

inbound communication without any TCP port restrictions. We recommend you disable these two rules after you've setup the Unified Messaging server, and create a new rule to allow only the ports required for the SESWorker process which include 5065 and 5067 for TCP (unsecured), 5066 and 5068 for mutual TLS (secured). For details, see [Exchange Network Port Reference](#).

8.4.4.1.1.1 Session Initiation Protocol

Session Initiation Protocol (SIP) is a protocol used for initiating, modifying, and ending an interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality. It's one of the leading signaling protocols for Voice over IP (VoIP), together with H.323. Most VoIP standards-based solutions use either H.323 or SIP.

However, several proprietary designs and protocols also exist. These VoIP protocols typically support features such as call waiting, conference calling, and call transfer.

SIP clients such as IP gateways and IP Private Branch eXchanges (PBXs) can use TCP and UDP port 5060 to connect to SIP servers. SIP is used only for setting up and tearing down voice or video calls. All voice and video communications occur over Real-time Transport Protocol (RTP).

8.4.4.1.1.2 Real-time Transport Protocol

Real-time Transport Protocol (RTP) defines a standard packet format for delivering audio and video over a specific network, such as the Internet. RTP carries only voice/video data over the network. Call setup and teardown are generally performed by the SIP protocol.

RTP doesn't require a standard or static TCP or UDP port to communicate with. RTP communications occur on an even number UDP port, and the next higher odd number port

is used for TCP communications. Although there are no standard port range assignments, RTP is generally configured to use ports 1024 and 65535. It's difficult for RTP to traverse firewalls because it uses a dynamic port range.

8.4.4.1.1.3 Unified Messaging Web Services

The Unified Messaging Web services installed on a Client Access server use IP for network communication between a client, the Unified Messaging server, the Client Access server, and computers running other Exchange 2010 server roles. There are several Exchange 2010 Outlook Web App and Microsoft Office Outlook 2007 client features that rely on Unified Messaging Web services to operate correctly.

The following Unified Messaging client features rely on Unified Messaging Webservices:

- Voice mail options available with Exchange 2010 Outlook Web App, including the Play on Phone feature and the ability to reset a PIN.
- Play on Phone feature found in the Outlook 2007 client.



Warning: When an organization uses the Play on Phone and other client features in Exchange 2010 Unified Messaging, a computer running the Client Access, Hub Transport, and Mailbox server roles within the same Active Directory site is required in addition to the computer or computers with the Unified Messaging server role installed.

8.4.4.1.1.4 Port Assignments

The following table shows the IP ports that Unified Messaging uses for each protocol and whether the IP ports used for each protocol can be changed.

IP ports used for Unified Messaging protocols.

Table 8-36: Unified Messaging

Protocol	TCP Port	UDP Port	Can Ports be Changed?
SIP (Microsoft Exchange Unified Messaging service)	5060 (unsecured) 5061 (secured) The service listens on both ports.		Ports can be changed in the Msexchangeum.config configuration file.
SIP (UM worker process)	5065 and 5067 for TCP (unsecured). 5066 and 5068 for mutual TLS (secured)		Ports can be changed in the Msexchangeum.config configuration file.
RTP		Ports between 1024 and 65535	Ports can be changed in the Msexchangeum.config configuration file. The Msexchangeum.config file is located in the \Program Files\Microsoft\Exchange\V14\bin folder on an Exchange 2010 Unified Messaging server.
Unified Messaging Web service	443		The port is configured on the Web site that hosts the Unified Messaging virtual directory. The port can be changed using IIS Manager.

In addition, the following table provides information about port, authentication, and encryption for data paths between UM servers and other servers.

8.4.4.1.1.4.1 Unified Messaging Server Data Paths

Table 8-37: Unified Messaging

Data Path	Required Ports	Default Authentication	Supported Authentication	Encryption Supported?	Encrypted by Default?
Active Directory access	389/TCP/UDP (LDAP), 3268/TCP (LDAP GC), 88/TCP/UDP (Kerberos), 53/TCP/UDP (DNS), 135/TCP (RPC netlogon)	Kerberos	Kerberos	Yes, using Kerberos encryption	Yes
Unified Messaging Phone interaction (IP PBX/VoIP Gateway)	5060/TCP , 5065/TCP, 5067/TCP (unsecured), 5061/TCP, 5066/TCP, 5068/TCP (secured), a dynamic port from the range 16000-17000/TCP (control), dynamic UDP ports from the range 1024-65535/UDP (RTP)	By IP address	By IP address, MTLS	Yes, using SIP/TLS, SRTP	No
Unified Messaging Web Service	80/TCP, 443/TCP (SSL)	Integrated Windows authentication (Negotiate)	Basic, Digest, NTLM, Negotiate (Kerberos)	Yes, using SSL	Yes
Unified Messaging server to Client Access server	5075, 5076, 5077 (TCP)	Integrated Windows authentication (Negotiate)	Basic, Digest, NTLM, Negotiate (Kerberos)	Yes, using SSL	Yes
Unified Messaging server to Client Access server (Play on Phone)	Dynamic RPC	NTLM/Kerberos	NTLM/Kerberos	Yes, using RPC encryption	Yes

Data Path	Required Ports	Default Authentication	Supported Authentication	Encryption Supported?	Encrypted by Default?
Unified Messaging server to Hub Transport server	25/TCP (TLS)	Kerberos	Kerberos	Yes, using TLS	Yes
Unified Messaging server to Mailbox server	135/TCP (RPC)	NTLM/Kerberos	NTLM/Kerberos	Yes, using RPC encryption	Yes

This page is intentionally left blank.

9 Office 365 Integration

The section below describes the deployment of the AudioCodes CloudBond Office 365 Connector in a multi-forest model and provides information for System technicians to perform on-site installation of the AudioCodes CloudBond Server.

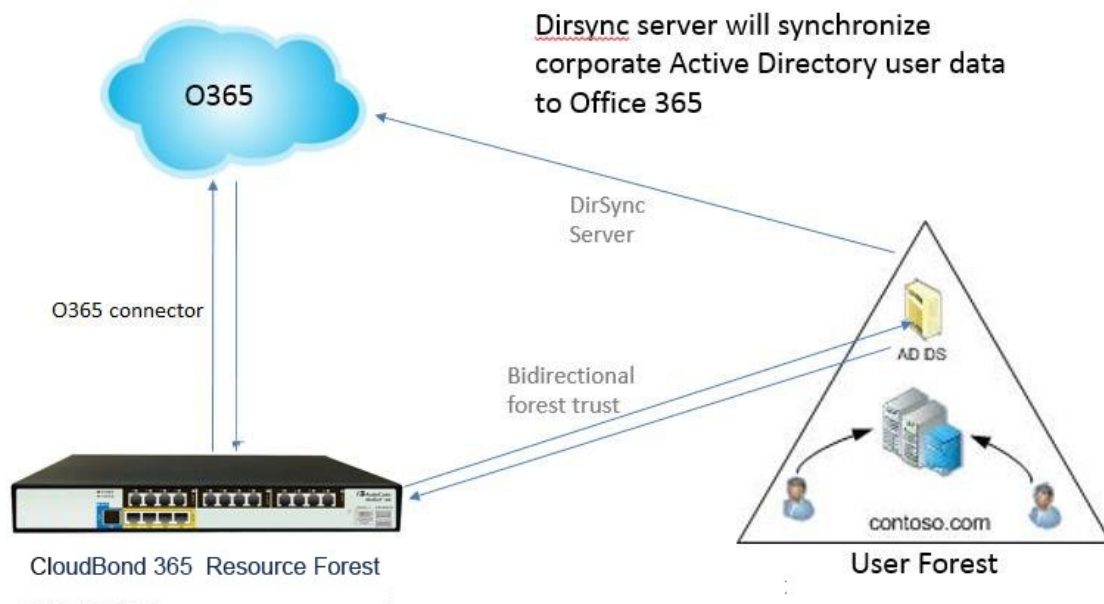
This guide provides:

- Guidelines for preparing the customer enterprise network
- AudioCodes CloudBond 365 Office 365 connector installation procedures
- Basic system and site configuration information

9.1 Overview

The figure below shows the integration of CloudBond 365 and Office 365.

Figure 9-1: CloudBond 365 and Office 365



9.1.1 What is Office 365?

Office 365 is a Software as a Service (SaaS) offering from Microsoft.

A subscription to Office 365 gives users the ability to use traditional office applications over the internet through a web browser interface.

Besides access to Word, Excel and Outlook, Office 365 can also provide access to backend office services, such as Active Directory (AD), Exchange Online, Skype for Business Online, and SharePoint Online.

Office 365 also has many other features and facilities, including download of office products, and is tightly integrated with other Microsoft offerings, such as OneDrive for online storage.

Microsoft web sites include detailed information about Office 365: <http://office.microsoft.com>.

A reasonable, non-Microsoft, overview of Office 365 can be found at http://en.wikipedia.org/wiki/Office_365.

9.1.2 Office 365 and Voice

Office 365 Skype for Business Online currently provides two ways for PSTN breakout / Enterprise Voice capabilities, being:

- Cloud PBX with PSTN Calling (only available in limited countries)
- Cloud PBX with on-premises PSTN connectivity.

In addition to a full hybrid deployment, which will be covered in Section 9.1.5.1 , CloudBond 365 can also be used in the Cloud PBX with on-premises PSTN connectivity scenario, by providing full administration capabilities for the Cloud PBX users homed in Office 365.

9.1.3 How does Skype for Business use Office 365?

A Skype for Business on-premises deployment, such as CloudBond 365, can take advantage of several features of Office 365:

- Office 365 can provide the Exchange Unified Messaging component to Skype for Business, allowing voicemail facilities, and some Automated Attendant facilities.
- Office 365 can provide the Outlook Client for Skype for Business, showing Skype for Business presence information for contacts, for calendar items, and allowing the scheduling of Conferences.
- Skype for Business Online and Skype for Business On-premises can share a SIP domain, allowing users who require limited Enterprise Voice features to be hosted entirely in the cloud, while still being part of the Skype for Business environment.



Note: You cannot have a split UM in cloud and Exchange mailbox on premise, or vice versa. If you do have Exchange On-premises, and also Office 365 Exchange Online, then a specific users Exchange mailbox must be wholly within the cloud, or wholly within the on-premises server.

For more information about Exchange Hybrid deployments, see: <https://technet.microsoft.com/en-us/library/jj200581%28v=exchg.150%29.aspx>. For more information about Skype for Business Hybrid deployments, see: <http://technet.microsoft.com/en-us/library/jj204805.aspx>.

9.1.4 What is Skype for Business Federation?

Skype for Business Federation allows Microsoft Skype for Business users to communicate with other Skype for Business users outside their organization. When enabled, federation allows you to add users from other organizations to your Contacts list, send instant messages to your federated contacts, invite contacts to audio calls, video calls, or conferences, and exchange presence information.

Skype for Business Federation is performed over the Internet through the Skype for Business Edge server of each organization. Skype for Business external connectivity requires the consent and correct configuration of both parties of the Federation relationship. After the federation is set up by the administrators of both sides, Skype for Business users in each company can see presence and communicate with users in the other company.

Skype for Business on-premises deployments can also federate with Skype for Business Online deployments. For example, Skype for Business Federation allows users in your on-premises deployment to communicate with Office 365 users in your organization.

Skype for Business Federation includes various inbuilt security mechanisms. Federation can be open (connect to anyone) or closed (connect to only allowed domains), and also includes block lists. User information can be limited to users buddy lists, or available to anyone, etc.

9.1.5 Domain Names and Shared Name Spaces

When you first subscribe to Office 365, you can create a Domain name in the format xxxxx.onmicrosoft.com (e.g., contoso.onmicrosoft.com).

Whilst you can use this domain name for all further Office 365 activity, it is more common to add your own domain name to Office 365 i.e., contoso.com. These are referred to as vanity domain names in some documentation. Microsoft will verify that you have the appropriate ownership of such a domain before adding it.

As these domain names can then be used for Office 365 sign-on, email addresses, and Skype for Business Online SIP domains, it is recommended you configure these before replicating users to Office 365.

See the following link for more details:

http://office.microsoft.com/en-au/Office_365-suite-help/work-with-domain-names-in-office-365-HA102818560.aspx

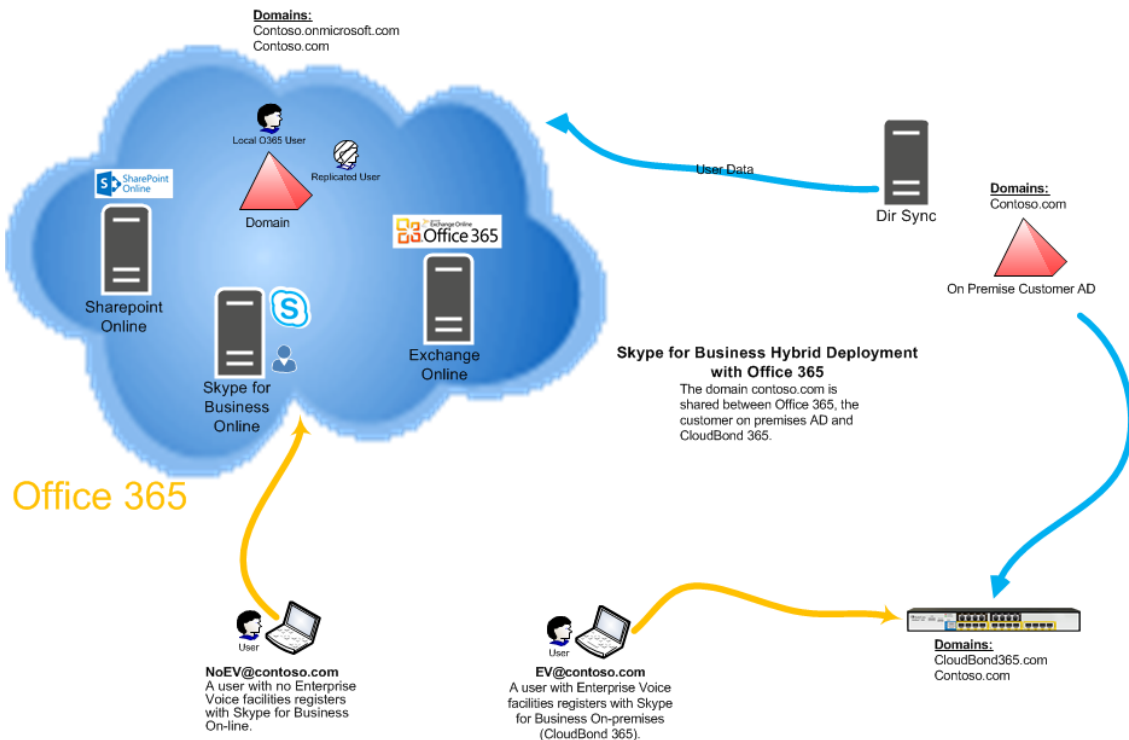
9.1.5.1 Skype for Business Hybrid Deployment

A Skype for Business Hybrid Deployment allows Skype for Business online and Skype for Business on-premises to co-exist. The two environments share the same SIP domain space in what is known as a split domain.

In a Skype for Business Hybrid deployment:

- Skype for Business Online users can use most Skype for Business features, such as presence, IM, and limited voice calls.
- Skype for Business On-premises users can enjoy all the same features as Skype for Business Online users, with the addition of full Enterprise Voice features.
<https://technet.microsoft.com/en-us/library/jj205403.aspx>.

Figure 9-2: CloudBond 365 Skype for Business Hybrid Deployment



With CloudBond 365, a user can be switched from Skype for Business online to Skype for Business on premises simply by changing their assigned FE Registrar pool in the SysAdmin web pages.

9.1.6 Replicating Users

Whilst Office 365 and CloudBond 365 users can be administered completely independently, significant benefits can be achieved by replicating users from one directory system to the other.

Azure Active Directory Sync Services (a.k.a. DirSync) is a Microsoft tool that allows the replication of users from an on-premises Active Directory deployment to the Office 365 Azure Active Directory. This means that the process of user administration can be simplified by automatically replicating user data.

There are multiple deployment options now available within DirSync, including selective replication, and replication with password hashes. DirSync can also be deployed with Active Directory Federation Services (ADFS) to provide even more features.

Some good background information on DirSync is available at the following links:
<http://blogs.office.com/2014/04/15/synchronizing-your-directory-with-office-365-is-easy/>
<https://blogs.office.com/2013/07/26/password-hash-sync-simplifies-user-management-for-office-365/>

9.1.6.1 DirSync

Deploying DirSync following Microsoft best practice requires a separate, Windows 2008 or 2012, domain member, and server. This server must either be located On-premises with the existing Active Directory (AD) server, or could be deployed in the cloud using Microsoft Azure.

DirSync server requirements: <http://technet.microsoft.com/en-us/library/jj151831.aspx> DirSync on Azure:

<http://technet.microsoft.com/en-us/library/dn635310%28v=office.15%29.aspx>

The DirSync server, once configured, will automatically replicate user information from the on-premises AD, to the Office 365 AD, making those user details available to Office 365.



Note: This replication is one-way. Changes or new accounts created in Office 365 are not replicated back to the on-premises AD by DirSync.

A recently added option within DirSync allows hashed passwords to also be synchronized from on-premises AD to Office 365 AD. This is the recommended configuration. When this option selected, a user may sign in to Office 365 and on-premises applications, such as Skype for Business, using the same user id and password. With the October 2015 release of DirSync, now named AADConnect, there is also full support for resource forest environments, bypassing the need to extend the enterprise user forest(s) with the Skype for Business schema extensions.



Note: This is not a Single sign-on system. A user logging in will still be prompted for a User ID and password in Office 365, even if the user is already signed in to the On-premises network.

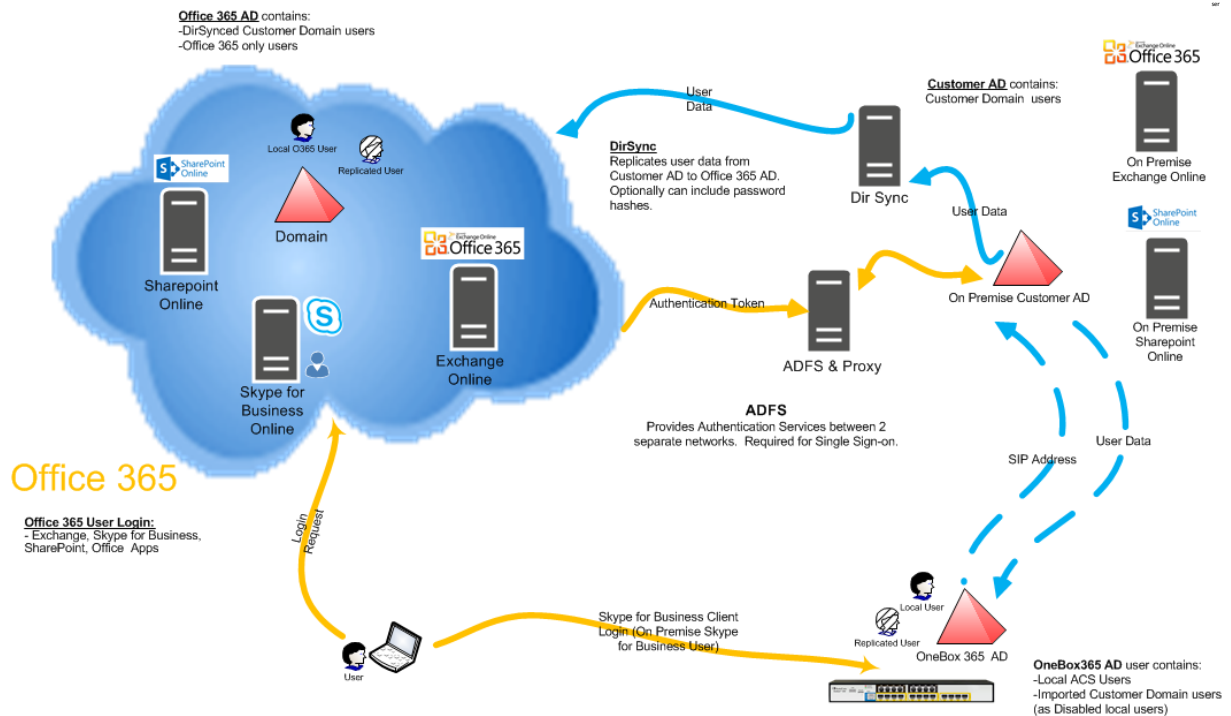
9.1.7 Active Directory Federation Services

Active Directory Federation Services (ADFS) provides, amongst other features, the capability of single sign on between two separate networks, including Office 365 and the on-premises AD. It essentially brings control of the sign on authentication process back to the on-premises environment.

A user signed on to the on-premises AD will be automatically signed in to the Office 365 environment.

ADFS is optional, and requires significant extra configuration.

Figure 9-3: ADFS Single Sign On



9.2 Pre-Requisites

The paragraphs below describe the prerequisites for a Skype for Business Server hybrid deployment.

9.2.1 Infrastructure Prerequisites

You must have the following available in your environment to implement and configure a Skype for Business Server 2015/Lync Server 2013 hybrid deployment:

- An Office 365 tenant with Skype for Business Online enabled.
- Optionally, if you want to support Single Sign-on with Office 365, an Active Directory Federation Services (AD FS) Server either on-premises or using Microsoft Azure. For more information about AD FS, see [Active Directory Federation Services \(AD FS\) 2.0](#), or [Configure Active Directory Federation Services for Windows Azure Pack](#).
- An on-premises deployment of Skype for Business Server 2015 or Lync Server 2013 with Cumulative Updates: March 2013 or later applied.
- Skype for Business Server 2015/Lync Server 2013 administrative tools.
- Directory Synchronization. For details about Directory Synchronization, see [Hybrid Identity Management](#).

Full details can be found at <https://technet.microsoft.com/en-us/library/jj205386.aspx>

9.2.2 Install DirSync

The Directory Synchronization tool will synchronize the customer's users from the local forest towards Office 365, where they can be licensed and enabled for Skype for Business Online using the Office 365 management portal. Only users "Synced with Active Directory" will work in a hybrid model.

Figure 9-4: Office 365 Users

Display name	User name	Status
ACS VPN Trust	acs@OCSHOST.onmicrosoft.com	Synced with Active Directory
acs replicate	acsreplicate@OCSHOST.onmicrosoft.com	Synced with Active Directory
ADFSSvcAcct	ADFSSvcAcct@activecommunications.eu	Synced with Active Directory

"In Cloud" users (those users created directly in Office 365) do not support hybrid deployments and should be mapped to on premise Active Directory users first, by following the steps in the following blog article for example: <http://blogs.4ward.it/how-to-map-onprem-active-directory-users-to-existing-office365-users/>

Following Microsoft best practice, DirSync should be installed on a member server of the domain from which you wish to replicate users. You will need to provide this server, as it is not included with CloudBond 365.

http://technet.microsoft.com/en-us/library/jj151800.aspx#BKMK_InstallDirSyncTool

The Setup Wizard will offer you the chance to run the Configuration Wizard after install completes.

The configuration wizard will prompt you to "Synchronize your directories now".

9.2.3 Ensure DirSync is Functioning

Make sure DirSync is deployed and all users have been replicated through DirSync and are present in Office 365.

Figure 9-5: DirSync Working

Display name	User name	Status
<input type="checkbox"/> ACS VPN Trust	acs@OCSHOST.onmicrosoft.com	Synced with Active Directory
<input type="checkbox"/> acs replicate	acsreplicate@OCSHOST.onmicrosoft.com	Synced with Active Directory
<input type="checkbox"/> ADFSsvcAcct	ADFSSvcAcct@activecommunications.eu	Synced with Active Directory

9.2.4 Deploy Skype for Business Schema Attributes

As the hybrid model with Office 365 relies on directory synchronization with the users Active Directory forest, it is required to prepare the user forest with the Skype for Business Schema Attributes when older DirSync applications then AADConnect are installed. The Active Directory schema can be prepared either through the Skype for Business wizard or by using LDIF as described below:

Prepare the user forest with the Skype for Business Schema Attributes (through the Skype for Business wizard or LDIF as below) (<http://technet.microsoft.com/en-us/library/gg398607.aspx>) :

The **Prepare Schema** step in the Skype for Business Server Deployment Wizard and the **Install-CsAdServerSchema** cmdlet, extend the Active Directory schema on domain controllers running a 64-bit operating system. If you need to extend the Active Directory schema on a domain controller running a 32-bit operating system, you can run the **Install-CsAdServerSchema** cmdlet remotely from a member server (recommended approach). If you need to run schema preparation directly on the domain controller, however, you can use the Ldifde.exe tool to import the schema files. The Ldifde.exe tool comes with most versions of the Windows operating system.

9.2.4.1 Using LDIFDE

If you use Ldifde.exe to import the schema files, you must import all four files, regardless of whether you are migrating from a previous version or performing a clean installation. You must import them in the following sequence:

1. ExternalSchema.ldf
2. ServerSchema.ldf
3. BackCompatSchema.ldf
4. VersionSchema.ldf



Note: The four .ldf files are located in Skype RTM\Support\Schema directory of your installation media or download.

To use Ldifde.exe to import the four schema files on a domain controller that is the schema master, use the following format:

[Copy](#)

```
ldifde -i -v -k -s <DCName> -f <Schema filename> -c DC=X  
<defaultNamingContext> -j logFilePath -b <administrator account>  
<logon domain> <password>
```

For example:

[Copy](#)

```
ldifde -i -v -k -s DC1 -f ServerSchema.ldf -c DC=X  
"DC=contoso,DC=com" -j C:\BatchImportLogFile -b Administrator  
contoso password
```



Note: Use the *b* parameter only if you are logged in as a different user. For details about the required user rights, see the "Administrator Rights and Roles" section earlier in this topic.

To use Ldifde.exe to import the four schema files on a domain controller that is not the schema master, use the following format:

[Copy](#)

```
ldifde -i -v -k -s <SchemaMasterFQDN> -f <Schema filename> -c DC=X  
<rootDomainNamingContext> -j logFilePath -b <administrator account>  
<domain> <password>
```

For details about using Ldifde, see Microsoft Knowledge Base article 237677, "Using LDIFDE to import and export directory objects to Active Directory," at <http://go.microsoft.com/fwlink/p/?linkId=132204>.

9.2.5 Deploy CloudBond 365

If you have not already done so, you should now install and deploy the CloudBond 365 system. Connect CloudBond 365 and set up the trust by following instruction in Section 8 page on page 67.

9.2.6 Prepare the User Forest Active Directory for Write Access

Prepare the User Forest Active Directory for write access from the Resource forest (CloudBond) administrator account.

The easiest configuration is to use the cloudbond365\administrator account as the user-id to perform updates to the User forest. If you wish to use a different account, see Section 15.11.

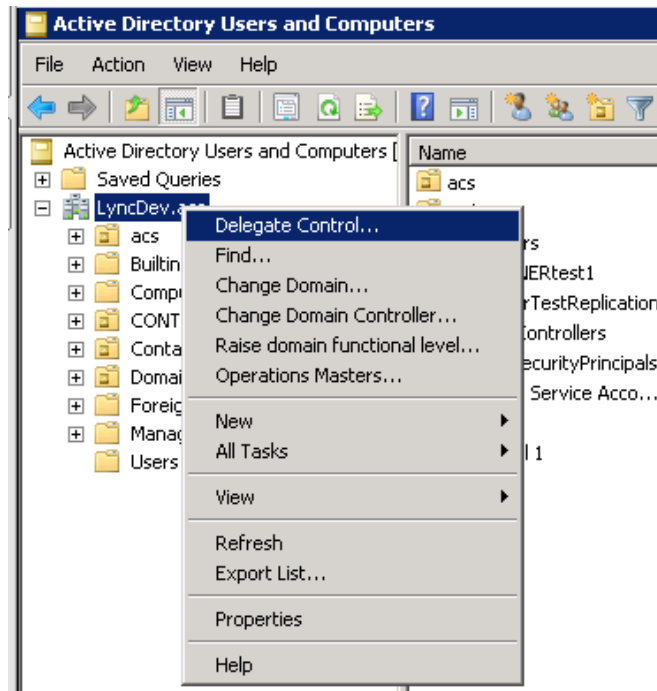
In the screenshots below:

- CloudBond 365 Administrator is OCSHOST\Administrator instead of AC-CloudBond\Administrator
- Customer corporate Domain is LyncDev.acs

➤ To prepare the User Forest Active Directory for Write Access:

1. On the Customer Corporate DC, open the Active Directory Users and Computers tool.
2. Right-click on the top level domain, and select **Delegate Control**.

Figure 9-6: Delegate Control

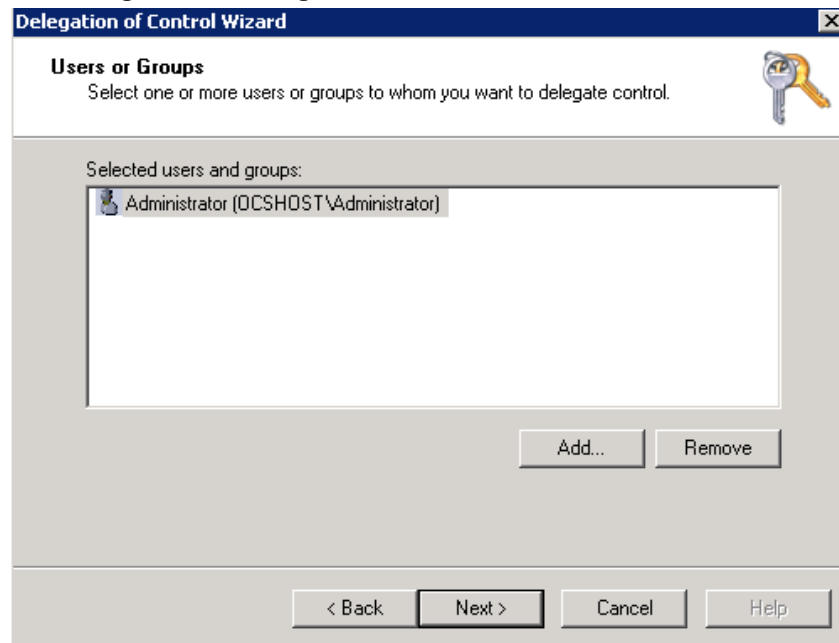


3. Click **Next**.

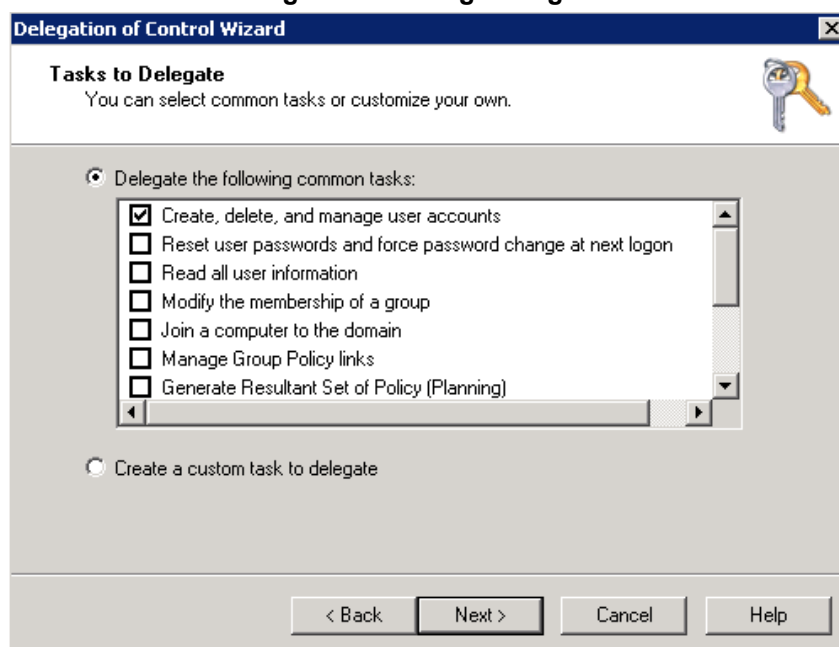
Figure 9-7: Delegate Control Wizard



4. Click **Next**.

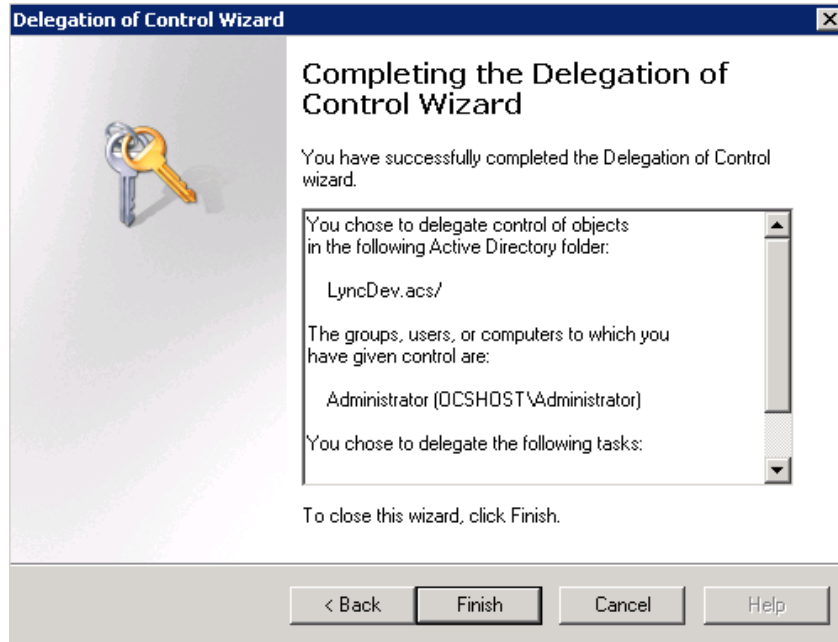
Figure 9-8: Delegate to CloudBond 365 Administrator

5. Select the 'Create, delete, and manage user accounts' check box, and then click **Next**.

Figure 9-9: Delegate Rights

6. Click **Finish**.

Figure 9-10: Complete the Wizard



Note: Administrator accounts within the Organizational Unit (OU) will not follow the delegation. Microsoft best practice is not to use administrator accounts for regular use. If an Administrator account needs to be enabled, the security settings need to be applied using DSACLs on the AdminSDHolder container.



For more information on using DSACLs see :

[https://technet.microsoft.com/en-us/library/cc772662\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772662(v=ws.10).aspx)

An example PowerShell script that can be used to set the minimum permissions using DSACLs can be found in Appendix [A](#).

9.3 Configuring Office 365 Integration

The paragraphs below describe Office 365 integration.

9.3.1 Prepare CloudBond 365 for Skype for Business Hybrid and Exchange UM

To enable a Skype for Business hybrid deployment, follow the instructions below. You can also use the following TechNet article as a guide.

<http://technet.microsoft.com/en-us/library/dn689117.aspx>

These instructions will:

- Enable shared address space in Office 365
- Allow Federation in CloudBond 365
- Create a Hosting Provider for Office 365 in CloudBond 365
- Perform initial replication
- Change users in the Corporate AD so they replicate to Office 365 correctly
- Update some DNS records to direct all SIP traffic to CloudBond 365

9.3.1.1 Start a Skype for Business Online PowerShell Session

On the CloudBond 365 Controller, open the Skype for Business Management Shell, then enter the following commands (this assumes the Controller has internet access. If not, use PowerShell on a workstation that does have internet access).

```
Import-Module SkypeOnlineConnector
$cred = Get-Credential
$CSSession = New-CsOnlineSession -Credential $cred
Import-PSSession $CSSession -AllowClobber
```

For more information about how to establish a remote PowerShell session with Skype for Business Online, see [Connecting to Skype for Business Online by using Windows PowerShell](#).

For more information about using the Skype for Business Online PowerShell module, see [Using Windows PowerShell to manage Skype for Business Online](#).



Note: You may need to update the Skype for Business Online PowerShell Module as Microsoft frequently updates Office 365. Check Microsoft for the latest version, or, you may also apply the latest Skype for Business Cumulative Update. See: <http://www.microsoft.com/en-us/download/details.aspx?id=39366>
<https://support.microsoft.com/en-us/kb/2809243>

9.3.1.2 Configuring Shared SIP Address Space

Your Skype for Business Online must be configured for Shared SIP Address Space. To do this, first start a remote PowerShell session with Skype for Business Online. Then run the following cmdlet:

```
Set-CsTenantFederationConfiguration -SharedSipAddressSpace $True
```

9.3.1.3 Allowing Federation

In your On-premises deployment, in Skype for Business Server Management Shell, type the following cmdlet to allow federation:

```
Set-CSAccessEdgeConfiguration -AllowOutsideUsers $true
```

```
-AllowFederatedUsers $true -UseDnsSrvRouting -
EnablePartnerDiscovery $true
```

9.3.1.4 Removing Existing Hosting Provider

On your On-premises deployment, in the Skype for Business Server Management Shell, type the following cmdlet to remove the existing Hosting Provider for Skype for Business Online:

```
Get-CsHostingProvider | where ProxyFqdn -eq
"sipfed.online.lync.com" | Remove-CsHostingProvider
```

9.3.1.5 Creating a Hosting Provider for Skype for Business Online

On your on-premises deployment, in Skype for Business Server Management Shell, type the following cmdlet to create the hosting provider for Skype for Business Online:

```
New-CSHostingProvider -Identity LyncOnline -ProxyFqdn
"sipfed.online.lync.com" -Enabled $true -EnabledSharedAddressSpace
$true
-HostsOCSUsers $true -VerificationLevel UseSourceVerification -
IsLocal $false
-AutodiscoverUrl
https://webdir.online.lync.com/Autodiscover/AutodiscoverService.svc/r
oot
```

9.3.2 Obtaining the Customer Specific Office 365 Information

Obtain the customer specific Office 365 information, to be saved in Office 365 Configuration under System Configuration in the CloudBond management suite (SysAdmin web pages). See AudioCodes CloudBond 365 Administrator Guide.

- User Name:
 - The login name of your Office 365 Administrator
- Host:
 - The location where your Office 365 environment is hosted
- Migration Override URL:
 - Explained further in this document
- Override Admin Domain:
 - Your original Office 365 domain prior to applying vanity domain names
- Password:
 - The Office 365 Administrator password

Figure 9-11: CloudBond - Office 365 Connector Information

The screenshot shows the 'Office 365 Settings' configuration page in the CloudBond interface. At the top, there is a dark blue header with two tabs: 'SYSTEM CONFIGURATION' (highlighted in light blue) and 'ABOUT'. Below the header is a light blue horizontal bar. The main content area is white and contains the 'Office 365 Settings' section. This section includes several input fields for configuration: 'User Name' (containing 'admin@ocshost.emea.microsoftonline.com'), 'Host' (containing 'sipfed.online.lync.com'), 'MigrationOverrideUrl' (containing 'https://admin0e.online.lync.com/HostedMigration/hostedmigration.service.svc'), and 'OverrideAdminDomain' (containing 'ocshost.onmicrosoft.com'). There are also two password fields labeled 'Password:' and 'Confirm password:', both containing masked characters (dots). At the bottom of the form is a blue 'Apply' button.

Office 365 Settings

User Name:
admin@ocshost.emea.microsoftonline.com

Host:
sipfed.online.lync.com

MigrationOverrideUrl:
https://admin0e.online.lync.com/HostedMigration/hostedmigration.service.svc

OverrideAdminDomain:
ocshost.onmicrosoft.com

Password:

Confirm password:

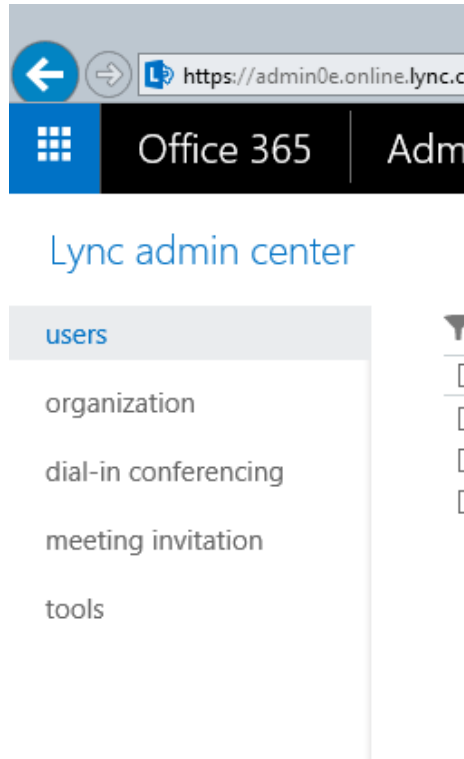
Apply

9.3.2.1 Determining Hosted Migration Service Override URL

- To determine the Hosted Migration Service Override URL for your Office 365 tenant:

 1. Log in to your Office 365 tenant as an administrator.
 2. Open the Skype for Business admin center.

Figure 9-12: Office 365 Skype for Business Admin Center



3. Ensure that the **Skype for Business admin center** is displayed, then select and copy the URL in the address bar up to **.com**. An example URL looks similar to the following: <https://webdir0e.online.lync.com/lscp/?language=en-US&tenantID=>
Replace "webdir" in the URL with "admin", resulting in the following:
<https://admin0e.online.Lync.com>
4. Append the following string to the URL:
</HostedMigration/hostedmigrationservice.svc>
5. The resulting URL, which is the value of the **HostedMigrationOverrideUrl**, should look like the following:
<https://admin0e.online.lync.com/HostedMigration/hostedmigrationservice.svc>

9.3.2.2 Determining Override Admin Domain

The Override Admin Domain is usually the default signup domain "something.onmicrosoft.com". Your Office 365 Administrator can supply this value.

9.3.3 Using Exchange Online for Voicemail

This section describes how to use Exchange Online for Voicemail.

9.3.3.1 Preparing Office 365 For Unified Messaging

To enable Office 365 Unified Messaging you need to first create a dial plan in Exchange Online to enable users to access their mailbox for configuration and message retrieval. Further information about Dial Plans can be found here:

<http://technet.microsoft.com/en-us/library/bb125151%28v=exchg.150%29.aspx>

Section 9.6 shows an example of creating a UM Dial Plan for Exchange Online.

Once the dial plan is created, you can enable the Office 365 users for Unified Messaging. Detailed information can be found at [https://technet.microsoft.com/en-us/library/jj673527\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj673527(v=exchg.150).aspx).

Next, you need to connect to Office 365 using Exchange Online PowerShell and run the following Cmdlet:

```
Set-UMmailboxpolicy -identity "Policy Name in O365" -  
SourceForestPolicy "ACS-O365UM"
```

Then finally on your on premise Exchange 2010 SP3 server (Note this is only if Unified Messaging is already configured on premise so that when you migrate a UM mailbox it doesn't fail otherwise if you don't run this step the remote move request will fail)

```
Set-UMmailboxpolicy -identity "On Premise UM Policy" -  
SourceForestPolicy "Policy Name in O365"
```

9.3.3.2 Allowing Users to Dial-in to Access Exchange Online Voicemail

CloudBond 365 provides native integration to Office 365 Unified Messaging by means of an intuitive interface. Once the pre-requisites as outlined in the earlier chapters are configured, there is no further need for PowerShell cmdlets and administration can be performed using the System Configuration pages.

➤ **To enable the Office 365 UM feature:**

1. Under the **System Configuration** group, select the **Office 365 Unified Messaging & Cloud PBX Policies** option.
2. Select the **Enable Office 365 UM** checkbox.
3. Select a registrar pool and SIP domain and specify the telephone number to be used.

Figure 9-13: Office 365 UM

The screenshot shows the 'SYSTEM CONFIGURATION' page in the CloudBond 365 interface. The left sidebar lists various configuration options, with 'Office365 Unified Messaging & CloudPBX Policies' highlighted. The main content area is titled 'CloudPBX VoiceRoutingPolicies Management'. It contains two tables: 'Voice Routing Policies' and 'PSTN Usage Records'. Below these tables is a section for 'Office365 UM' settings, which is highlighted with a red box. This section includes a checkbox for 'Enable Office365 UM', a dropdown for 'RegistrarPool' (set to 'UC-FE.cloudbond365.com'), a dropdown for 'sipDomain' (set to 'cloudbond365.com'), and a text field for 'Displaynum*' (set to '+31365461223'). There are also 'Save VRP/PstnUsages settings' and 'Save Office365 UM settings' buttons.

- Once enabled, users can be assigned Office 365 UM on the user edit page by enabling the Office 365 Exchange UM policy checkbox.

Figure 9-14: Office 365 Exchange UM Policy

The screenshot shows the 'Edit Account' page in the CloudBond 365 interface. The left sidebar lists user management options. The main content area is titled 'Account Information' and contains fields for user details. Below this is a section for 'Policies', which is highlighted with a red box. This section includes a 'Voice Policy' dropdown and a checkbox for 'Office365 Exchange UMPolicy', which is checked. There are also checkboxes for various features like 'Enable call Forward', 'Enable Delegation', 'Enable Call Transfer', 'Enable team call', 'Enable call park', and 'Enable simultaneous ringing of phones'.

9.4 Initial Replication

An initial replication cycle needs to be run for CloudBond 365 resource forest to retrieve all Skype for Business enabled users from the Office 365 environment.

Once the Office 365 Skype for Business enabled users are replicated to the CloudBond 365 resource forest, they are mapped to the original User accounts homed in one of the customer forests that CloudBond 365 has a trust with by the objectGUID attribute, which is a standard unique object identifier in Office 365 directory synchronization. If mapping to the standard objectGUID fails, the CloudBond 365 Office 365 connector will try to map the Office 365 Skype for Business user against the user's msDS-ConsistencyGuid attribute, as described in Paul Williams' blog article: <http://blog.msresource.net/2014/03/10/windows-azure-active-directory-connector-part-3-immutable-id/>, to support more complex and custom build environments as well.

When replication and user mapping has finished (these two tasks are run as a single process), the users Active Directory forest needs to be updated with the Skype for Business Online attributes.

On completion, check one of the user objects in the customer Active Directory forest that is enabled for Skype for Business Online for the presence of values in the user attributes. If the AcsUserReplication task succeeded in writing the values back into the user forest, you can continue with the final step in the replication cycle, being a manual directory synchronization cycle with Office 365.

There are several components to the user replication process:

- On the CloudBond 365 Controller, there is a scheduled task which runs o365sync –s O365. This will take account information from Skype for Business Online to CloudBond 365, and perform the mapping to original user accounts.
- There is another scheduled task on the CloudBond 365 Controller which runs ACSUserReplication. This will replicate the msRTCSIP attributes from CloudBond 365 to the customer AD.
- Finally, DirSync will replicate information from the customer AD to Skype for Business Online.

Before users can be moved between Skype for Business Online and CloudBond 365, all three replication steps must be completed.

1. Start the initial replication for all Office 365 users through:

```
C:\acs\OFFICE365Sync\SysAdmin.O365.Sync.exe -S O365
```

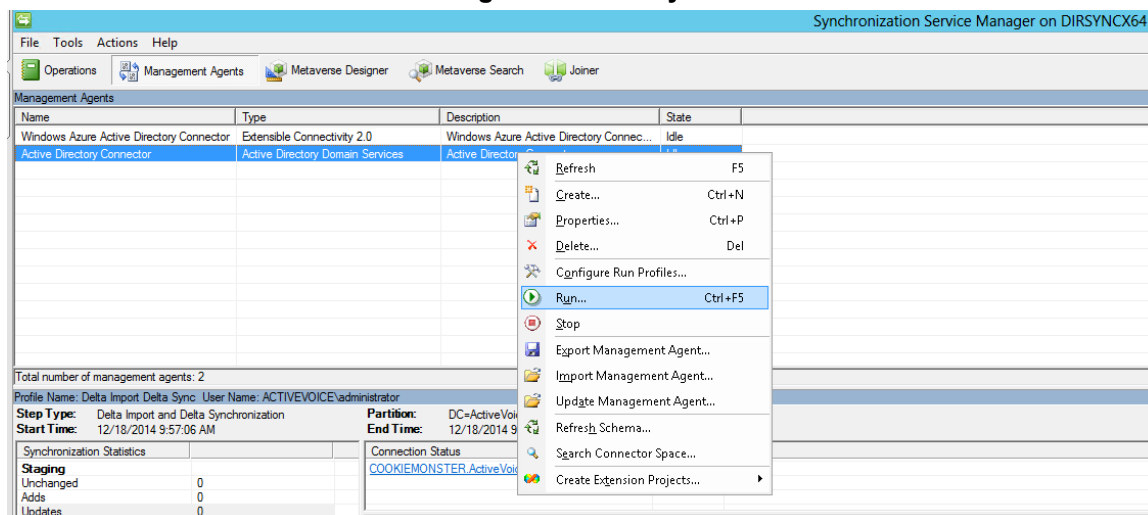
2. Match the objects with the user forest through:

```
C:\acs\AcsUserReplication\AcsUserReplication.exe
```

3. Perform a manual DirSync replication cycle on the DirSync server through:

```
C:\Program Files\Windows Azure Active Directory  
Sync\SYNCBUS\Synchronization Service\UIShell\miisclient.exe
```

Figure 9-15: DirSync



The manual DirSync operation should be completed in the following order:

1. Active Directory Connector Delta Import Delta Sync
2. Windows Azure Active Directory Connector Delta Import Delta Sync
3. Windows Azure Active Directory Connector Export

9.4.1 After Initial Replication

Once the initial replication cycle has been performed, the environment is ready for the production stage. This step requires the public DNS records to be changed, where the specific Skype for Business SRV and A records need to point to the on premise Edge server instead of to the Office 365 environment. From now on all users will register against the local Edge environment and eventually be redirected to Office 365 if their Skype for Business account is still homed there.

9.4.1.1 Update DNS Records

Update appropriate DNS records to direct all SIP traffic to Skype for Business on-premises:

- Update the **lyncdiscover.contoso.com** A record to point to the FQDN of the on-premises reverse proxy server.
- Update the **_sip._tls.contoso.com** SRV record to resolve to the public IP or VIP address of the Access Edge service of Skype for Business on-premises.
- Update the **_sipfederationtls._tcp.contoso.com** SRV record to resolve to the public IP or VIP address of the Access Edge service of Skype for Business on-premises.
- If your organization uses split DNS (sometimes called “split-brain DNS”), make sure that users resolving names through the internal DNS zone are directed to the Front End Pool.

9.4.1.2 Assigning User Registrar Pool

After initial replication, all systems will be synchronized, including the correct Skype for Business Registrar (home system). Users can now be moved back and forth from Office 365 to CloudBond 365 by using the User Management Edit page.

Assigning the Registrar Pool in the Edit User page assigns a user to that Front-End pool as their home system.

Figure 9-16: User List

Status	Full Name	Call Forward
Offline	fsdfsdf fsdfsdf	n/a
Unavailable	Xerox Workcentre M123	Unavailable
Unavailable	LyncDev 1228	Unavailable
Unavailable	analog 151028	Unavailable
Unavailable	Vergaderzaal	Unavailable
Offline	AA Dummy User	...
Offline	Alex Champness	n/a
Offline	Administrator	n/a
Offline	Adrian Radu Iovescu	Off...
Offline	alert service	n/a

Assign a destination Frontend pool:

Figure 9-17: Editing a User Registrar Pool

Account Information

Account type: Enterprise; Remote account: ACTIVEVOICE\O365HV (Office 365)
MARKED FOR REPLICATION Cancel Replication

First Name*: Hybrid

Last Name*: Voice

Sign-in Name*: O365HV

Registrar Pool: Office 365

Fax:

Note that the change to a user's Registrar Pool will be cached, and performed later by several back round scheduled tasks. It may take some time for all tasks to complete.

Though the screenshots show a move from Skype for Business online to Skype for Business on premise, the opposite direction is obviously also possible. For this to happen, Office 365 should be selected as the destination Registrar Pool.

After the move is performed, the Skype for Business online address book environment needs to be updated for which a full replication cycle is needed again.

As both the ACSUserReplication and Office 365 Directory Synchronization tasks run in a scheduled interval though, there is no need to perform a manual action, unless you would like to force replication to happen.

9.5 Ongoing Replication

There are a series of scheduled tasks which will keep all servers synchronized with each other on an ongoing basis.

You may need to adjust the frequency of such tasks to meet your requirements.

- A Scheduled task occurs at a regular interval (once every 24 hours) The task will retrieve all information from Office 365 to CloudBond 365.

```
C:\acs\O365Sync\SysAdmin.O365.Sync.exe -S O365
```

- A Scheduled task occurs at a regular interval (once every 15 minutes) The task will update all user Registrar information.

```
C:\acs\O365Sync\SysAdmin.O365.Sync.exe
```

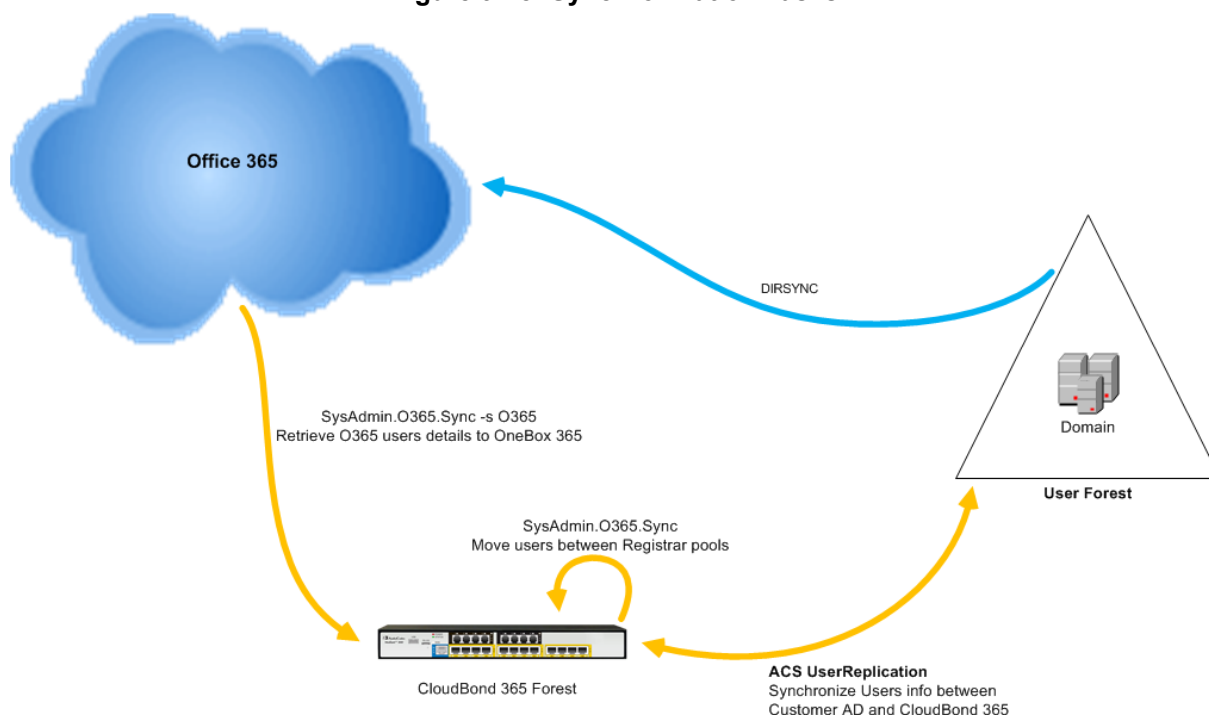
- A Scheduled task occurs at a regular interval (daily)

The task will synchronize all Skype for Business and Active Directory information between CloudBond 365, and the customer Active Directory.

```
C:\acs\O365Sync\ACSUserReplication.exe
```

- Scheduled tasks (DirSync) occurs at regular intervals to replicate all Active Directory information from the customer Active Directory to Office 365.

Figure 9-18: Synchronization Tasks



Warning: If multiple management servers are installed for redundancy, the scheduled tasks on the redundant servers should be disabled and enabled only if the primary server goes down, thereby preventing stale objects from being created in the Active Directory.

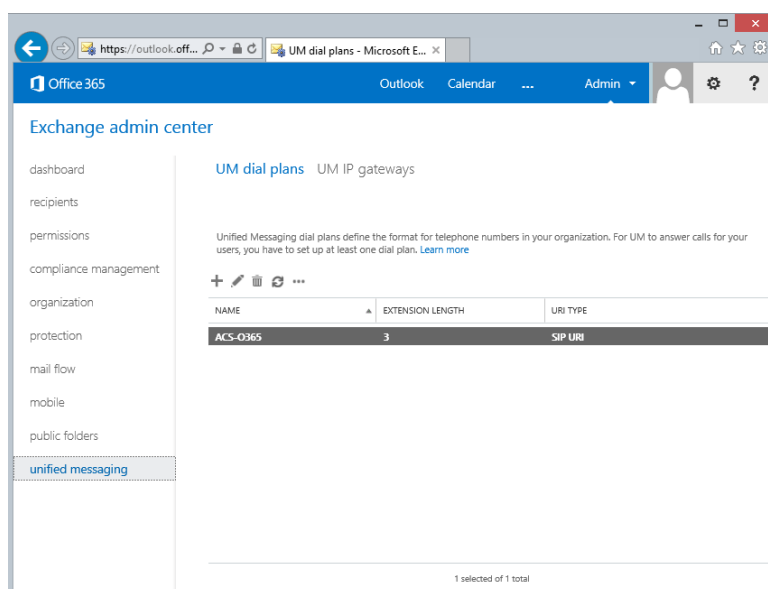
9.6 Adding a Dial Plan to Exchange Online

The procedures below describe how to add a Dial Plan to Exchange Online.

➤ **To add a Dial Plan to Exchange Online:**

1. Log into the Office 365 Wave 15 tenant using a Web browser and your Office 365 Administrator account.
2. In the Exchange admin center, under Unified Messaging, you can view and edit any existing UM dial plans, or create new dial plans as needed.

Figure 9-19: Exchange Online - UM Dial Plans



3. Navigate to **Unified Messaging > UM Dial Plans > New**.

Figure 9-20: New Dial Plan

new UM dial plan

Use UM dial plans to manage the UM features for a group of users who are enabled for voice mail.
[Learn more](#)

*Name:

*Extension length (digits):

*Dial plan type:

*Audio language:

*Country/Region code:

i After you click Save, select this dial plan and click Edit to configure dial codes, Outlook Voice Access, voice mail settings, and dialing rules.

4. After saving the dial plan, select the **Dial Plan > Configure**. For this you should try and match the company's on premise configuration. Below is an example:

Figure 9-21: Edit the Dial Plan

BF Voicemail

general

dial codes

Outlook Voice Access

settings

dialing rules

dialing authorization

transfer & search

UM dial plans are groups of users who are enabled for UM. They share common settings for greetings, prompts, audio language, and dialing codes for incoming and outgoing calls.

Name:	BF Voicemail
Extension length (digits):	4
Dial plan type:	SIP URI
Audio language:	English (United Kingdom)

Figure 9-22: Dial Codes

Voicemail Dial Plan

general
▶ **dial codes**
Outlook Voice Access
settings
dialing rules
dialing authorization
transfer & search

Set the outside line access code, country/region code, and other dial codes for users in this dial plan.

Dial codes for outgoing calls

Outside line access code:

International access code:

National number prefix:

*Country/Region code:

Number formats for dialing between dial plans

Country/Region number format:

International number format:

Number formats for incoming calls within the same dial plan:

✎ —

+

Figure 9-23: Voice Access

Voicemail

general
dial codes
▶ **Outlook Voice Access**
settings
dialing rules
dialing authorization
transfer & search

Add greetings and access numbers for Outlook Voice Access.

Welcome greeting:
Default greeting

change

Informational announcement:
<None>

change

☐ Allow announcement to be interrupted

E.164 routing numbers for your SIP server:

✎ —

+

+4420 [redacted]

Outlook Voice Access numbers:

✎ —

+

+4420 [redacted]

Figure 9-24: Settings

Voicemail Dial Plan

- general
- dial codes
- Outlook Voice Access
- settings
- dialing rules
- dialing authorization
- transfer & search

Use this section to set the options available for users of this UM dial plan.

Primary way to search for names:

Secondary way to search for names:

Audio codec:

Operator extension:

*Number of sign-in failures before disconnecting:

Timeouts and retries:

*Maximum call duration (minutes):

*Maximum recording duration (minutes):

*Recording idle time out (seconds):

*Number of input failures before disconnecting:

Audio language:

Figure 9-25: Dialing Rules

Voicemail Dial Plan

- general
- dial codes
- Outlook Voice Access
- settings
- dialing rules
- dialing authorization
- transfer & search

Specify dialing rules to control the types of calls users can make. For rules to take effect, authorize them in the dial plan, UM mailbox policies, and UM auto attendants.

In-country/region dialing rules:

+ -

GROUP NAME	NUMBER PATTERN	DIALED NUMBER
All Extensions	*	*

International dialing rules:

+ -

GROUP NAME	NUMBER PATTERN	DIALED NUMBER
------------	----------------	---------------

Figure 9-26: Dialing Authorizations

Voicemail Dial Plan

general
dial codes
Outlook Voice Access
settings
dialing rules
▶ **dialing authorization**
transfer & search

Select the types of calls to authorize for users of this UM dial plan.

☒ Calls in the same UM dial plan
☒ Allow calls to any extension

Authorized in-country/region dialing rule groups:

+ -

NAME
All Extensions

Authorized international dialing rule groups:

+ -

NAME

Figure 9-27: Transfer and Search

Voicemail Dial Plan

general
dial codes
Outlook Voice Access
settings
dialing rules
dialing authorization
▶ **transfer & search**

Specify how callers to users in this dial plan can dial and search for users.

Allow callers to:

☒ Transfer to users
☒ Leave voice messages without ringing a user's phone

Allow callers to search for users by name or alias:

☐ In this dial plan only
☒ In the entire organization
☐ Only on this auto attendant

☐ Only for this extension

☐ In this address list

Information to include for users with the same name:

None

9.7 Skype for Business PowerShell

PowerShell is a command line interface for managing a Windows 2008 or 2012 server. It is a similar, however much more powerful, environment than the DOS prompts included in previous Windows releases.

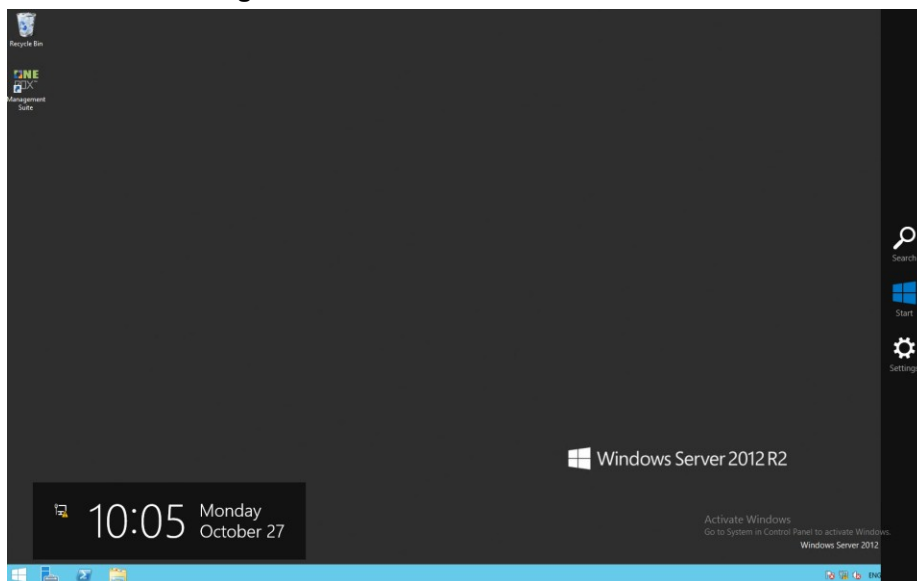
The Skype for Business Server Management Shell is a PowerShell environment with a Skype for Business specific command extension module added, which enables you to manage the Skype for Business environment from the command line. Similar modules are available for other products, such as Exchange.

There are numerous ways to access the PowerShell and Skype for Business PowerShell environments, either remotely or via a locally attached console and keyboard.

The easiest method is as follows:

1. Use Remote Desktop to access the CloudBond 365 Controller (UC-DC).
2. Open the charms bar on the Windows desktop.
3. Use the search facility to look for 'Skype for Business'.
4. Select 'Skype for Business Server Management Shell'.

Figure 9-28: Windows Server 2012 R2



5. Open the charms bar.

6. Use the Windows + C key combination, or hover the mouse in the top or bottom right corners of the desktop.

Figure 9-29: Searching for Skype for Business

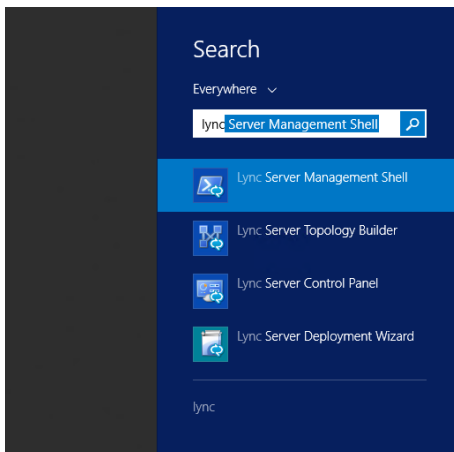
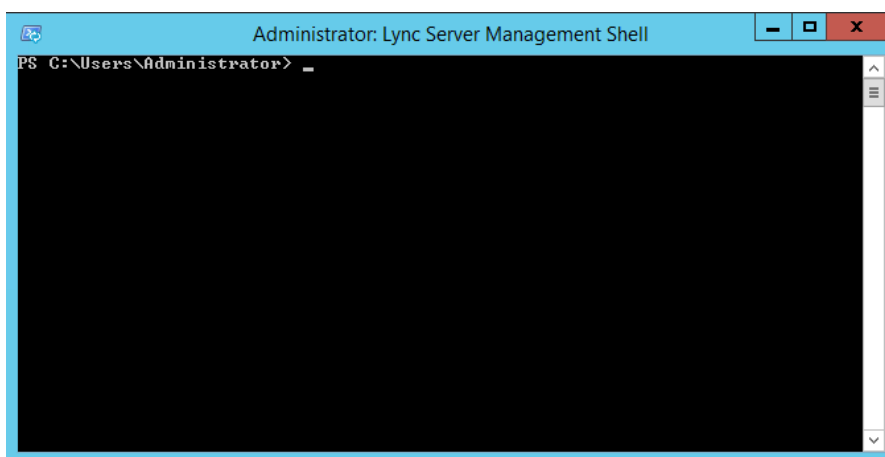


Figure 9-30: The Skype for Business Server Management Shell



9.8 PowerShell for Skype for Business Online

The following provides a sample PowerShell script which connects to Skype for Business On-Line to allow entering PowerShell command line configuration items. You will need to satisfy the pre-requisites detailed in the following links, prior to using PowerShell for online components:

- for Azure AD <http://aka.ms/aadposh>
- for Skype for Business Online <http://www.microsoft.com/en-us/download/details.aspx?id=39366>

9.8.1 Connecting to Office 365 using PowerShell:

```
# Configurable parameters
# The OverrideAdminDomain property needs to be set to the default
domain that was included with your Office 365 subscription.
$OverrideAdminDomain="ocshost.onmicrosoft.com"
# Script starts here - No configuration required Import-Module
Skype for BusinessOnlineConnector
import-module msonline
$credentials=Get-Credential
Connect-MsolService -Credential $credentials
$OnlineSession=New-CsOnlineSession -Credential $credentials
-OverrideAdminDomain
$OverrideAdminDomain
$ExchangeSession = New-PSSession -ConfigurationName
Microsoft.Exchange - ConnectionUri
https://ps.outlook.com/powershell/ -Credential $credentials -
Authentication Basic -AllowRedirection
Import-PSSession $OnlineSession -AllowClobber Import-PSSession
$ExchangeSession -AllowClobber
```

Sample execution of the PowerShell script.

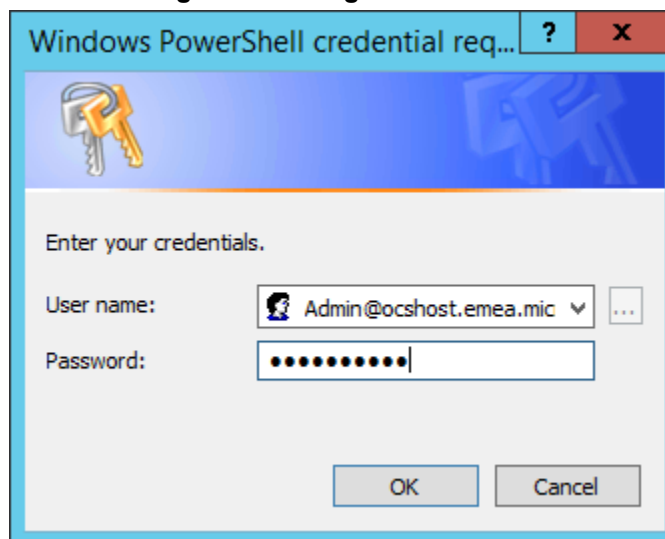
(Note that the Microsoft Online Service Module is out of date, and a newer version should be downloaded.)

Figure 9-31: Windows PowerShell

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.OCSHST> # Configurable parameters
PS C:\Users\administrator.OCSHST> # The OverrideAdminDomain property needs to be set to the default domain that was included with your Office 365 subscription.
PS C:\Users\administrator.OCSHST> $OverrideAdminDomain="ocshost.onmicrosoft.com"
PS C:\Users\administrator.OCSHST> # Script starts here - No configuration required
PS C:\Users\administrator.OCSHST> Import-Module LyncOnlineConnector
PS C:\Users\administrator.OCSHST> import-module msonline
PS C:\Users\administrator.OCSHST> $credentials=Get-Credential
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential:
PS C:\Users\administrator.OCSHST> Connect-MsolService -Credential $credentials
WARNING: There is a newer version of the Microsoft Online Services Module. Your current version will still work as expected, however the latest version can be downloaded at https://portal.microsoftonline.com.
PS C:\Users\administrator.OCSHST> $LyncSession=New-CsOnlineSession -Credential $credentials -OverrideAdminDomain $OverrideAdminDomain
PS C:\Users\administrator.OCSHST> $ExchangeSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell/ -Credential $credentials -Authentication Basic -AllowRedirection
WARNING: Your connection has been redirected to the following URI:
https://pods1047psb.outlook.com/powershell-liveid?PSVersion=4.0
PS C:\Users\administrator.OCSHST> Import-PSSession $LyncSession -AllowClobber
ModuleType Version Name ExportedCommands
-----
Script 1.0 tmp_aeazcyw4.pao {Copy-CsVoicePolicy, Disable-CsMeetingRoom, Enable-CsMeeti...
PS C:\Users\administrator.OCSHST> Import-PSSession $ExchangeSession -AllowClobber
WARNING: The names of some imported commands from the module 'tmp_h2uwuhyoc.bag' include unapproved verbs that might make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.
ModuleType Version Name ExportedCommands
-----
Script 1.0 tmp_h2uwuhyoc.bag {Add-AvailabilityAddressSpace, Add-DistributionGroupMember...
PS C:\Users\administrator.OCSHST>
PS C:\Users\administrator.OCSHST>
PS C:\Users\administrator.OCSHST>
```

The script will prompt you for login credentials. Use your Office 365 administrator account.

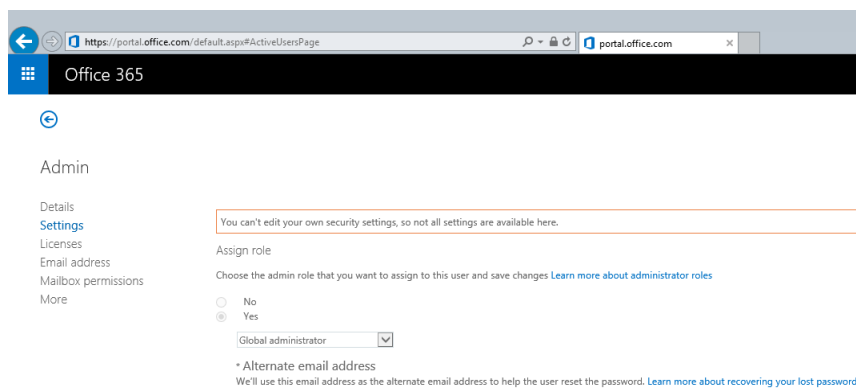
Figure 9-32: Login Credentials

When the script completes, you can enter Skype for Business Online PowerShell commands to configure your Skype for Business Online environment.

9.9 Troubleshooting

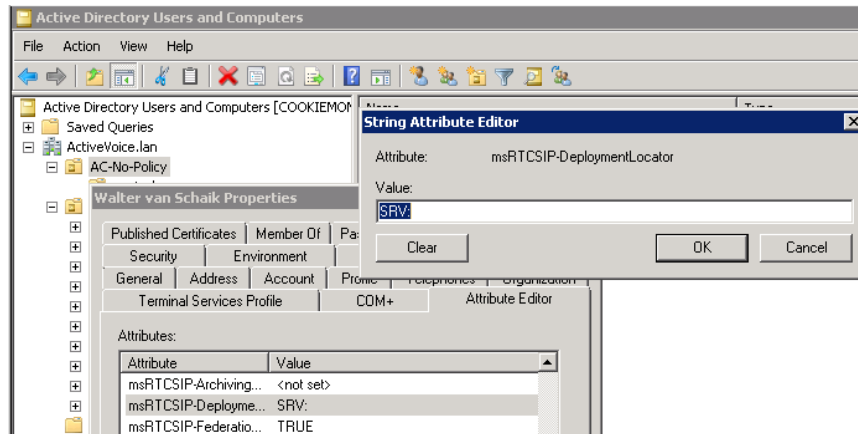
As the multi-forest environment relies on multiple replication processes here are some general guidelines for troubleshooting the environment.

- Verify the administrator account in the Office 365 configuration settings is a global administrator in Office 365 by signing in to the portal: <https://portal.microsoftonline.com/> with those credentials and verifying the settings under the users section for the particular account.

Figure 9-33: Admin Settings

- Verify the ACSUserReplication scheduled task can write back the Skype for Business specific attributes into the customer forest by opening Active Directory Users and Computers for the user forest, with the credentials used in the scheduled task (default: resource forest\administrator). Navigate to a user and try to manually set one of the attributes:

Figure 9-34: String Attribute Editor



- On the CloudBond 365 controller (or any other customer server or workstation that has the Office 365 PowerShell prerequisites installed), start a PowerShell session and use the following cmdlets to verify that Office 365 directory synchronization has populated the on-premises data to the cloud:

```
$OverrideAdminDomain="<the OverRideAdminDomain as in the O365
settings page>"
$WarningPreference='silentlycontinue' $credential = Get-
Credential
$CSSession=New-CsOnlineSession -Credential $credential -
OverrideAdminDomain $OverrideAdminDomain
Import-Module SkypeOnlineConnector
Import-PSSession $CSSession -AllowClobber| Out-Null
Get-CsOnlineUser | Where-Object {$_.sipaddress -match "<a sip
address to check>"}
```


An example output for the Get-CsOnlineUser cmdlet looks like the following:

Figure 9-35: Get-CsOnlineUser Attributes

```

PS C:\Users\wsc> Get-CsOnlineUser | Where-Object {$_.sipaddress -match 'corp'}

RunspaceId      : 0aa16efa-b5f1-4e00-95f5-5d281db2cceb
UserAccountControl : PasswordNotRequired, NormalAccount
Id              : CN=49290bf3-d625-4df2-9612-a02c93f710ed,OU=c524b5f5-fd18-43c0-964c-bc5d35525eaa,OU=OC5 Tenants,DC=lync0e001,DC=local
CountryAbbreviation :
Company         :
Department      :
Description      : {}
Fax             :
HomePhone       :
IPPhone         :
City            :
Manager         :
MobilePhone     :
OriginatorSid    :
OtherTelephone   : {}
Office          :
PostalCode      :
PreferredLanguage :
Puid            : 10038FFD8C12084C
StateOrProvince :
Street          :
ThumbnailPhoto   :
Title           :
Phone           :
WebPage         :
AdminDescription :
AssignedPlan     : {<XmlValueAssignedPlan xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                    <Plan AssignedTimestamp="2014-10-14T08:20:33Z"
                    ServicePlanId="0faeb32-d00e-4d6e-bb5-43b583db82c" CapabilityStatus="Enabled"
                    SubscribedPlanId="c4b86aed-a92a-42ea-a84a-d21487ed014f"
                    ServiceInstance="MicrosoftCommunicationsOnline/Instance03-S"
                    xmlns="http://schemas.microsoft.com/online/directoryservices/change/2008/11">
                    <Capability>
                    <Capability Plan="MCOPProfessional"
                    xmlns="http://schemas.microsoft.com/online/MCO/2009/01" />
                    </Capability>
                    </Plan>
                    </XmlValueAssignedPlan>}
Alias            : corporatead
BaseImplUrl      : https://meet.lync.com/ocshost
DirSyncEnabled   : True
ObjectId         : 49290bf3-d625-4df2-9612-a02c93f710ed
UsageLocation    : NL
HideFromAddressLists : False
OnPremHideFromAddressLists : False
ProvisionedPlan  : {}
ProvisioningStamp :
UpgradeRetryCounter : 0
SyncingCounter   : 0
ProvisioningCounter : 0
PublishingStamp  :
OnPremHostingProvider : SRV:
OnPremOptionFlags : 257
OnPremSIPEnabled : True
OnPremSIPAddress  : sip:corporatead@activecommunications.eu
OnPremLineURI    :
OnPremValidationErrors : {}
  
```

We are specifically interested in the following attributes:

- OnPremHostingProvider: SRV:
- OnPremOptionFlags 257
- OnPremSIPEnabled : True
- OnPremSIPAddress : sip:corporatead@activecommunications.eu

This informs us that directory synchronization with Office 365 was successfully completed and that the msRTCSIP attributes from the CloudBond 365 resource forest were brought to Office 365.

When a user is homed in Skype for Business Online, the OnPremHostingProvider attribute holds the value of the Host entry on the Office 365 settings page in the CloudBond 365 Management suite, defaulting to sipfed.online.lync.com.

If these attributes are displayed empty, perform the manual steps as described in Initial Replication Section 9.4 for the particular user and make sure that the Office 365 Directory Synchronization agents replicate these values by right-clicking their properties and verifying the Properties.z file.

Figure 9-36: Windows Azure AD Properties

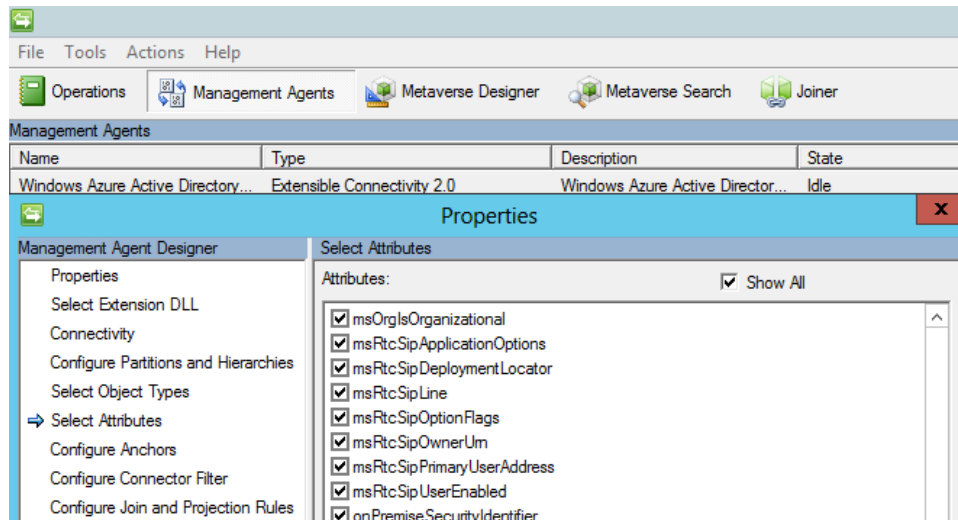
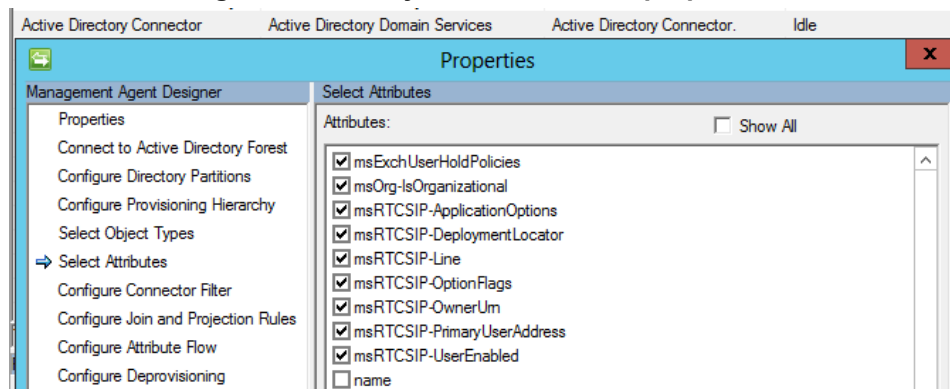


Figure 9-37: DirSync AD Connector properties



A default installation of the Office 365 Directory Synchronization environment will have those attributes checked by default.

9.10 Custom User IDs for Cross Domain Updates

The following paragraphs describe the Custom User IDs for Cross Domain updates.

9.10.1 Updating the User Forest AD

It is possible to use a different account to perform updates to the User forest if there is a reason to avoid using cloudbond365\administrator.

You will first need to manually create a new account within the cloudbond365 AD. This account should be made an administrator as a member of the

- cloudbond365\Administrators

or

- cloudbond365\Domain Admins

This account will also need to be a member of the Skype for Business administrators groups:

- csAdministrator
- acs-Admin
- rtcComponentUniversalServices
- rtcUniversalServerAdmins
- rtcUniversalUserAdmins

The updates to the User forest are performed by a scheduled task. The scheduled task runs C:\acs\AcsUserReplication\AcsUserReplication.exe. This task will need to be modified to execute as the new user you have created.

The AcsUserReplication.exe process updates the following attributes within the User forest:

- SIP entry in proxyAddresses
- msRTCSIP-DeploymentLocator
- msRTCSIP-OptionFlags
- msRTCSIP-PrimaryUserAddress
- msRTCSIP-UserEnabled

If you wish to tighten security, you may restrict the newly created admin user to only have write access to the above fields within the User forest AD.

9.10.2 Retrieving User Data from Office 365

The updates to the cloudbond365 directory from Office 365 are performed by a scheduled task. The scheduled task runs the following:

```
C:\acs\OFFICE365Sync\SysAdmin.O365.Sync.exe -S O365
```

This task will use the User ID you have created within Office 365. The user will need to be granted rights within Office 365.

With regards to the “Global Administrator Rights” in Microsoft Online, Microsoft has made changes in its latest release, where now the Skype for Business administrator role will be sufficient (see screenshot below):

Figure 9-38: Administrator Roles

Choose the admin role that you want to assign to this user
and save changes [Learn more about administrator roles](#)

- ☐ User (no administrator access)
- ☐ Global administrator
- ☒ Customized administrator
 - ☐ Billing administrator
 - ☐ Exchange administrator
 - ☐ Password administrator
 - ☒ Skype for Business administrator
 - ☐ Service administrator
 - ☐ SharePoint administrator
 - ☒ User management administrator

This role is required when moving users from Office 365 to on premise and vice versa, which move is performed by the O365 Connector.

The newly created Office 365 User ID and password needs to be specified within the SysAdmin web pages, on the O365 Connector settings.

Figure 9-39: Office 365 Settings

SYSTEM CONFIGURATION ABOUT

Office 365 Settings

User Name:

Host:

MigrationOverrideUrl:

OverrideAdminDomain:

Password:

Confirm password:

Apply

This page is intentionally left blank.

10 Configuring Certificates

This section provides a background introduction to Certificates and their use with CloudBond 365. It also describes CloudBond's Certificate requirements, and provides procedures for requesting and generating internal certificates, as well as installing Microsoft Certificate Authority utility if required.



Note: If you intend to use CloudBond 365 for external connectivity (External users, External conferencing, Federation etc.) you will need to obtain additional certificates.



Note: You must change or add a valid SIP domain for external access as the default SIP domain and associated Simple URL's, DNS references, etc. are not suitable for the public internet. See Section 14 on page 239.

10.1 Background

Those who are familiar with Certificates, and their implementation with Microsoft products can skip to the next section.

For those unfamiliar with certificates, some background concepts are provided here.

10.1.1 Public Key Infrastructure

Skype for Business uses a Public Key Infrastructure (certificates) to enable secure MTLS and TLS communication between servers and clients. In other words, Skype for Business clients and servers can “trust” each other, and communications between them is generally encrypted.

More background information on how the Public Key Infrastructure works can be found at: http://en.wikipedia.org/wiki/Public_key_infrastructure

10.1.2 What Purpose does Certificates Serve?

Certificates within Microsoft perform two major functions:

- Allow different computer services to verify they are communicating with the server they intended to communicate with (trust)
- Allow communication to be encrypted with public and private keys if required (privacy).

10.1.3 Trust

Certificate trust works on a third-party system. i.e., The two communicating computers may not trust each other directly, however they must ultimately trust a third-party Authority, who will vouch for their identity.

To do this, each server will obtain a certificate from a Certificate Authority (CA) which will include various information, including who issued the certificate, the servers' name, and its private and public encryption keys.

Any other server can attempt to communicate with this server by its name, and for security, will request that the server provide the public information of its certificate. The requesting server can then perform validity checks on the certificate, such as that it trusts the CA that issues the certificate (through the certificate chain), it has not expired or has been revoked, that the certificate matches the server name requested, and various other items. If the certificate is considered valid, then communication will proceed.

Trust may be established in one direction, or in both directions. Both servers may use different Certificate Authorities.

10.1.3.1 Trust and Certificate SANs

Simple certificates are issued to one server name only. These certificates contain the server name within the subject field of the certificate.

It is possible to obtain certificates which are issued to multiple servers, or to single servers hosting multiple services with multiple server names. In these certificates, each server name is listed in the certificate Subject Alternate Name (SAN) field. These certificates are commonly called Multi-SAN or UC certificates.

Multi-SAN certificates require the subject name to be included as one of the SAN entries.



Note: The subject field will be depreciated in future, and no longer used.

10.1.3.2 Wildcard Certificates

Another possible certificate variation is the Wildcard Certificate. Essentially, this is a certificate which can be applied to a single domain, and will cover any server within the domain or sub-domain. E.g. *.contoso.com

Wildcard certificates can be used within CloudBond 365 in limited configurations, however may introduce complexities with Federation and other external access. They are generally not suitable for CloudBond 365 deployments with multiple SIP domains.

10.1.4 Privacy

A component of certificates are a pair of public and private “keys”.

The public key is published and available for anyone to use when communicating with the server. Anything encrypted with the public key can only be decrypted with the private key.

The private key is kept secret by the computer to which the certificate was issued. This key can be used to decrypt any information encrypted with the public key, and ensure its integrity. It can also be used to encrypt any outgoing information, which can only be decrypted with the matching public key. This ensures the information actually came from the holder of the certificate.

10.1.5 Certificate Authorities

There are many Certificate Authorities (CAs’) available to issue certificates. For a certificate to be trusted, its certificate chain is checked until an issuer is found in the computers Trusted CAs’.

Microsoft operating systems and web clients come with several pre-installed third-party Root Certificates from some well-known public Certificate Authorities. These include Digicert, Microsoft, Thwate, Verisign to name just a few. Microsoft products will automatically trust certificates issued by these Certificate Authorities.

For those CAs’ not automatically trusted, you can import a Certificate Chain, which will add those Certificate Authorities to the trusted list. A certificate chain is used, as issuing of certificate may be delegated to lower tier CAs’. Trust must be maintained between each tier within the chain of CAs’.

Microsoft also provides the tools to create your own Certificate Authority within your Domain. These private, internal CAs’ are typically installed along with a Domain Controller. The Root

Certificate and chain for these Internal CAs' is automatically distributed to all domain member computers within the domain. This allows any member computer within a domain to trust any other member within the domain automatically.

10.1.5.1 Where to Obtain Certificates?

Certificates can be obtained from private corporate Certificate Authorities (free, however generally valid for internal use only), or can be purchased from a Public Certificate Authority.



Warning: Public Certificate Authorities will no longer issue certificates containing internal DNS names or reserved IP addresses valid beyond Nov 1, 2015. This includes common private DNS namespaces, such as .local, and .lan, as well as popular IP address ranges 192.168.x.x and 10.x.x.x. In practice, all internal private certificates will need to be generated from a private certificate authority beyond that date.

10.1.5.2 How to Obtain a Certificate?

The exact process for obtaining a certificate varies from vendor to vendor. Consult your certificate vendors' documentation when obtaining public certificates.

In general, a "certificate request" file is generated, based on information provided. The information includes organization, location, server name and subject alternate names, encryption key length etc. The certificate request file is then presented to the CA, who will generate and sign a certificate based on the certificate request file. The resulting certificate file is then imported into a server certificate store, and assigned a role within the Skype for Business environment.

10.2 CloudBond 365 Default Certificates

10.2.1 CloudBond 365 Included Certificates

All CloudBond 365 systems come with several private certificates generated by the private CA installed on the CloudBond 365 Controller (UC-DC). Whilst these certificates could be used, they will not be trusted by most client machines.

It is usually required to generate or otherwise obtain certificates from a trusted source, such as a Corporate CA, or public CA.

A public certificate is required for most external connections to CloudBond 365.

10.2.2 CloudBond 365 External Certificates

If you intend to use CloudBond 365 for external connectivity (External users, External conferencing, Federation etc.) you will need to obtain additional certificates.

Any public certificate you obtain cannot include the default server names, as these are registered to AudioCodes.



Note: You must change or add a valid SIP domain for external access as the default SIP domain and associated Simple URL's, DNS references, etc. are not suitable for the public internet. See Section 14 on page 239.

10.3 CloudBond 365 Certificate Requirements

For the CloudBond Skype for Business deployment, certificates are used for server to server communication, for client to server communication, and for external access to the servers.

To accomplish this, certificates are deployed on the CloudBond 365 Front End server for both internal and external access, and also on the CloudBond 365 Edge server for both internal and external access.

- CloudBond 365-Front End
 - Internal
 - ◆ SIP/TLS communications
 - External (through reverse proxy)
 - ◆ Simple URLs
 - ◆ External Web Services
- CloudBond 365-Edge
 - Internal
 - ◆ Connection to Front End
 - ◆ SIP/TLS Communications
 - External
 - ◆ Web Conferencing Service
 - ◆ A/V Edge Service
 - ◆ Access Edge Service

Whilst Skype for Business allows numerous certificates to be used for many Skype for Business components, it is possible to reduce the requirements down to one Public Multi-SAN (UC) certificate for all external roles.

Depending upon server and domain names chosen during build of CloudBond 365 system, it may be possible to use a single public certificate for both internal and external roles.

Most commonly, a single Public certificate is used for the External roles, whilst a single or multiple private certificate(s) are used for the internal roles.

More information on Certificate requirements can be found in Section 10.11 on page 199.

10.3.1 Notes

With regards to Public Skype for Business users connecting the system from an out of office location, an additional Public Certificate is required at all times.

The default certificate from CloudBond 365 is suitable for internal network use only.



Warning: Public Certificate Authorities will no longer issue certificates containing internal DNS names or reserved IP addresses valid beyond Nov 1, 2015. This includes common private DNS namespaces, such as .local, and .lan, as well as popular IP address ranges 192.168.x.x and 10.x.x.x. In practice, all internal private certificates will need to be generated from a private certificate authority beyond that date.

10.4 Public Certificates

Public certificates for CloudBond 365 are required for all external access, such as external users, federation, external conferencing etc.

Public certificates, other than the one supplied, cannot be used for internal access for the CloudBond 365 Standard Edition system as the domain names are registered to AudioCodes.

Public Certificates may be used for internal access on CloudBond 365, depending upon domain and server names chosen during Software Installation.

10.4.1 Minimizing Cost

Obtaining a Public Certificate from a certificate authority can be a costly exercise. Whilst single year, single server certificates are relatively cheap, Multi-SAN (UC) certificates for multi-year periods can be very costly. Typically, the cost of the certificate will increase with the number of SAN entries included.

With cost in mind, it is best to reduce the number of SAN entries to the minimum required. For a CloudBond Skype for Business deployment, SAN entries will be required for the following:

- Each Simple URL
- External Web Services
- A/V Edge Service
- External Access Edge service
- Web Conferencing Edge service

In a default Skype for Business deployment with multiple SIP domains, this can quickly escalate to multiple individual certificates, or multiple SAN entries.

The Skype for Business Topology Builder does however, allow you to optimize the number of SAN entries required, thus reducing the cost of public certificates. In particular, there are multiple options for Simple URL naming conventions, which can greatly reduce the number of SAN entries required on a public certificate. There are also different options for Edge external access services, which can reduce SAN requirements.

10.4.2 Planning

Before generating your public certificate requests, you should plan, review, and adjust your Skype for Business Topology to reduce the number of SAN's required. When using the Skype for Business certificate wizards, the certificate requests they create are based on the information within the Skype for Business Topology.

10.4.2.1 Minimize the Number of SIP Domains

Skype for Business supports a primary SIP domain, and additional SIP domains. Microsoft recommends that the SIP domain should match a user's email domain. This simplifies many features of Skype for Business for the user, such as logging in using a Skype for Business Client, where the user logs in using a SIP domain.

Whilst the SIP domain is not used directly on certificates, it does form the basis for many other entries, such as simple URLs' and Edge services. For this reason, it is best to minimize the number of SIP domains where possible.



Note: You can have additional SIP domains for internal use only. If these domains are not accessed externally, they will not require public certificate entries.



Note: You must change or add a valid SIP domain for external access as the default SIP domain and associated Simple URL's, DNS references, etc. are not suitable for the public internet. See Chapter 6.

A CloudBond 365 has a default primary SIP domain of cloudbond365.local. Any other SIP domains must be added or changed after deployment.

The default SIP domain and associated URL's (cloudbond365.local) cannot be used for External public access.

It is generally easier to add your email domain as an Additional SIP Domain, rather than replace the Primary SIP Domain.

For example:

- Primary SIP Domain
 - cloudbond365.local
 - (Not used Externally, so no SAN entry required.)
- Alternate SIP Domain
 - contoso.com
 - (Used Externally, so simple URLs etc. based on this)

10.4.2.2 Minimize the Variations in Simple URLs

Skype for Business' simple URL's are anything but simple.

For a single SIP domain, Simple URL's are straight forward. A single URL for Dialin Conferencing, and another for Meetings. It is common not to use an Administrative access URL.

An additional SIP Domain automatically adds a new Meeting URL for you. Nice and easy... but wait.

Each new base URL requires a new DNS entry, which requires a new SAN entry on your SSL certificate... so it would be nice to keep these extra URL's to a minimum.

Skype for Business allows 3 main methods of configuring Simple URL's, which have varying economies on DNS entries and SSL Certificate SAN's.

See <http://technet.microsoft.com/en-us/library/gg398287.aspx> for details.

Each simple URL base or "root" will require an additional SAN entry on a public certificate.

It is possible to reduce the number of SAN entries to one, with judicious use of the Simple URL naming options.

As a quick summary:

- Option 1 – Base URL contains role and SIP Domain. Roles are Dialin, Meet, Admin
 - <https://dialin.contoso.com>
 - <https://meet.contoso.com>
 - <https://admin.contoso.com>
 - <https://dialin.fabrikam.com>

- <https://meet.fabrikam.com>
- <https://admin.fabrikam.com>
- i.e., 1 DNS entry per role, per domain = 6 DNS entries and 6 SAN entries
- Option 2 – Same Base URL for each SIP domain. Role becomes a suffix.
 - <https://meet.contoso.com/dialin>
 - <https://meet.contoso.com/meet>
 - <https://meet.contoso.com/admin>
 - <https://meet.fabrikam.com/dialin>
 - <https://meet.fabrikam.com/meet>
 - <https://meet.fabrikam.com/admin>
 - i.e., 1 DNS entry per domain = 2 DNS entries and 2 SAN entries
- Option 3 – Same Base URL for all SIP Domain. Role and Domain become suffix.
 - <https://meet.contoso.com/contoso.com/dialin>
 - <https://meet.contoso.com/contoso.com/meet>
 - <https://meet.contoso.com/contoso.com/admin>
 - <https://meet.contoso.com/fabrikam.com/dialin>
 - <https://meet.contoso.com/fabrikam.com/meet>
 - <https://meet.contoso.com/fabrikam.com/admin>
 - i.e., 1 DNS entry per Skype for Business system = 1 DNS entry and 1 SAN entry

The most economical method in terms of DNS and SAN entries is Option 3. In this option, the base or “root” part of the URL is kept the same, resulting in only one DNS and one SAN entry to cover all the Simple URL’s. The SIP domains are maintained in the part of the URL following the base, and thus do not require additional SAN entries.

e.g., For option 3 above, the SAN entry required is: meet.contoso.com



Warning: The Topology builder will check for conflicting URL’s. The Simple URL’s base component must be unique from that used for External Web Services on the FE Pool, even though they will point to the same server within CloudBond 365.



Warning: If you’ve changed the primary SIP domain, you will have to change the Simple URL, Edge server External FQDNs, DNS entries, and Certificate SANs to match, regardless of which Option you choose. This is because you are changing the base part of the URL.



Warning: Changing the default Simple URL’s may require one or more additional DNS entries in your corporate DNS servers. (e.g. meet.contoso.com)

10.4.2.3 The External Web Services

One SAN entry is required for the External Web Services URL. This entry cannot be the same as any Simple URL root. e.g. ewslync.contoso.com.



Warning: The Topology builder will check for conflicting URL's. The Simple URL's base component must be unique from that used for External Web Services on the FE Pool, even though they will point to the same server within CloudBond 365.

10.4.2.4 Minimize the Edge External Service Names

Edge External FQDN's allow users to access your Skype for Business system from outside your organization. This includes Access Edge for external users, Web Conferencing Edge for external conferences, and A/V Edge for voice and video calls.

The three external services on the Edge server must be distinguished from each other. There are several naming options available.

They could have three separate server names and share the same TCP port number, requiring three SAN entries.

Alternatively, they could share a single server name, with three different port numbers. This option requires only one SAN entry for the certificate. e.g. sip.contoso.com



Note: It is common to use "sip" + sip domain name for the External Edge server, as this simplifies the Skype for Business Client built in search and access methods. It is also common to use "sip" + sip domain name for the Internal FE server, for the same Skype for Business client reasons. This solution works well with the same URL pointing to FE Internal and Edge External servers, and reduces the number of SAN entries when a public certificate is used internally.

10.4.2.5 What About LyncDiscover?

The Lyncdiscover DNS entry is used by the Skype for Business Mobile Client built in search to locate the Skype for Business Server. Do you need a SAN entry on a certificate for it? A very good question... The Skype for Business certificate wizard and most Skype for Business documentation includes a Lyncdiscover SAN entry for each SIP domain.

The Microsoft Remote Connectivity Analyser web site will currently fail when performing a Skype for Business Autodiscover test if this SAN entry is not present.

However...

The mobile client can communicate with the LyncDiscover URL over port 80, which is not encrypted or secured. Configuration information is passed back to the mobile client to allow it to login securely using a different URL to Lyncdiscover.

No SAN entry is required for the Lyncdiscover DNS entry in this configuration.

If you choose to configure secured access for the Skype for Business Mobile clients, you will require a SAN entry.

For further information, see:

<http://technet.microsoft.com/en-us/library/hh690012.aspx>
<http://technet.microsoft.com/en-us/library/hh690030.aspx>

10.4.2.6 Are There Other SAN Entries?

You may require other SAN entries on your public certificate, depending upon how you deploy CloudBond 365, and what Skype for Business options you choose.

For instance, deploying the XMPP (PIC) gateways and integration usually requires a SAN entry for the top level of each SIP domain.

Some Reverse Proxy servers require a SAN entry for their local server name as well as for the Skype for Business External names.

If you are deploying a single public certificate for both external and internal use, you will need SAN entries matching the FE and Edge internal server names.

10.4.2.7 So What is the Minimum Configuration / Certificate Request?

In our example, a single public multi SAN certificate with the following entries: Subject:

- meet.contoso.com

SAN:

- meet.contoso.com
- ewslync.contoso.com
- sip.contoso.com

Additional SAN entries may be required if:

- Mobile client access is configured for secured connections
- Certificate is to be used internally
- PIC Integration is to be configured

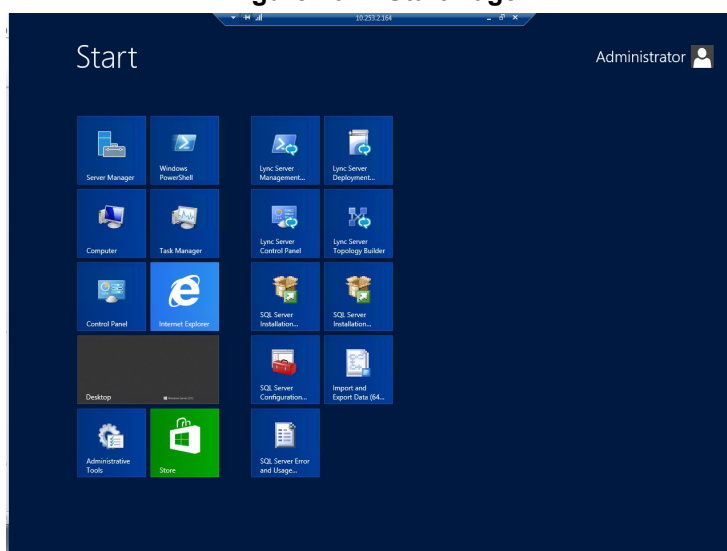
10.5 Using the Topology Builder

The procedure below describes how to use the Topology Builder.

➤ To use the Topology Builder:

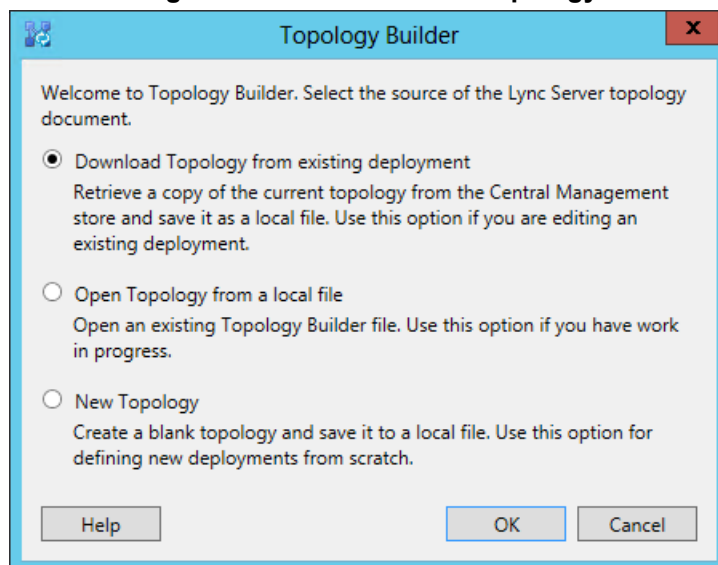
7. Open the topology builder. The Topology Builder is available on the CloudBond 365-Controller

Figure 10-1: Start Page



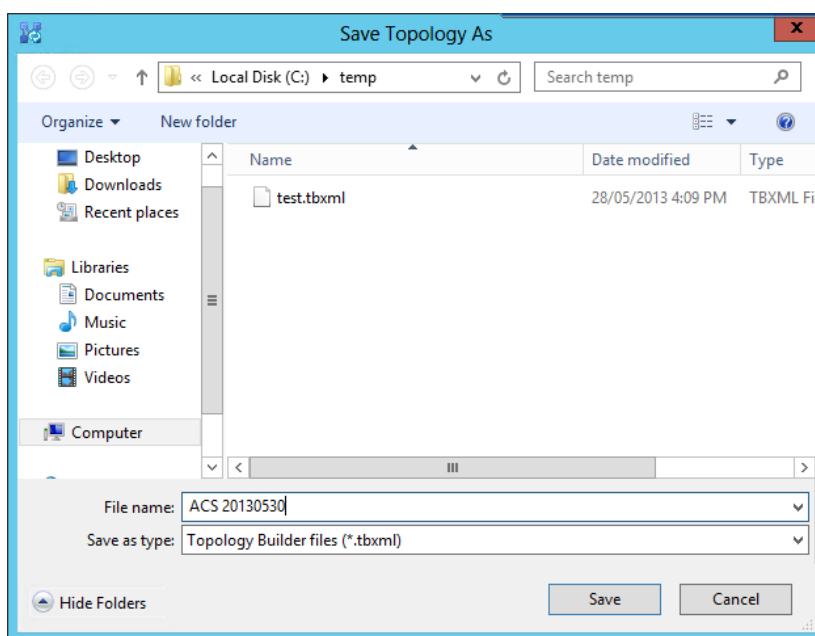
8. Click the **Download Topology from existing deployment** option, and then click **OK**.

Figure 10-2: Source of the Topology



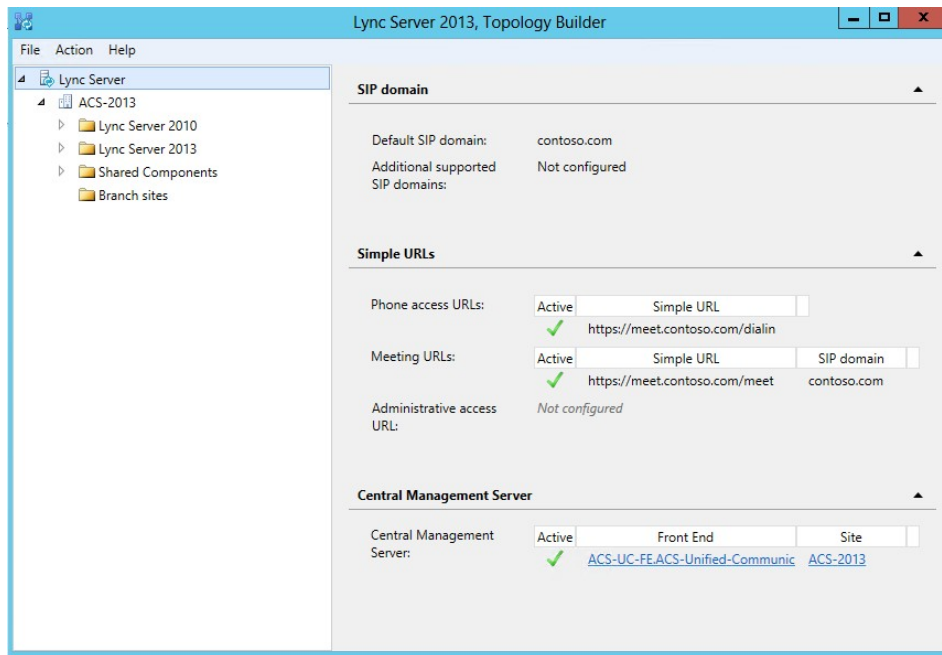
9. Click **Save**.

Figure 10-3: Saving the Topology



10. View the Topology, and adjust properties as required.

Figure 10-4: Topology Builder

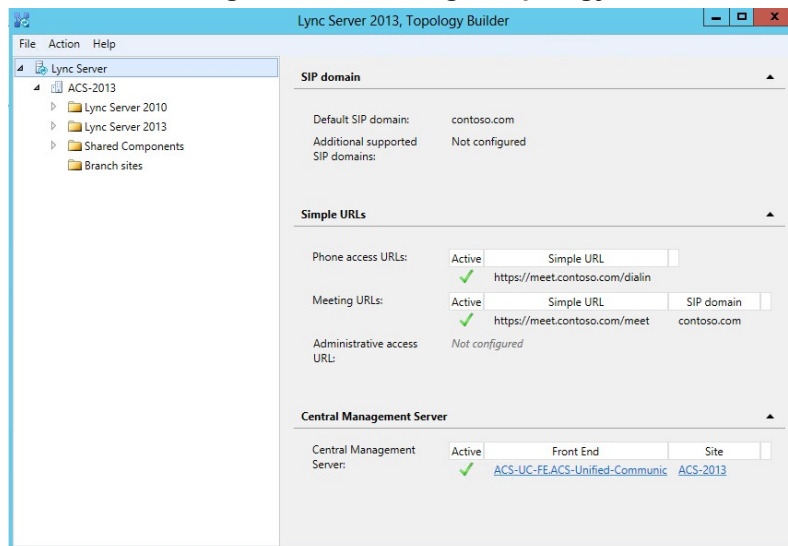


10.5.1 SIP Domain

SIP Domains are properties of the whole Topology.

1. In the Topology Builder, right-click the server (**Skype for Business Server 2015\Lync Server 2013**).

Figure 10-5: Viewing a Topology



2. From the menu options, select **Edit Properties**.

Figure 10-6: Edit Properties of the Server



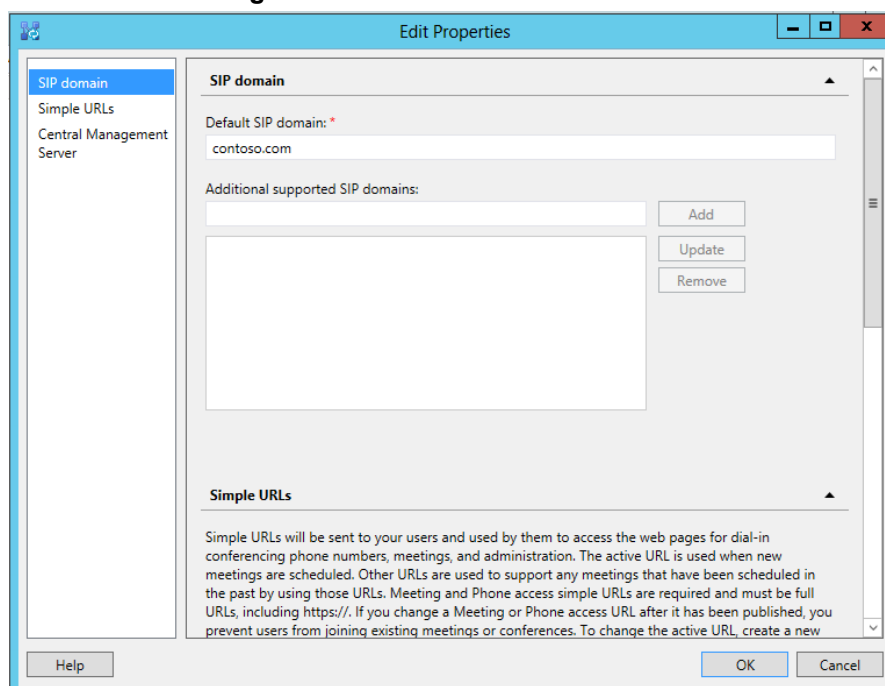
10.5.1.1.1 Adding the New SIP Domain to the Topology

The procedure below describes how to add a new SIP Domain to the topology.

- **To add a new SIP Domain to the topology**

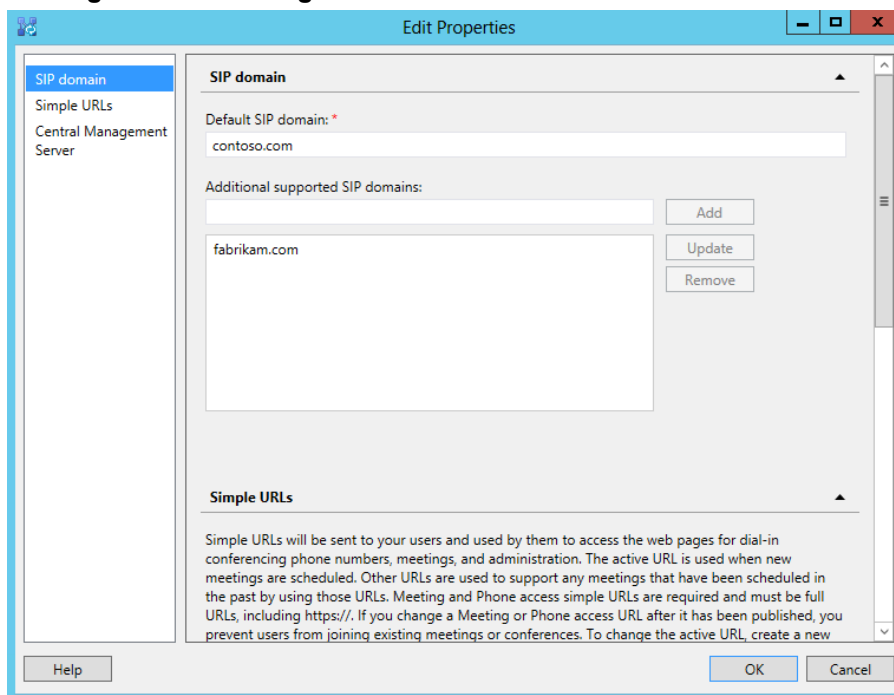
1. Open the **Edit Properties** page.

Figure 10-7: Additional SIP Domains



2. In the **Additional supported SIP domains** group, add "fabrikam.com", and then click **OK**.

Figure 10-8: Adding fabrikam.com as an additional SIP domain



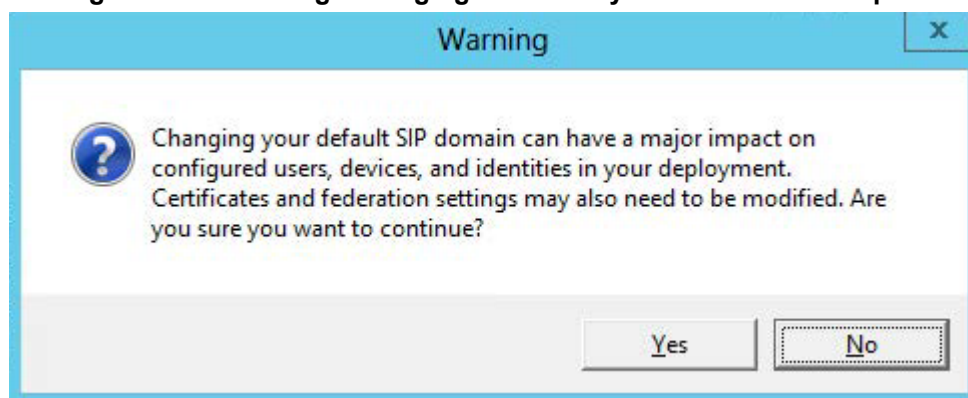
10.5.1.1.2 Changing the Default (Primary) SIP Domain

If you change the primary SIP domain, the following warning message is displayed, to remind you of some of the implications of making the change.

In general, it is usually easier to add an Additional SIP domain, rather than change the default SIP domain.

After changing the default SIP domain, you MUST review both the Simple URL's and Edge Server properties to make appropriate changes.

Figure 10-9: Warning: Changing the Primary SIP Domain is Complex



Note: Under some circumstances, such as when using Office 365 and Exchange Online as a voicemail server for PSTN calls, it is necessary to change the default SIP domain. Even in these cases, it is easier to add the new domain as an “Additional SIP domain”, then at a later time use the Skype for Business Management Shell to issue the command:

```
Set-CsSipDomain -Identity fabrikam.com -IsDefault $True
```

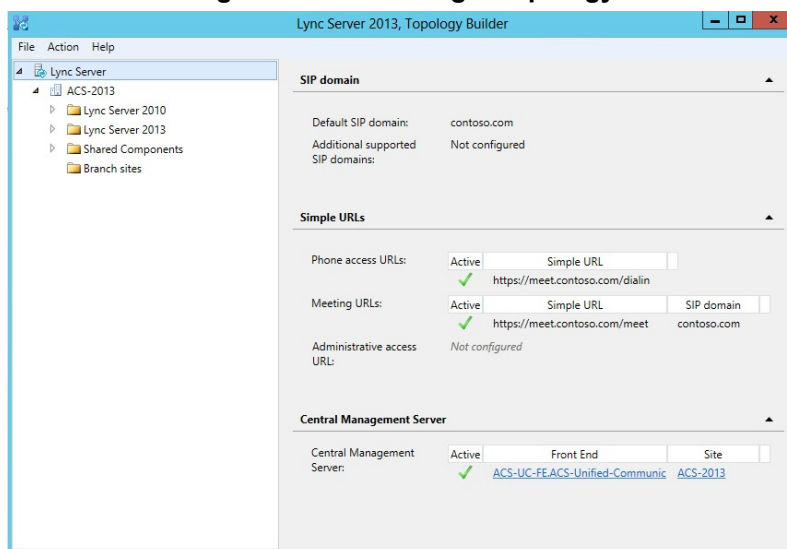
10.5.1.2 Managing Simple URL's

Simple URL's are also properties of the whole server topology.

➤ **To manage Simple URL's:**

1. In the Topology Builder, right-click the server (**Skype for Business Server 2015\Lync Server 2013**), and select **Edit Properties**.

Figure 10-10: Viewing a Topology



2. Scroll down, or select Simple URLs in the left panel.
3. Select a URL and click **Edit URL** to change it.
4. Select a URL and click **Remove** to remove the URL.

Figure 10-11: Topology Simple URLs – Using Option 2

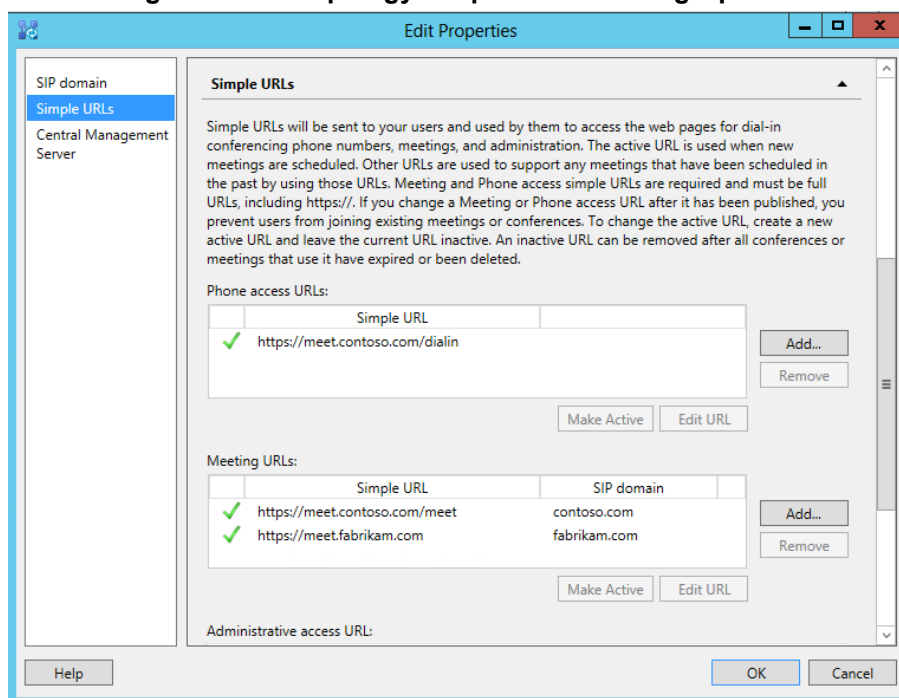


Figure 10-12: Simple URL's Using Option 3

Edit Properties

Simple URLs

Simple URLs will be sent to your users and used by them to access the web pages for dial-in conferencing phone numbers, meetings, and administration. The active URL is used when new meetings are scheduled. Other URLs are used to support any meetings that have been scheduled in the past by using those URLs. Meeting and Phone access simple URLs are required and must be full URLs, including https://. If you change a Meeting or Phone access URL after it has been published, you prevent users from joining existing meetings or conferences. To change the active URL, create a new active URL and leave the current URL inactive. An inactive URL can be removed after all conferences or meetings that use it have expired or been deleted.

Phone access URLs:

Simple URL
https://lync.contoso.com/dialin

Buttons: Add..., Remove, Make Active, Edit URL

Meeting URLs:

Simple URL	SIP domain
https://lync.contoso.com/acs-unified-commu	acs-unified-communicatio
https://lync.contoso.com/contoso.com/meet	contoso.com
https://lync.contoso.com/fabrikam.com/meet	fabrikam.com

Buttons: Add..., Remove, Make Active, Edit URL

Administrative access URL:

https://lync.contoso.com/admin

Buttons: Help, OK, Cancel



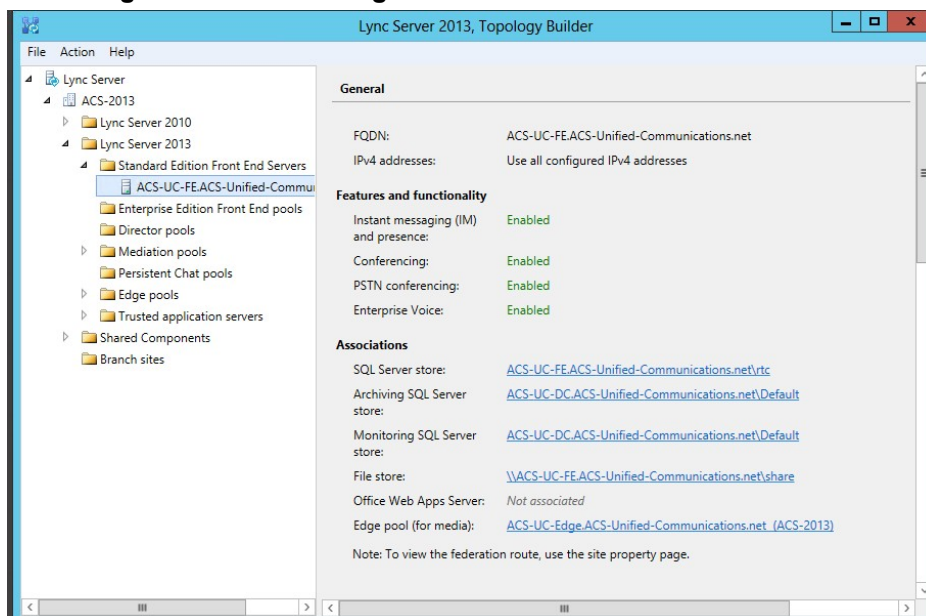
Warning: The Topology builder checks for conflicting URL's. The Simple URL's base component must be unique to the URL used for External Web Services on the FE Pool, even though they will point to the same server within CLOUDBOND 365.

10.5.1.3 Using External Web Services

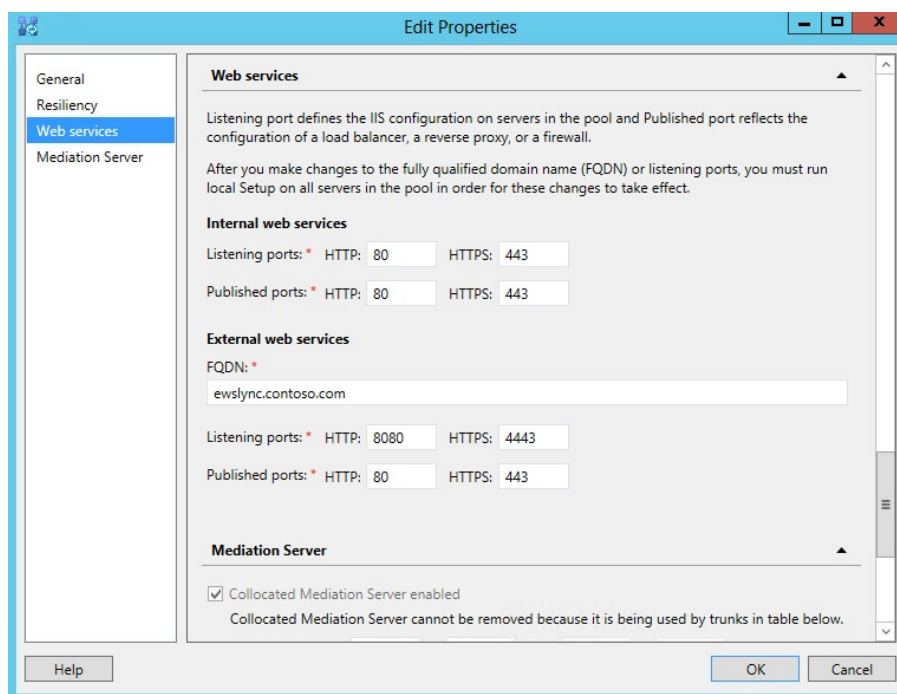
The External Web Services FQDN is a property of the Skype for Business Standard Edition Front End servers pool.

➤ **To use External Web Services:**

1. In the Topology Builder, navigate to the server (**Skype for Business Server 2015/Lync Server 2013**) Standard Edition server
2. Right-click, and select **Edit Properties**.

Figure 10-13: Selecting the Standard Edition Front End Pool

3. Scroll down, or select **Web Services** from the left pane.
4. Modify the External Web Services FQDN as required.
5. Click **OK**.

Figure 10-14: The External Web Services URL must be unique from the Simple URL's

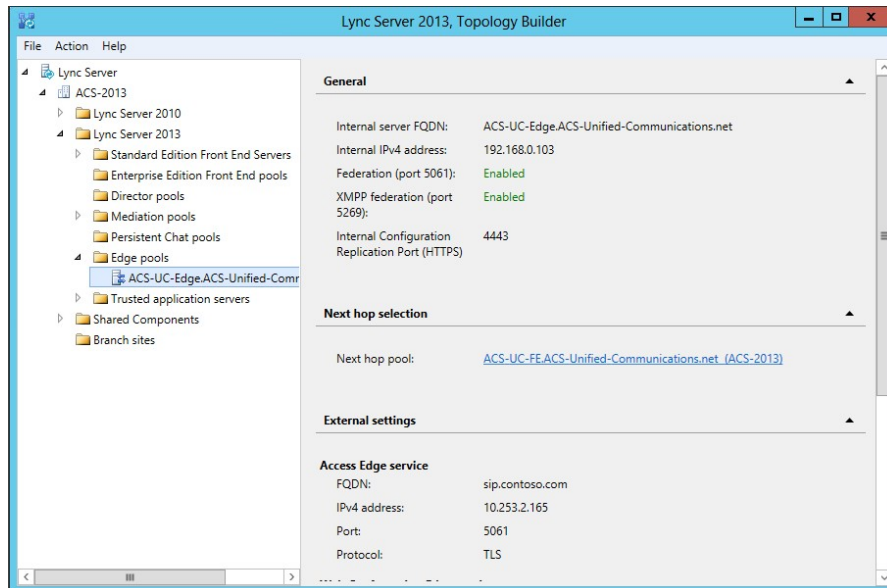
10.5.1.4 Configuring Edge Services

The Edge Server configuration is a property of the Skype for Business Server\Lync Server Edge pools.

➤ **To configure Edge Services:**

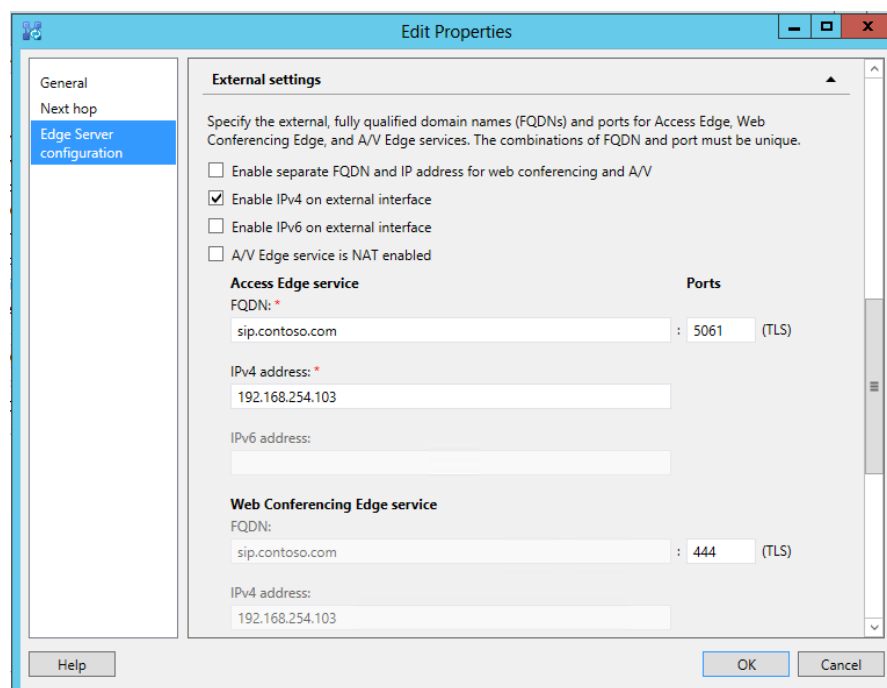
1. In the Topology Builder, navigate to the server (**Skype for Business Server 2015/Lync Server 2013 > Edge Pools**).
2. Right-click and select **Edit Properties**.

Figure 10-15: Selecting the Edge Server from the Edge Pool



3. Scroll down, or select **Edge Server Configuration** from the left pane.

Figure 10-16: Edge Server External Access FQDNs



4. Modify the service FQDNs' as required.
5. Click **OK**.



Note: The **Enable separate FQDN and IP Address for web conferencing and A/V** check box controls whether separate FQDN's may be entered for each service. The combination of FQDN and Port must be unique for each service.

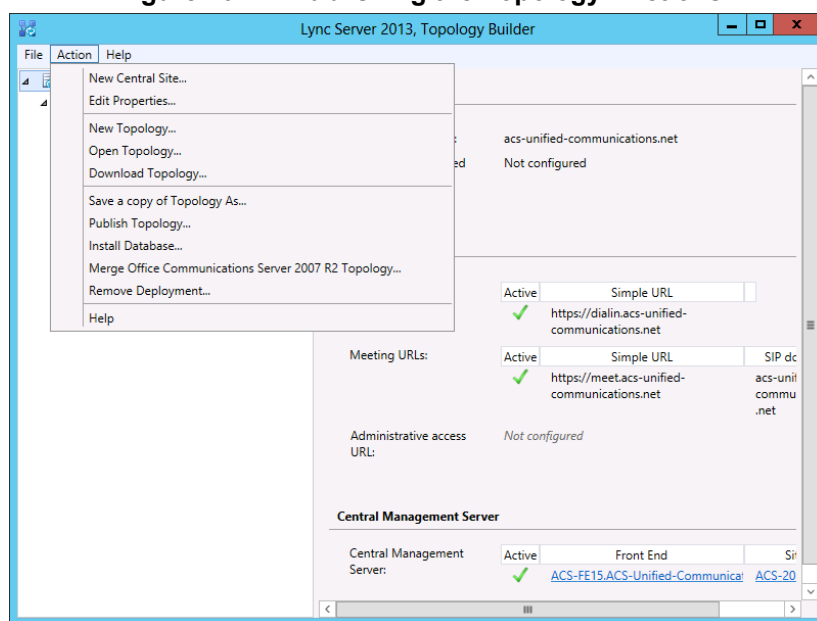
10.5.1.5 Publishing Topology and Deploy

If you have made changes to the Skype for Business Topology, you will need to Publish those changes to the Skype for Business Central Management Store (CMS), and then Deploy those changes to both the FE and Edge servers.

10.5.1.5.1 Publishing Topology

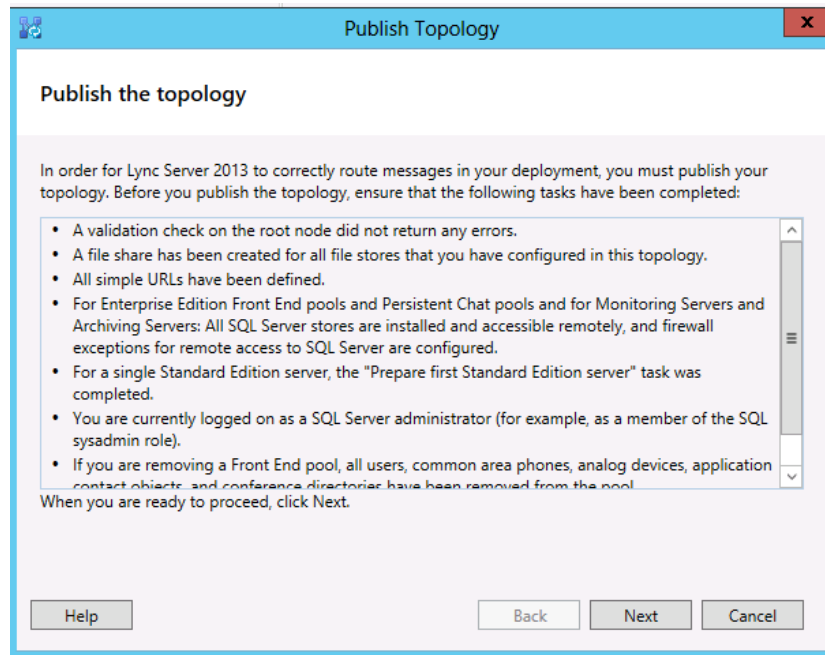
In Skype for Business Server\Lync Server Topology Builder make the required additions, like additional sip domains or voice gateways for example and select **Publish Topology...** to continue the installation:

Figure 10-17: Publishing the Topology - Actions



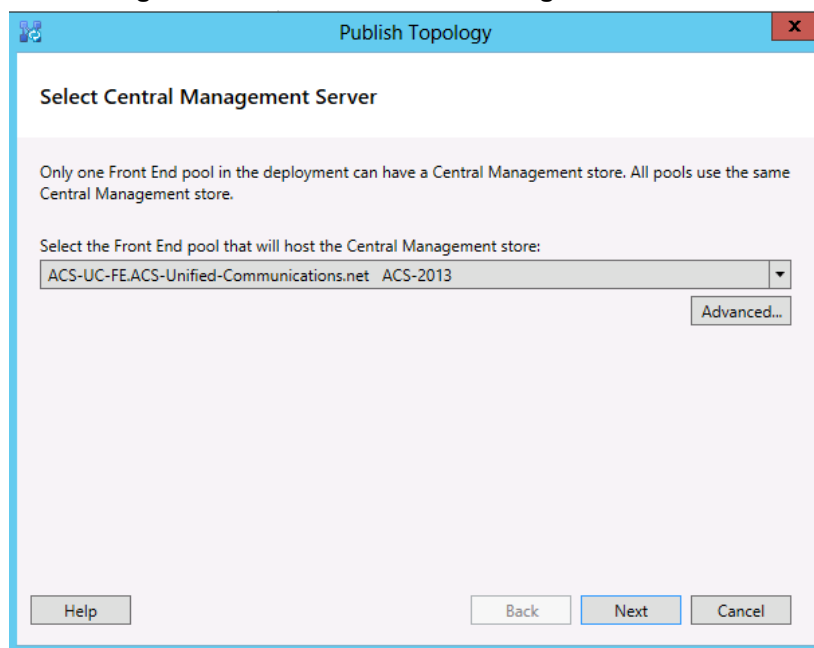
1. Continue the wizard by clicking **Next**.

Figure 10-18: Publishing the Topology



2. Click **Next**.

Figure 10-19: Select Central Management Server



3. Click **Next**.

Figure 10-20: Create Databases

Create databases

The following dedicated databases are part of your topology. Some of the databases listed below have not been created. If you have the appropriate permissions on the SQL Server, you can create the databases when you publish your topology. If you do not have the appropriate permissions, someone with appropriate permissions can create the databases later.

Create the following databases during the publish process:

	Store	Site	Database paths
<input checked="" type="checkbox"/>	ACS-UC-DC.ACS-Unifie...	ACS-2013	Automatically determine database file locat...

Advanced...

Note: Only databases on dedicated SQL Servers can be installed from here. Databases on SQL servers that are collocated with other server components must be installed by running local setup on the machine. Databases for Lync Server 2010 components must be installed by running Install-CsDatabase in the Lync Server 2010 Management Shell.

Help Back Next Cancel



Note: This screen won't be displayed unless you are publishing a topology for the first time.

4. Click **Finish**.

Figure 10-21: Publishing the Topology Completes

Publishing wizard complete

Your topology was successfully published.

Step	Status
✓ Publishing topology ...	Success
✓ Downloading topology...	Success
✓ Downloading global simple URL settings...	Success
✓ Updating role-based access control (RBAC) roles...	Success
✓ Enabling topology...	Success

View Logs

To close the wizard, click Finish.

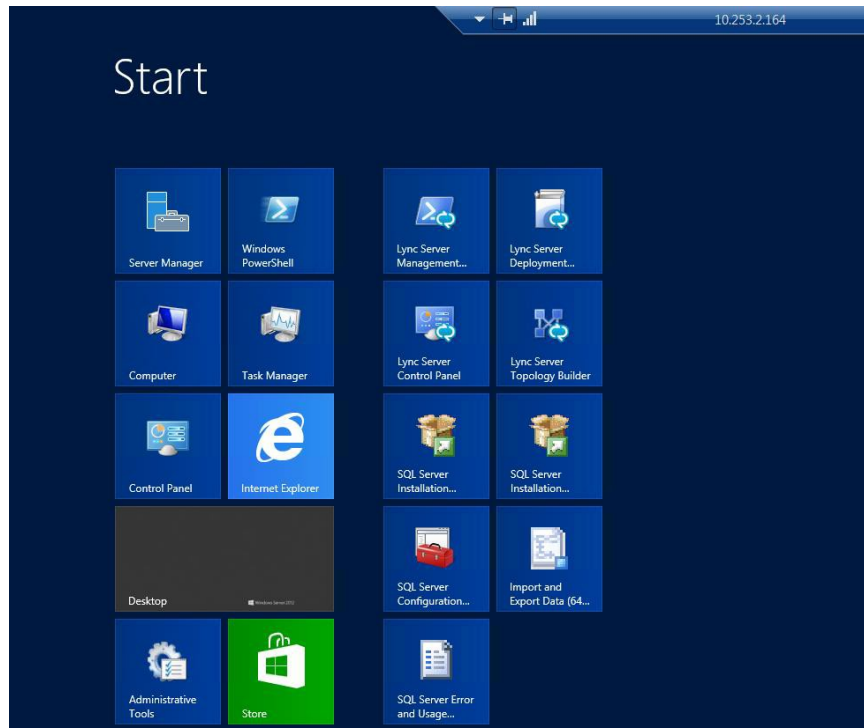
Help Back Finish Cancel

10.5.1.5.2 Running Deployment Wizard

The deployment wizard must be run on both the CloudBond 365 FE and Edge servers. The deployment wizard will implement any changes from the newly published topology.

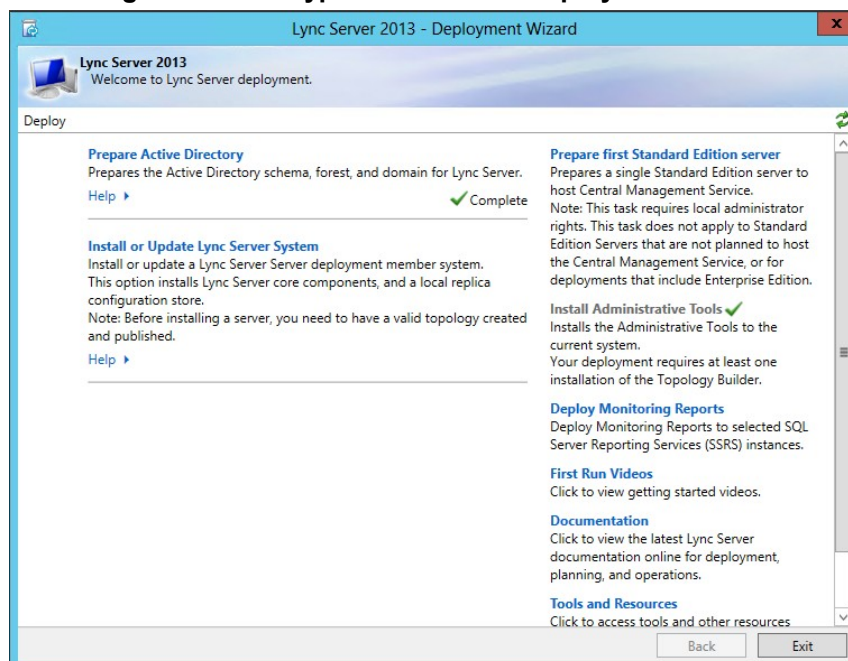
- **To run the Deployment Wizard:**

Figure 10-22: Starting the Deployment Wizard



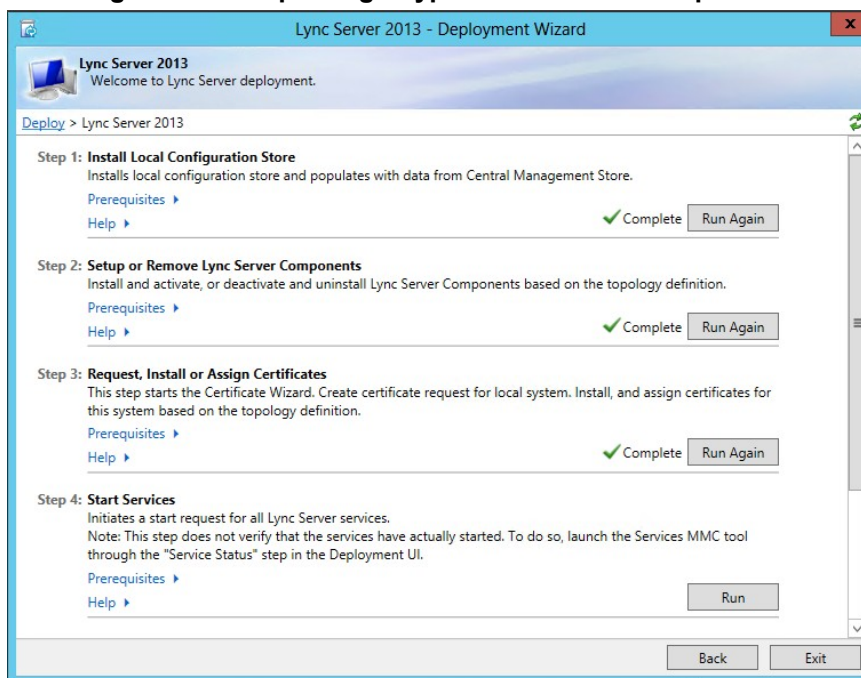
1. **Select Install or Update Lync Server System.**

Figure 10-23: Skype for Business Deployment Wizard



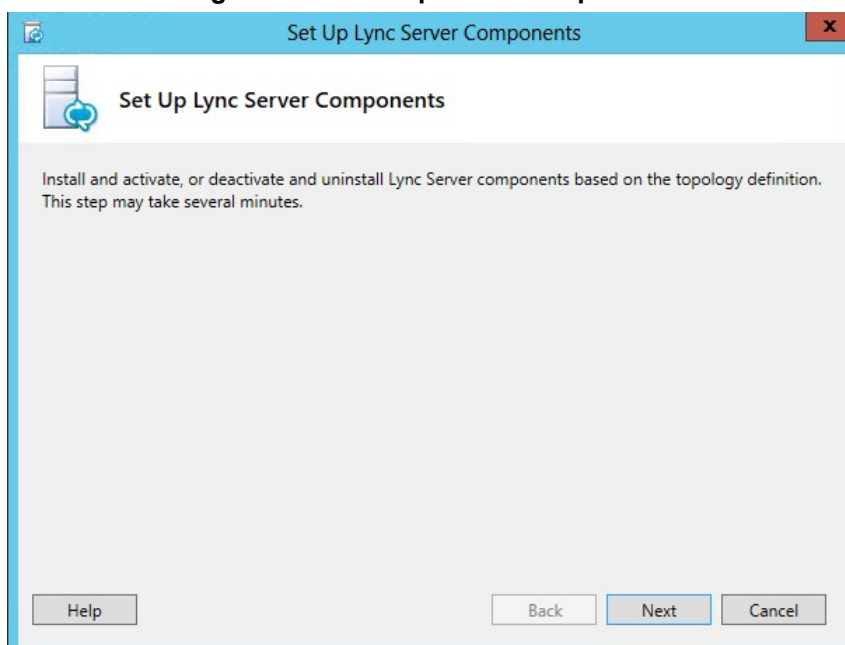
2. Select **Setup or Remove Lync Server Components** and then click **Run Again**.

Figure 10-24: Updating Skype for Business Components



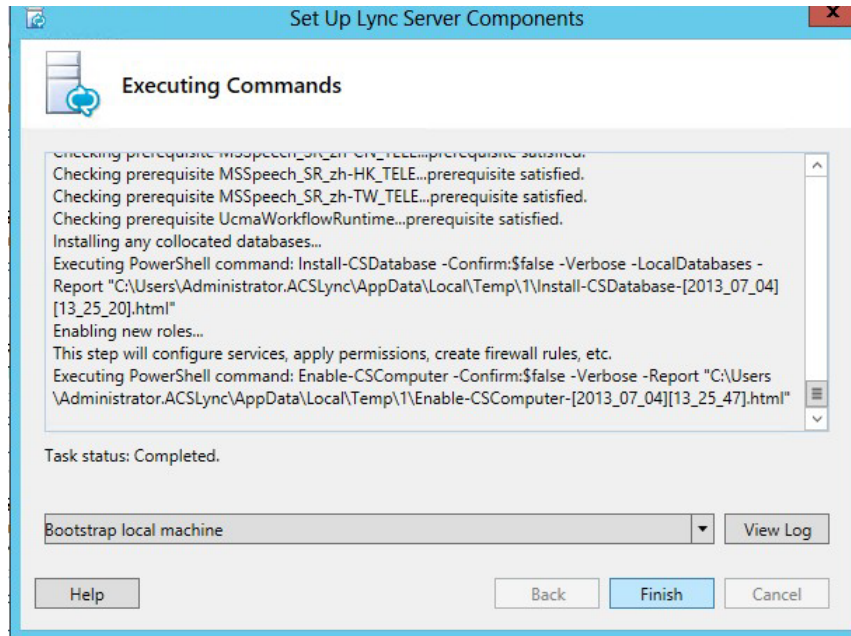
3. Click **Next**.

Figure 10-25: Setup Server Components



4. Click **Finish**.

Figure 10-26: Finishing the Wizard



10.6 Obtaining and Deploying Certificates

There are generally four steps required to Obtain and Deploy certificates for CloudBond 365, regardless of the certificate type and use.

- Generate a Certificate Request (CSR)
- Generate the Certificate (CER)
- Import the certificate (CER)
- Assign the certificate to a Skype for Business role.

10.6.1 Certificate Requests

Generating a private certificate for internal use can be easily accomplished with the Skype for Business Certificate Wizards.

Generating a public certificate request is generally a manual and vendor specific process.

10.6.2 Generating a Certificate

A certificate is actually created by the Certificate Authority.

The process of generating an internal certificate from a certificate request on an internal CA is usually fairly simple, quick, and can be automated.

The process of generating a public certificate from an vendor CA can be complex and time consuming.

10.6.3 Importing the Certificate

Importing the certificate is a simple process through the Skype for Business Certificate Wizard. The process for internal private certificates can be automated.

Importing a public certificate can also be performed through the Skype for Business Certificate Wizard. You may also need to import a certificate chain.

10.6.4 Assigning a Certificate to a Skype for Business Role

This can easily be achieved from the Skype for Business Certificate Wizard.

10.7 Using an Internal Certificate Authority

If a public certificate for internal use is not available, then the easiest way of deploying a resource appliance such as CloudBond 365, is by using internal certificates issued by the enterprise Certificate Authority. These internal certificates are required for the frontend and edge internal services.

Since all domain members in the enterprise forest automatically trust the enterprise forest root CA, then using certificates issued by that CA will allow trust of the CloudBond 365 system.

See Section 10.12.3 on page 206 if an enterprise Certificate Authority is not available.

The CloudBond 365 System is deployed in a resource forest and domain. As the CloudBond 365 servers are not members of the corporate domain, there is no automatic trust of the enterprise domain CA.

If the enterprise Exchange server is installed in the enterprise domain, you will also need to establish trust between the Exchange server and CloudBond 365 using the method below.

10.7.1 How to Trust the Enterprise Root CA

To trust the enterprise CA, its root certificate needs to be added to the “Trusted Root Certification Authorities” environment on all three CloudBond 365 servers (CloudBond 365 Controller, Front-End server, and Edge). To install this root certificate, follow the steps below.

After the CA Root certificate has been deployed to the members of the CloudBond 365 domain, a private certificate can be requested and assigned to each of the CloudBond 365 servers for the internal roles.



Note: Microsoft have recently introduced a new restriction to the certificate store. For a certificate to be placed in the “Trusted Root Certificates”, it must now be a Self-Signed certificate. Previously, any certificate could be stored here, including those from delegated CA’s further down a certificate chain.



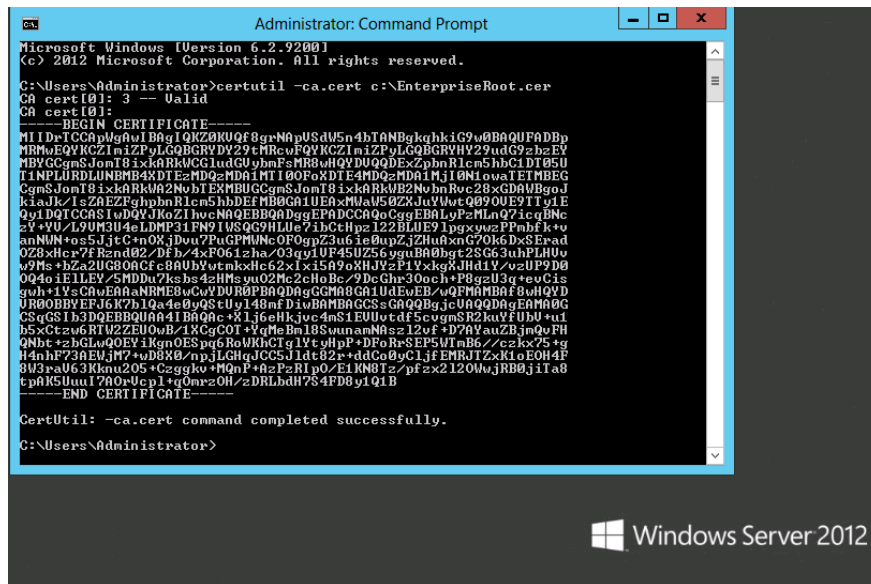
Note: Private Internal Certificates cannot be used for any external connectivity features of CloudBond 365, such as external users, federation, or external conferencing, and mobile clients. A public certificate is required for these features.

10.7.1.1 Obtain the Enterprise Root Certificate

To get the enterprise root certificate, log on to the enterprise Certificate Authority server and issue the following command from a command window:

```
certutil -ca.cert c:\EnterpriseRoot.cer
```

Figure 10-27: Obtaining the CA Root Certificate



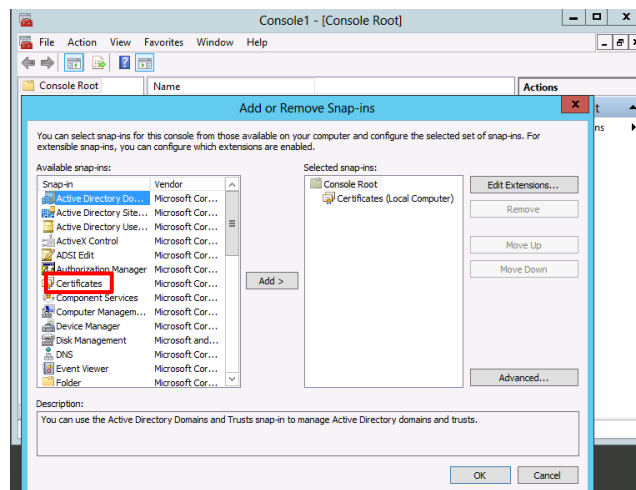
10.7.1.2 Install the Enterprise Root Certificate on CloudBond 365

The procedure below describes how to install the Enterprise Root Certificate on CloudBond 365.

➤ **To install the Enterprise Root Certificate on CloudBond 365:**

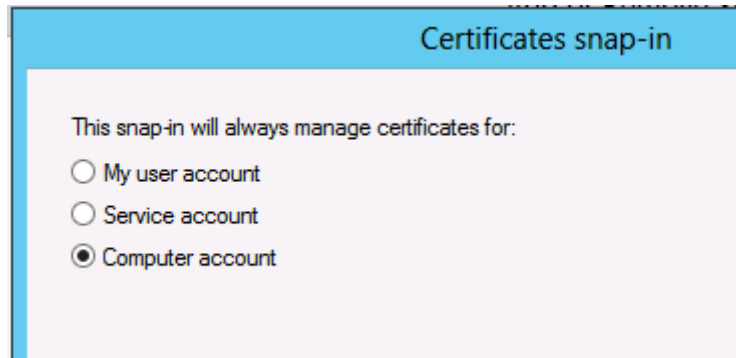
1. Copy the **EnterpriseRoot.cer** file from this server to the CloudBond 365 system and perform the following steps to import the enterprise CA as a trusted authority:
2. Open the MMC utility on all CloudBond 365 Servers (Frontend, Edge, and Controller).
3. Click **File > Add/Remove Snap-in**.
4. Select **Certificates > Add**.

Figure 10-28: Install the Root Certificate – Add or Remove Snap-ins



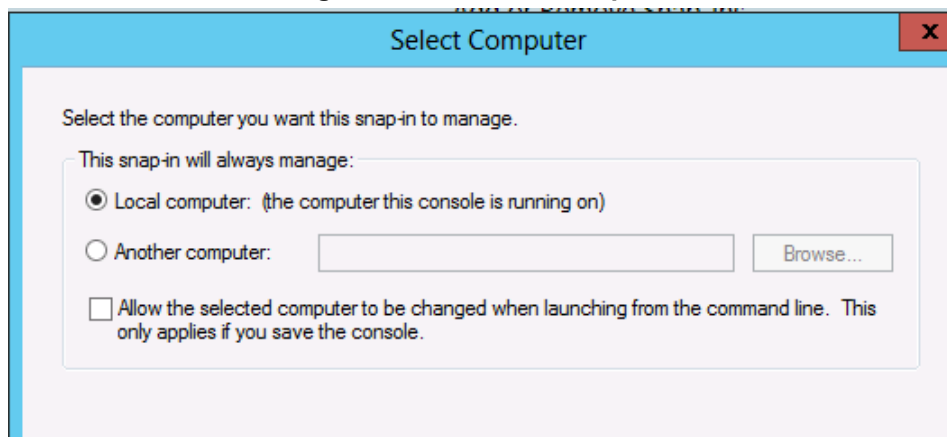
5. Click the **Computer account** option.

Figure 10-29: Install the Root Certificate – Computer Account



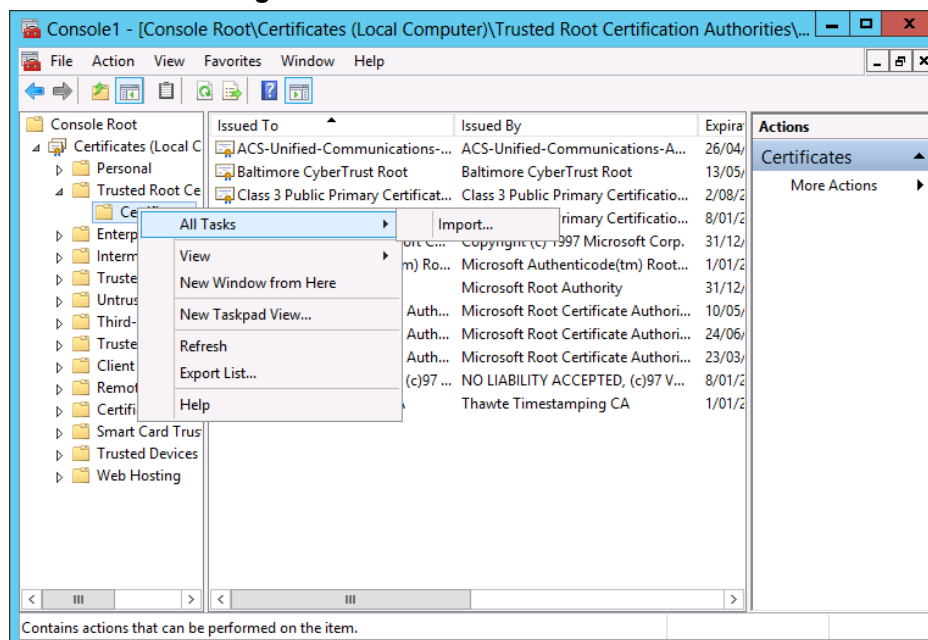
6. Select **Local computer**.

Figure 10-30: Select Computer



7. Click **Finish**, and then click **OK**.
8. Right-click **Trusted Root Certification Authorities > All Tasks** and select **Import**.

Figure 10-31: Trusted Root Certificates



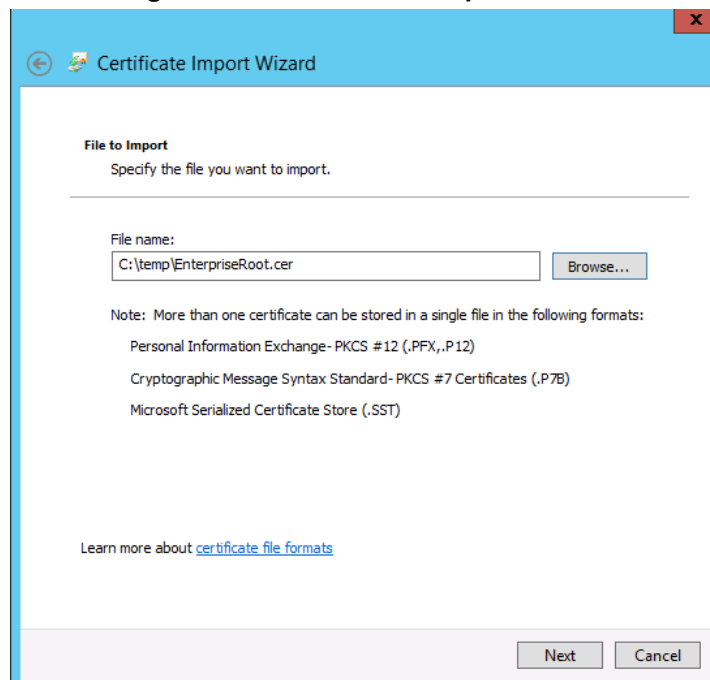
9. Complete the **Certificate Import Wizard**.

Figure 10-32: Importing the Certificate



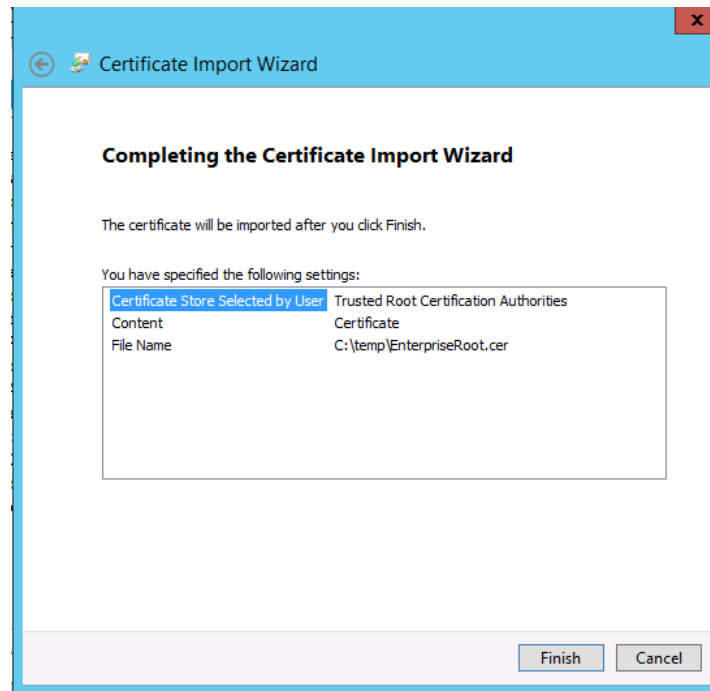
10. Specify the certificate file copied from the Enterprise CA.

Figure 10-33: Certificate Import Wizard



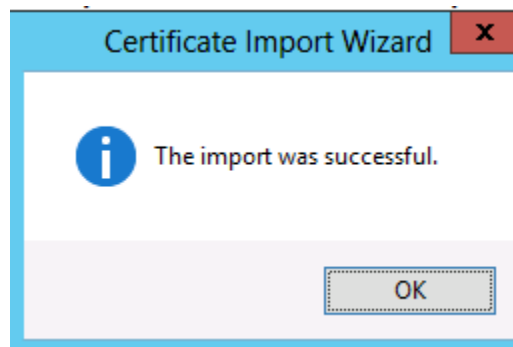
11. Click **Finish**.

Figure 10-34: Completing Certificate Import Wizard



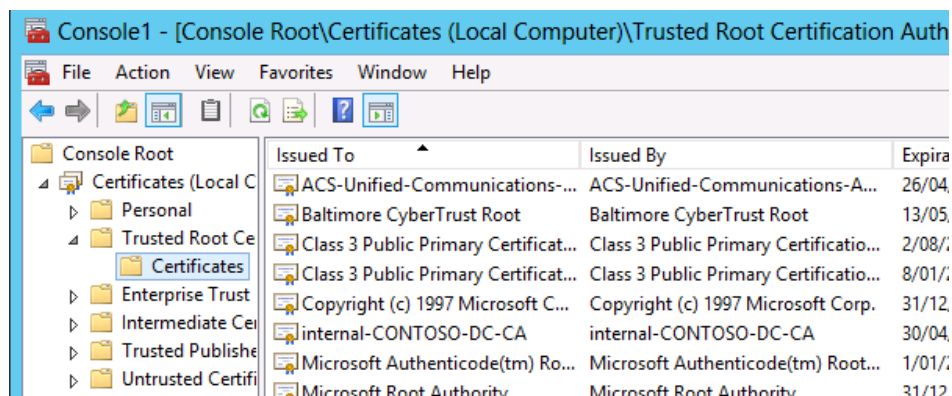
12. Click **OK**.

Figure 10-35: Successful Import



13. The Enterprise root certificate will now appear in the list of trusted root certificates.

Figure 10-36: Trusted Root Certificates



10.8 Skype for Business Certificate Wizards

Skype for Business includes a Certificate Wizard within the Skype for Business Deployment wizard tool, which in some cases, can make the creation of Certificates and their deployment easier, particularly for internal private certificates.

The Skype for Business Certificate Wizards:

- Generate Certificate Requests
- Send Certificate Requests to Certificate Authorities
- Import Certificates
- Assign Certificates to Skype for Business Roles

Skype for Business Roles supported by the Wizard include:

- Front End Internal Web Server Certificates
- Front End External Web Server Certificates
- Edge Server Internal Certificates
- Edge Server External Certificates

The certificate wizard must be run on both FE and Edge servers, and will create at least two separate certificate requests, one or more for each of the servers, and typically one certificate per role.

Certificates can only be assigned to roles running on the server where the Certificate Wizard is run.



Note: It is possible to use a single public certificate for all 4 major Skype for Business roles within CloudBond 365. It is not possible to generate a certificate request for such a single public certificate using the Skype for Business Certificate wizard. However, it is possible to use the Skype for Business Certificate Wizard to import such a certificate and assign Skype for Business roles to that certificate.

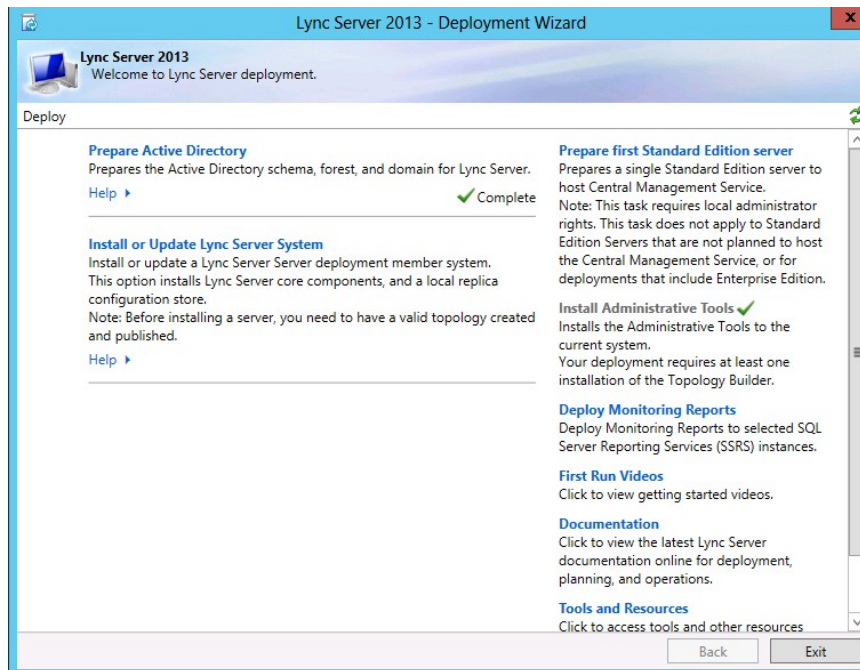
10.8.1 Using the Certificate Wizards

The easiest way to generate a Certificate Request is to use the certificate wizards built in to the Skype for Business Deployment Wizard. These certificate wizards can be used for both internal CAs' and sometimes public CAs'. They can generate separate requests for internal and external certificates. The request summary page can also be used as a guide to the required SAN entries when requesting certificates from a public CA.

10.8.1.1 Accessing the Certificate Wizard

1. Log on to the appropriate server (UC-FE or UC-Edge).
2. Start the Deployment Wizard.
3. Select **Install or Update Skype for Business Server 2015/Lync Server 2013 System**.

Figure 10-37: Skype for Business Deployment Wizard



4. Click the **Run Again** button in **Step 3: Request, Install or Assign Certificates**.

Figure 10-38: Requesting a Certificate



You will see the Certificate Wizard screen similar to one of those below. Expand the Section for the certificate you wish to work with, and select the roles.

- Front End – Server default and Internal Web Services
- Front End – External Web Services
- Edge – Internal
- Edge – External

The OAuthTokenIssuer is used for Microsoft Exchange 2013 integration.

Figure 10-39: Front-End Certificate for Internal Use

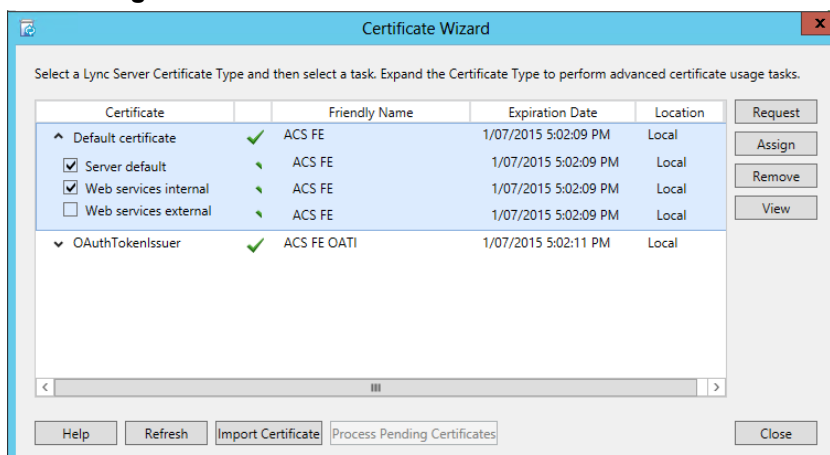
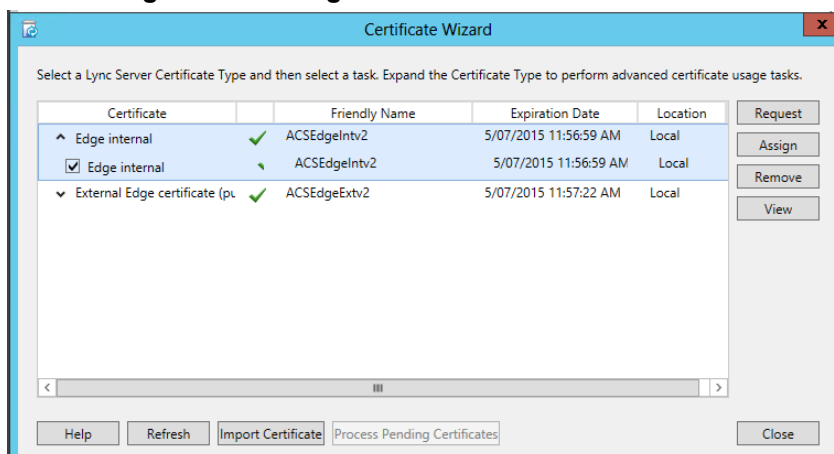


Figure 10-40: Edge Certificate for Internal Use



10.9 Requesting New Internal Certificates

Once the root certificate is added to the trusted root authorities list, it is possible to request new certificates for the CloudBond 365 system Front End and Edge internal roles, from the Enterprise Certificate Authority.

It is common practice to take root CAs' offline, or place them in a secure network, to increase the security and prevent fraudulent issue of certificates.

10.9.1 Enterprise CA Accessible

If the Enterprise Certification Authority can be accessed online, the preferred way will be "Send the request immediately to an online certification authority". Doing so combines and automates part of the certificate request, generation, import, and assignment process.

Requesting a certificate online will result in a window where the name of the enterprise certificate authority can be entered and an automated certificate request processed. The format of a default CA server common name is:

```
<computername>.<FQDN>\<netbios domain name>-<computername>-CA  
(Example: contoso-DC.internal.contoso.com\contoso-contoso-dc-CA)
```



Note: Consult the Enterprise domain administrator for the CA name if required.

10.9.2 Enterprise CA Not Accessible

If the Enterprise Certification Authority is not accessible directly, or you are obtaining a certificate from a public CA, similar steps to those of the wizard below can be used to generate a certificate request file. The request file must be supplied to a Certificate Authority, a certificate generated, and the resulting certificate imported into the Skype for Business Certificate Wizard.



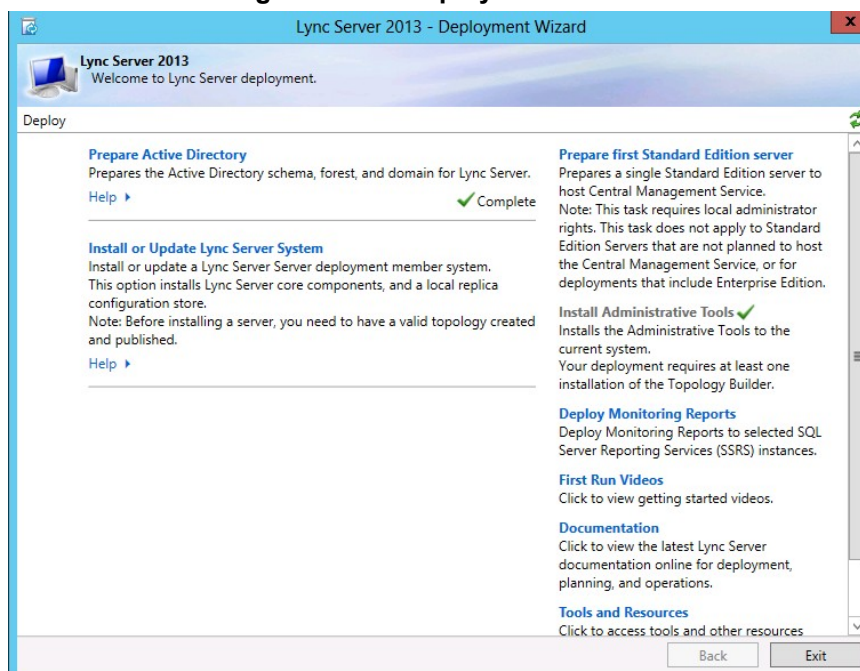
Note: Skype for Business introduced a new Authorization method for server to server communications. This includes a new certificate requirement for an OAuth certificate on the Skype for Business Front End server. This OAuth certificate is only used for communicating with Exchange 2013 and SharePoint 2013, and can also be used with Office 365.

10.9.3 Requesting Certificates (CA Accessible)

10.9.3.1 Generating the Certificate Request

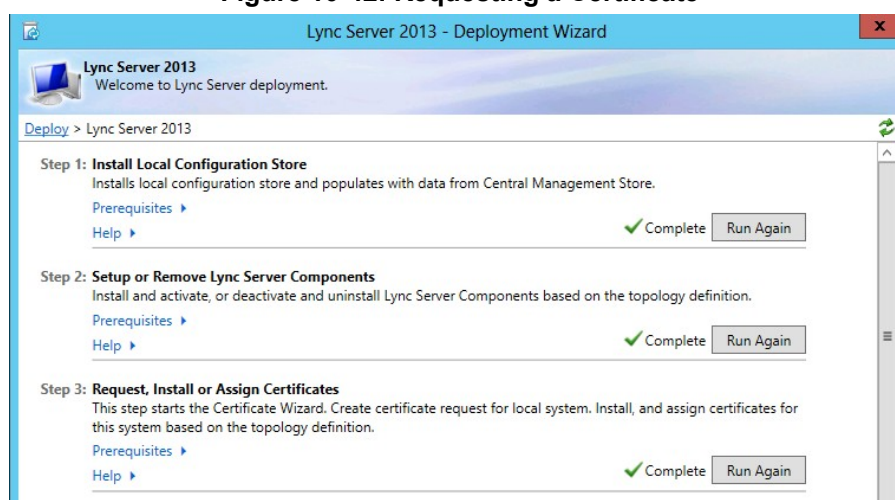
1. Start the Deployment Wizard.
2. Select **Install or Update Lync Server System**.

Figure 10-41: Deployment Wizard



3. Click the **Run Again** button in **Step 3: Request, Install or Assign Certificates**.

Figure 10-42: Requesting a Certificate



4. Expand the Default Certificate and ensure the appropriate roles are selected. Click **Request**.

Figure 10-43: Front-End Certificate for Internal Use

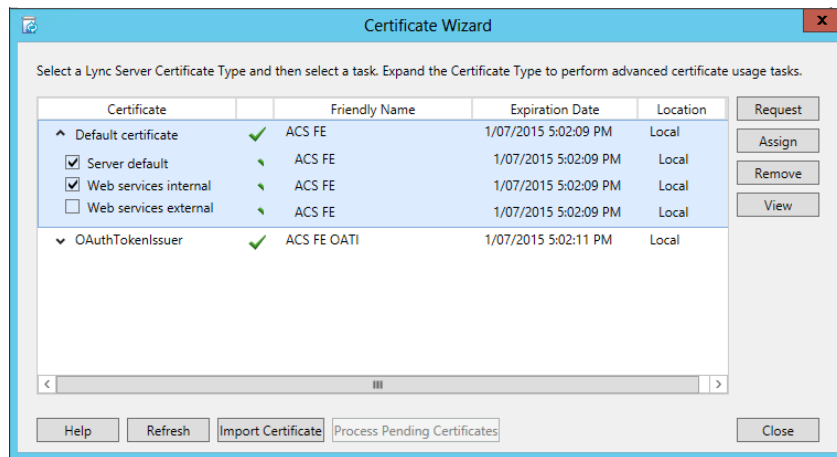
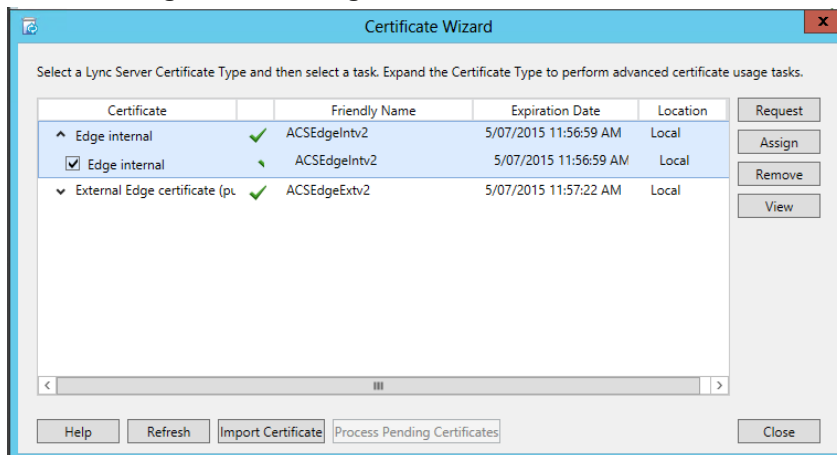
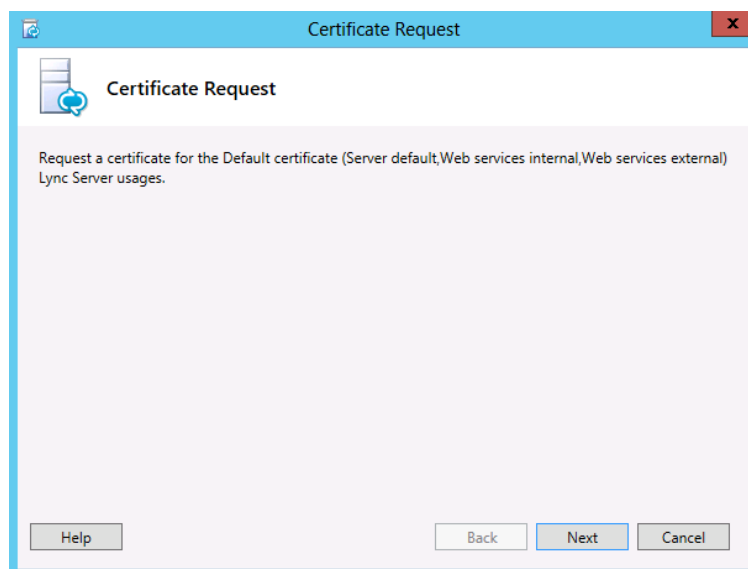


Figure 10-44: Edge Certificate for Internal Use



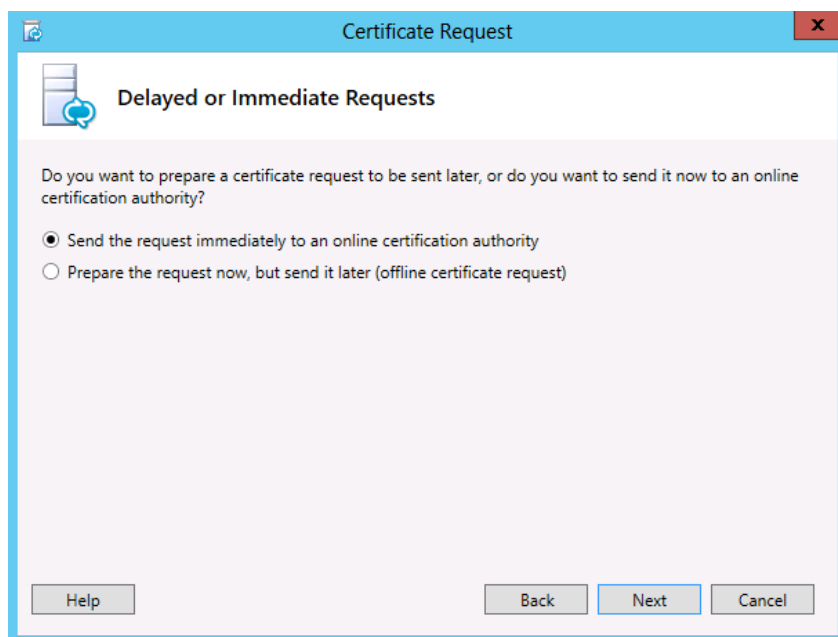
5. Complete the Wizard.

Figure 10-45: Certificate Request



6. Select **Send the request immediately**.

Figure 10-46: Delayed or Immediate Requests

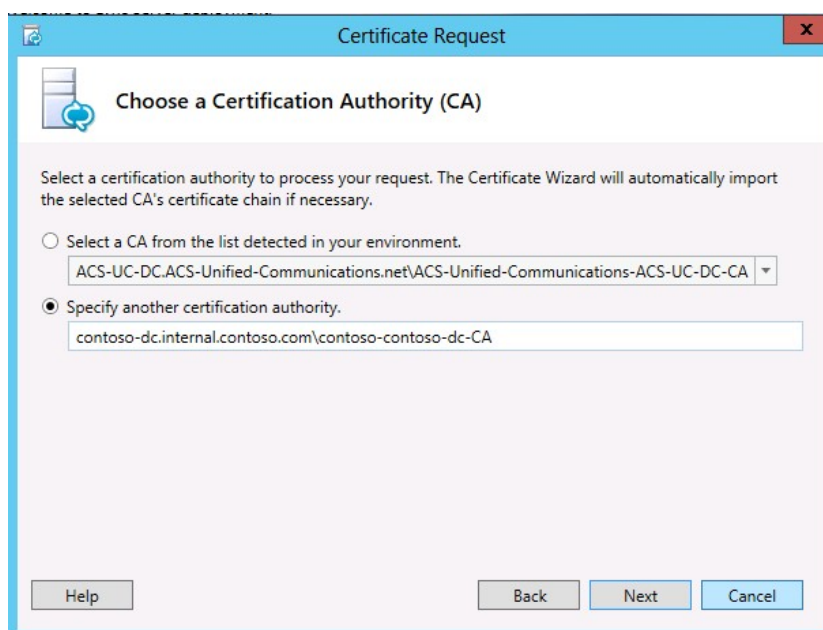


The dialog box is titled 'Certificate Request' and contains the following elements:

- Title Bar:** 'Certificate Request' with a close button (X).
- Icon:** A blue icon representing a document with a circular arrow.
- Section Header:** 'Delayed or Immediate Requests'.
- Text:** 'Do you want to prepare a certificate request to be sent later, or do you want to send it now to an online certification authority?'
- Options:**
 - ☒ Send the request immediately to an online certification authority
 - ☐ Prepare the request now, but send it later (offline certificate request)
- Buttons:** 'Help', 'Back', 'Next' (highlighted), and 'Cancel'.

7. Specify the Enterprise CA.

Figure 10-47: Creating Certificate Requests



The dialog box is titled 'Certificate Request' and contains the following elements:

- Title Bar:** 'Certificate Request' with a close button (X).
- Icon:** A blue icon representing a document with a circular arrow.
- Section Header:** 'Choose a Certification Authority (CA)'.
- Text:** 'Select a certification authority to process your request. The Certificate Wizard will automatically import the selected CA's certificate chain if necessary.'
- Options:**
 - ☐ Select a CA from the list detected in your environment.
Dropdown menu: ACS-UC-DC.ACS-Unified-Communications.net\ACS-Unified-Communications-ACS-UC-DC-CA
 - ☒ Specify another certification authority.
Text box: contoso-dc.internal.contoso.com\contoso-contoso-dc-CA
- Buttons:** 'Help', 'Back', 'Next', and 'Cancel'.

8. Enter Enterprise Domain credentials.

Figure 10-48: Certification Authority Account

Certificate Request

Certification Authority Account

☒ Specify alternate credentials for the certification authority.

User name:
administrator

Password:
.....

Help Back Next Cancel

9. Click **Next**.

Figure 10-49: Specify Alternate Certificate Template

Certificate Request

Specify Alternate Certificate Template

By default a Lync Server certificate request will use the WebServer certificate template. To specify a different certificate template, select the following check box.

☐ Use alternate certificate template for the selected certification authority

Certificate template name:
.....

Note: The custom template must be installed on the certification authority (CA), and must meet the requirements for Lync Server certificates.

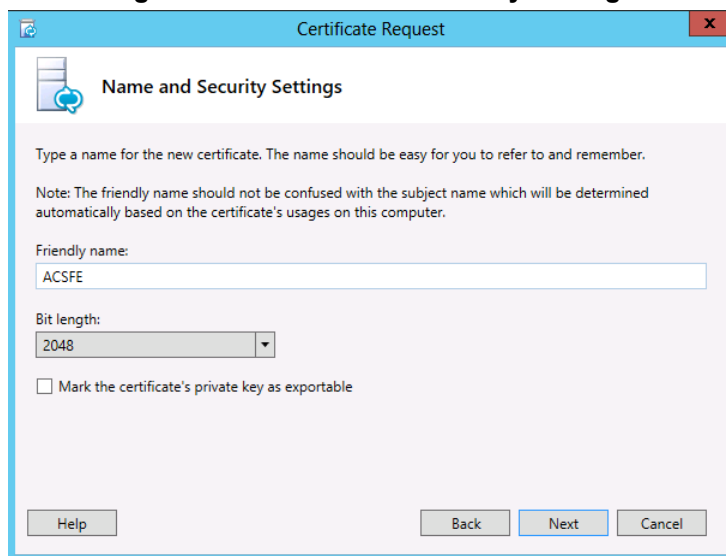
The template name must be specified, which may differ from the template display name.

For details about custom certificate templates, see the product documentation.

Help Back Next Cancel

10. Enter a friendly name, and then click **Next**

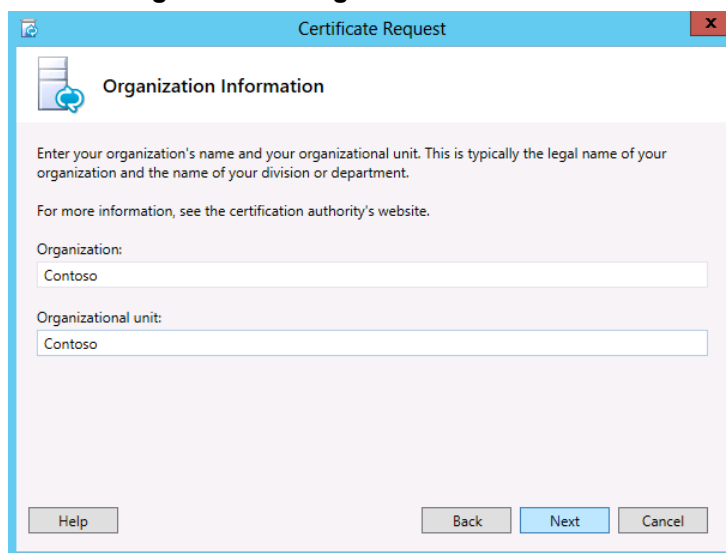
Figure 10-50: Name and Security Settings



The screenshot shows a Windows-style dialog box titled 'Certificate Request'. The main heading is 'Name and Security Settings'. Below the heading, there is a text box for 'Friendly name' containing the text 'ACSFE'. Below that is a 'Bit length' dropdown menu set to '2048'. There is an unchecked checkbox labeled 'Mark the certificate's private key as exportable'. At the bottom, there are four buttons: 'Help', 'Back', 'Next' (highlighted in blue), and 'Cancel'.

11. Enter the organization details, and then click **Next**

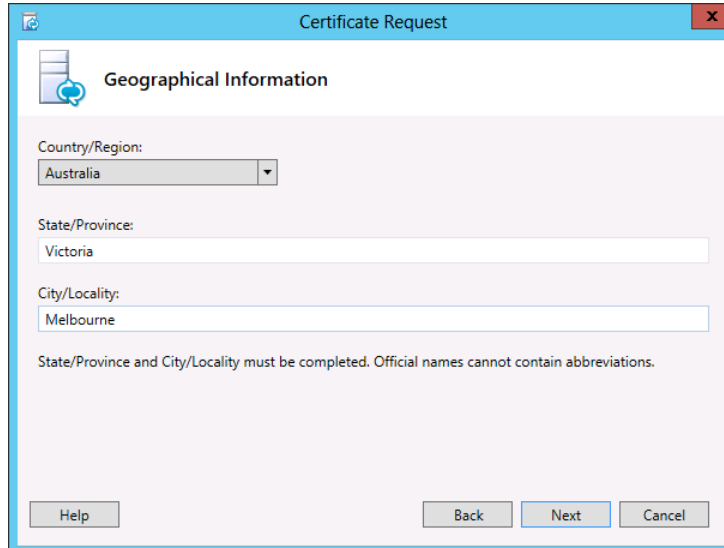
Figure 10-51: Organization Information



The screenshot shows the same 'Certificate Request' dialog box, but the 'Organization Information' tab is selected. It contains text boxes for 'Organization' and 'Organizational unit', both containing the text 'Contoso'. At the bottom, there are four buttons: 'Help', 'Back', 'Next' (highlighted in blue), and 'Cancel'.

12. Enter the Geographical information, and then click **Next**.

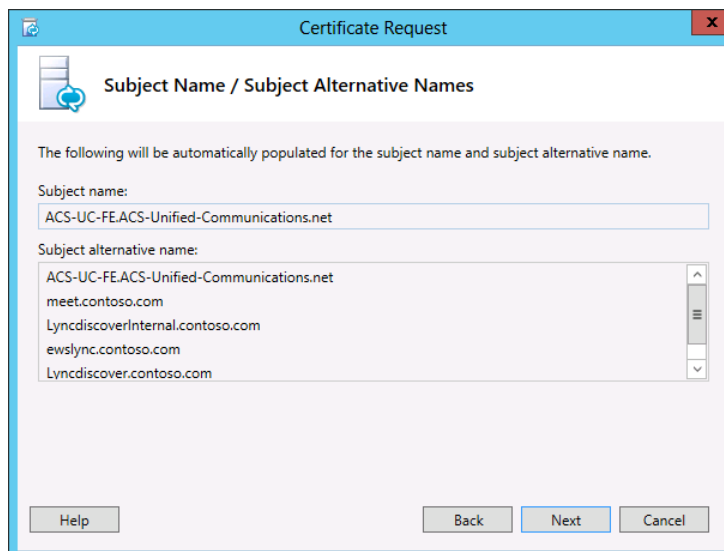
Figure 10-52: Geographical Information



The screenshot shows a window titled "Certificate Request" with a sub-header "Geographical Information". It contains three input fields: "Country/Region:" with a dropdown menu showing "Australia", "State/Province:" with a text box containing "Victoria", and "City/Locality:" with a text box containing "Melbourne". Below these fields is a note: "State/Province and City/Locality must be completed. Official names cannot contain abbreviations." At the bottom are buttons for "Help", "Back", "Next", and "Cancel".

13. Take note of the generated Subject and SAN names. On the FE, they will match both internal domain names of the server, as well as the Skype for Business simple URL's for the SIP domains.

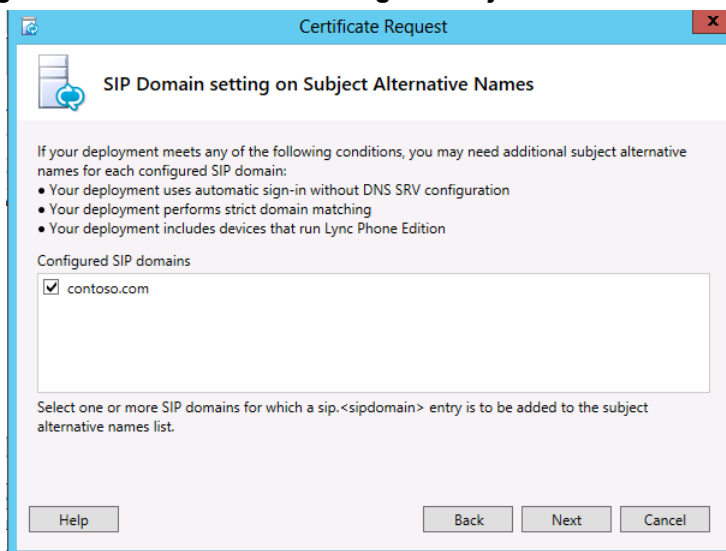
Figure 10-53: Subject Name / Subject Alternative Names



The screenshot shows a window titled "Certificate Request" with a sub-header "Subject Name / Subject Alternative Names". It contains a message: "The following will be automatically populated for the subject name and subject alternative name." Below this is a "Subject name:" field with the value "ACS-UC-FE.ACS-Unified-Communications.net". Underneath is a "Subject alternative name:" list box containing the following entries: "ACS-UC-FE.ACS-Unified-Communications.net", "meet.contoso.com", "LyncdiscoverInternal.contoso.com", "ewslync.contoso.com", and "Lyncdiscover.contoso.com". At the bottom are buttons for "Help", "Back", "Next", and "Cancel".

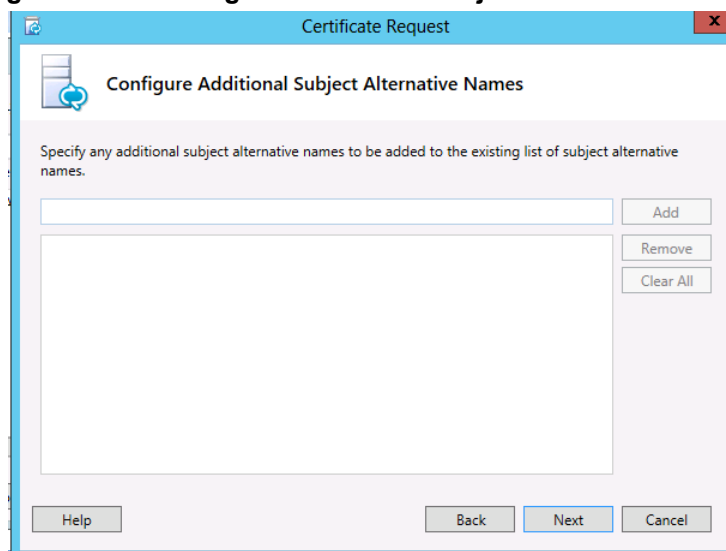
14. Enable any SIP domains, and then click **Next**

Figure 10-54: SIP Domain Setting on Subject Alternative Names



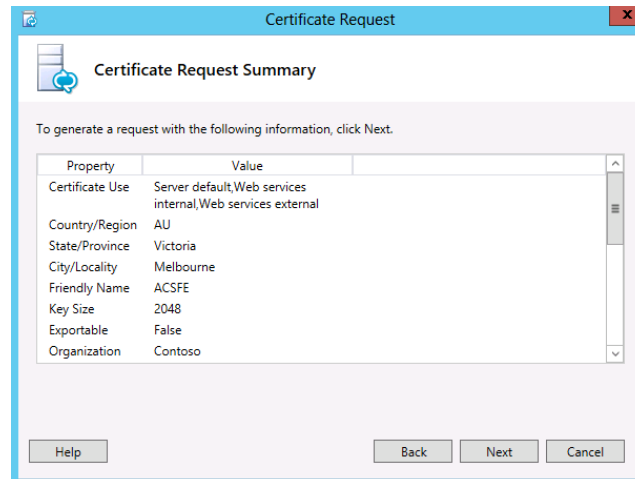
15. Configure additional subject alternative names, and then click **Next**.

Figure 10-55: Configure Additional Subject Alternative Names



16. Click **Next**.

Figure 10-56: Certificate Request Summary



The dialog box titled "Certificate Request" shows a "Certificate Request Summary" section. It contains a table with the following properties and values:

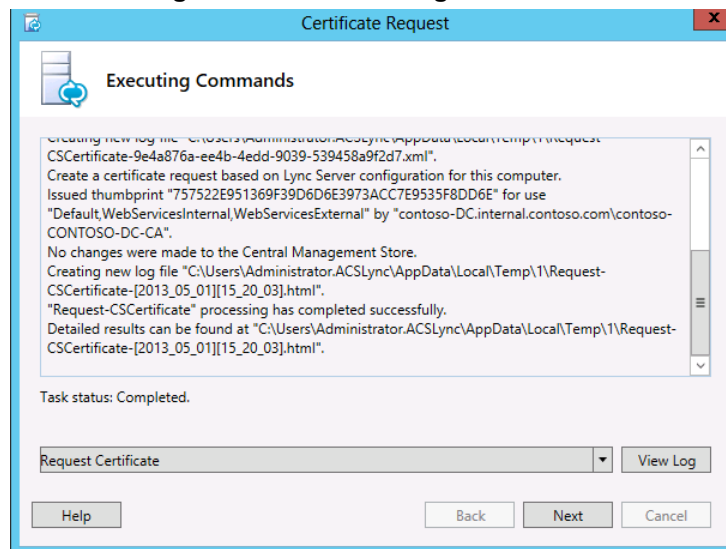
Property	Value
Certificate Use	Server default, Web services internal, Web services external
Country/Region	AU
State/Province	Victoria
City/Locality	Melbourne
Friendly Name	ACSFE
Key Size	2048
Exportable	False
Organization	Contoso

Below the table are buttons for "Help", "Back", "Next", and "Cancel".

10.9.3.2 Generating and Installing the Certificate

The certificate request is sent to the nominated CA, where a matching Certificate is generated. The Certificate is returned to the requestor and imported automatically as part of the process.

Figure 10-57: Executing Commands



The dialog box titled "Certificate Request" shows an "Executing Commands" section. It displays the following text:

```

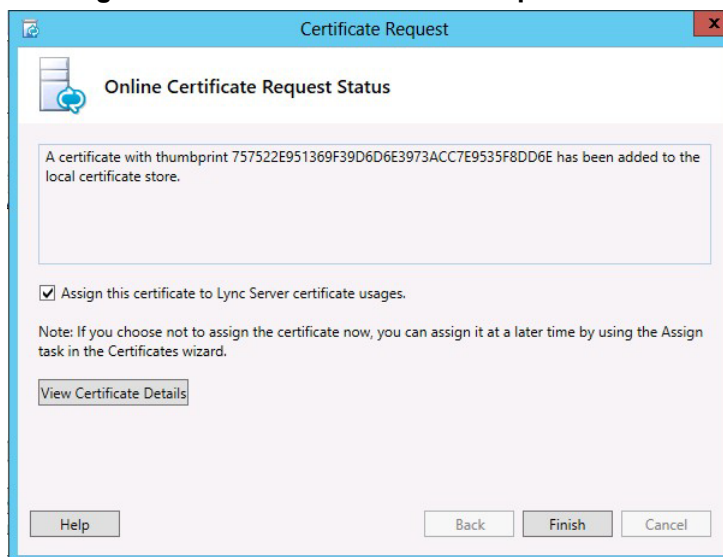
Creating new log file "C:\Users\Administrator\ACSLync\AppData\Local\Temp\1\request-
CSCertificate-9e4a876a-ee4b-4edd-9039-539458a9f2d7.xml".
Create a certificate request based on Lync Server configuration for this computer.
Issued thumbprint "757522E951369F39D6D6E3973ACC7E9535F8DD6E" for use
"Default, WebServicesInternal, WebServicesExternal" by "contoso-DC.internal.contoso.com\contoso-
CONTOSO-DC-CA".
No changes were made to the Central Management Store.
Creating new log file "C:\Users\Administrator\ACSLync\AppData\Local\Temp\1\request-
CSCertificate-[2013_05_01][15_20_03].html".
"Request-CSCertificate" processing has completed successfully.
Detailed results can be found at "C:\Users\Administrator\ACSLync\AppData\Local\Temp\1\request-
CSCertificate-[2013_05_01][15_20_03].html".
    
```

Below the text, it says "Task status: Completed." and there is a "View Log" button. At the bottom, there is a dropdown menu showing "Request Certificate" and buttons for "Help", "Back", "Next", and "Cancel".

The certificate has now been generated and imported into the server certificate store.

10.9.3.3 Assign the Certificate to a Skype for Business Role

1. Ensure **Assign this certificate to Skype for Business certificate usages** is selected for the wizard to continue.

Figure 10-58: Online Certificate Request Status

2. Continue the wizard to automatically assign the certificate to the Skype for Business roles on the server.

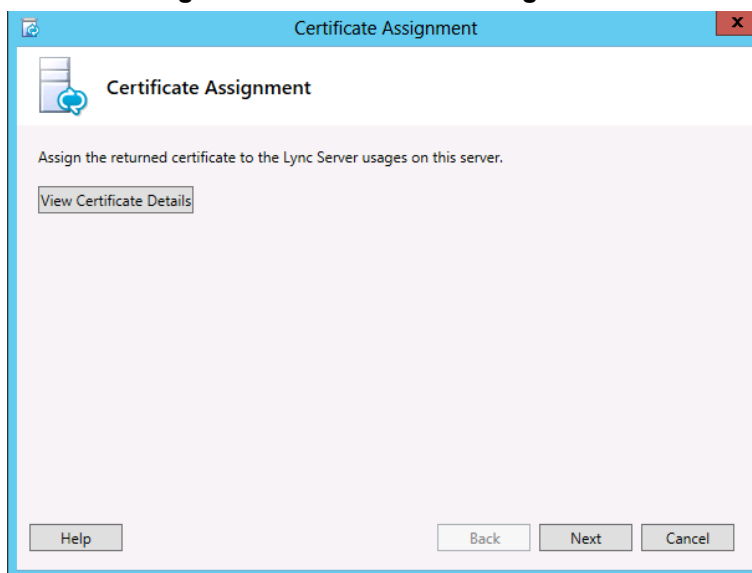
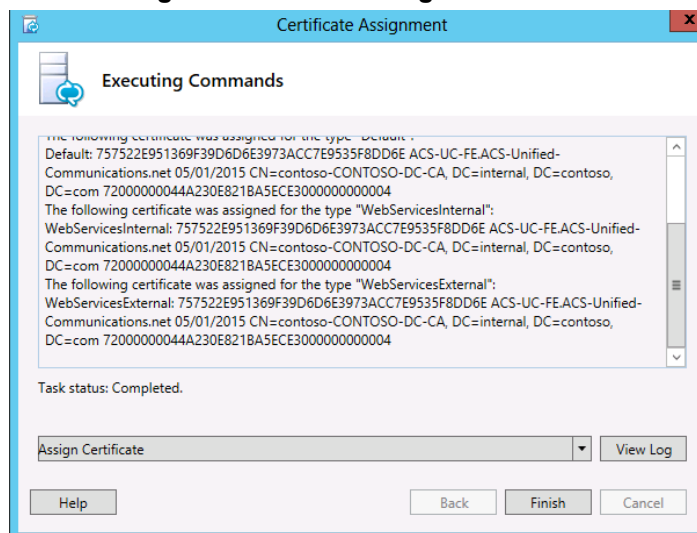
Figure 10-59: Certificate Assignment

Figure 10-60: Executing Commands



3. Repeat the above steps on the CloudBond 365 Edge server internal network to assign an Enterprise CA certificate.

10.9.4 Requesting Certificates (CA is Not Available)

This section describes how to request certificates when the CA is not available.

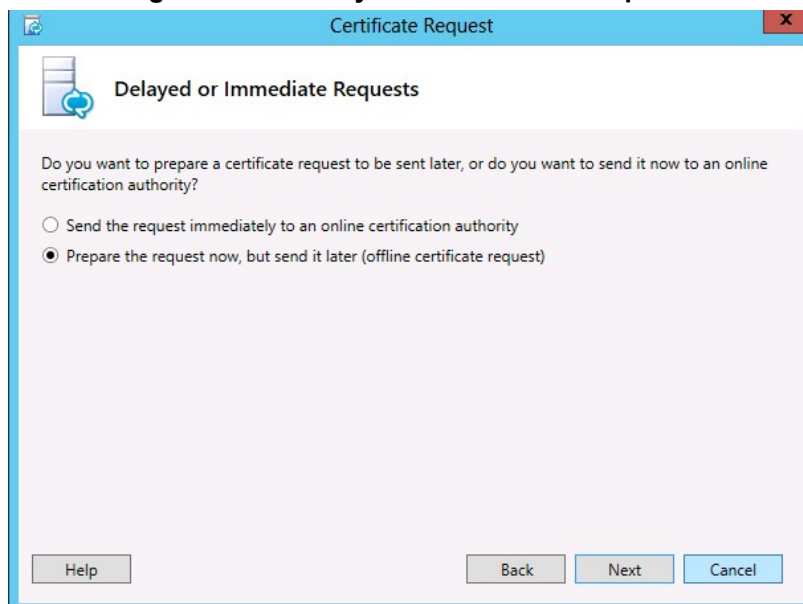
10.9.4.1 Generating the Certificate Request

If the Enterprise Certificate Authority is not available, or a public certificate is to be used, the steps for producing a certificate request, generating the certificate, and then importing and assigning the certificate are shown below. The examples are for the CloudBond 365 Edge internal certificate.

Many of these steps are similar to the previous wizard for requesting a certificate.

➤ To generate the Certificate Request:

1. Start the Skype for Business Deployment Wizard.
2. Select **Install or Update Skype for Business Server 2015\Lync Server 2013 System**.
3. Click the **Run Again** button in Step 3: Request, Install or Assign Certificates.
4. Click **Request** and complete the wizard.
5. Select **Prepare the request now**, however send it later.

Figure 10-61: Delayed or Immediate Requests

6. Specify a file name to store the certificate request.

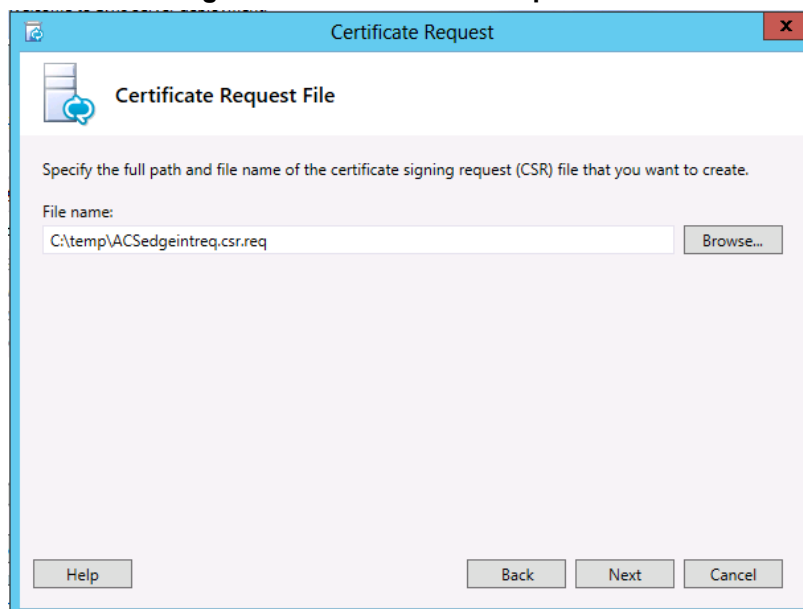
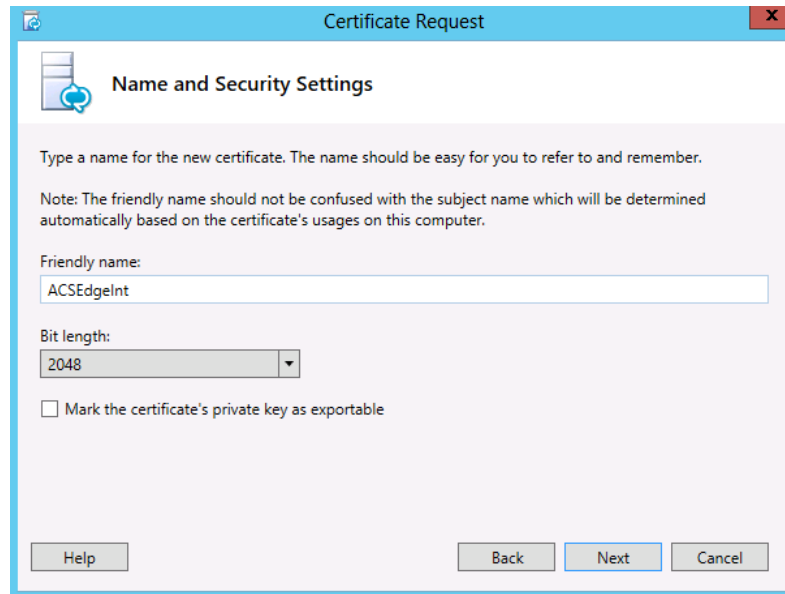
Figure 10-62: Certificate Request File

Figure 10-63: Name and Security Settings



7. Enter organization details.
8. Take note of the generated Subject and SAN names On the FE, they will match both internal domain names of the server, as well as the Skype for Business simple URL's for the SIP domains.
9. Enable any SIP domains.
10. The wizard will complete, generating a certificate request file.

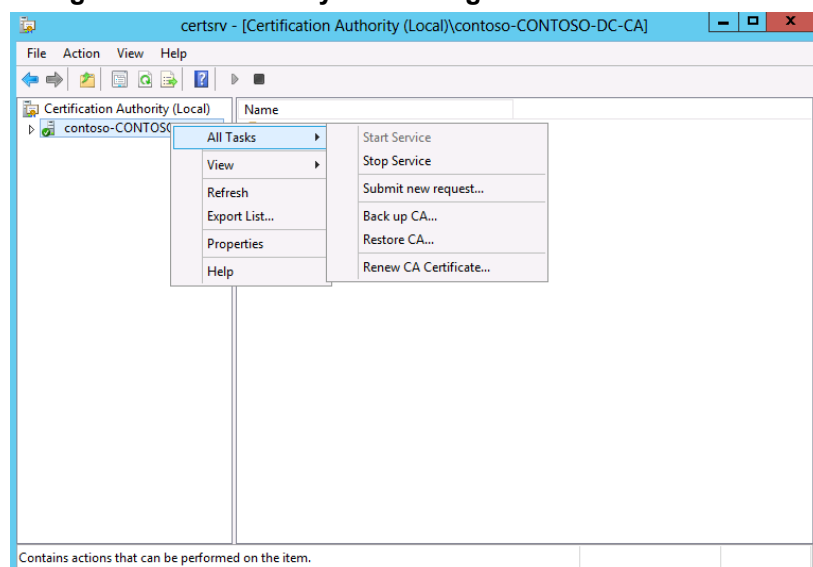
10.9.4.2 Generating the Certificate

The procedure below describes how to generate the certificate.

➤ **To generate the certificate:**

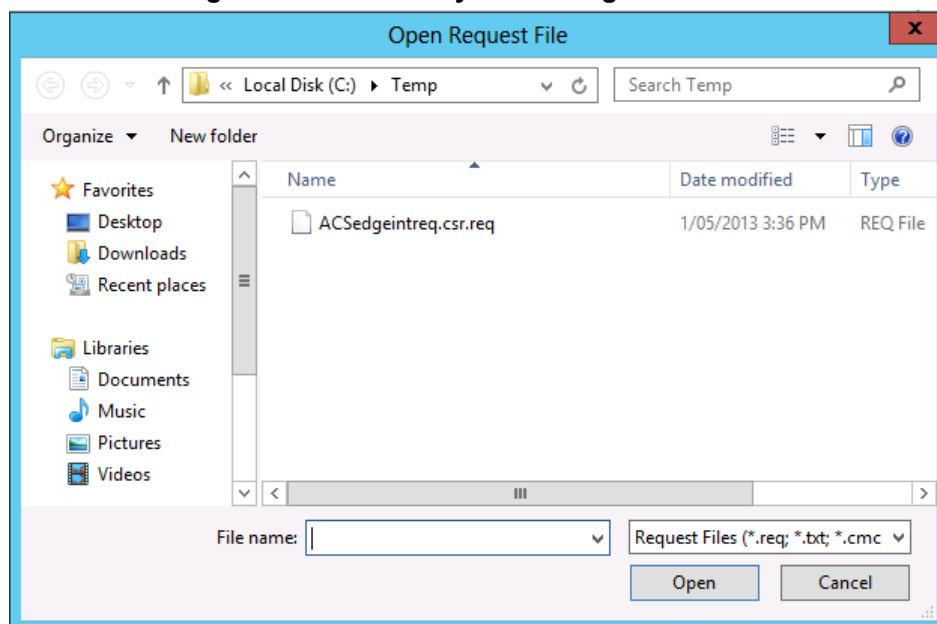
1. Copy the Certificate Signing Request File that was just created to the enterprise Certification Authority server and start the Certificate Authority management console.
2. Right-click the server and select **All Tasks** -> **Submit new request**.

Figure 10-64: Manually Generating a Certificate – All Tasks



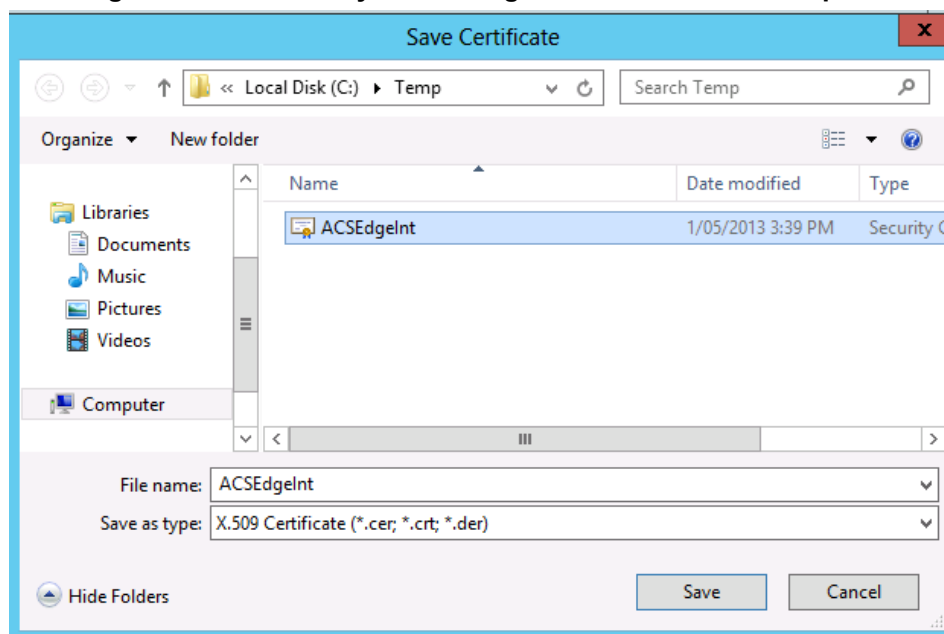
3. Open the request file and click **Open**.

Figure 10-65: Manually Generating a Certificate



4. A similar window appears to save the requested certificate.

Figure 10-66: Manually Generating a Certificate – Save Request



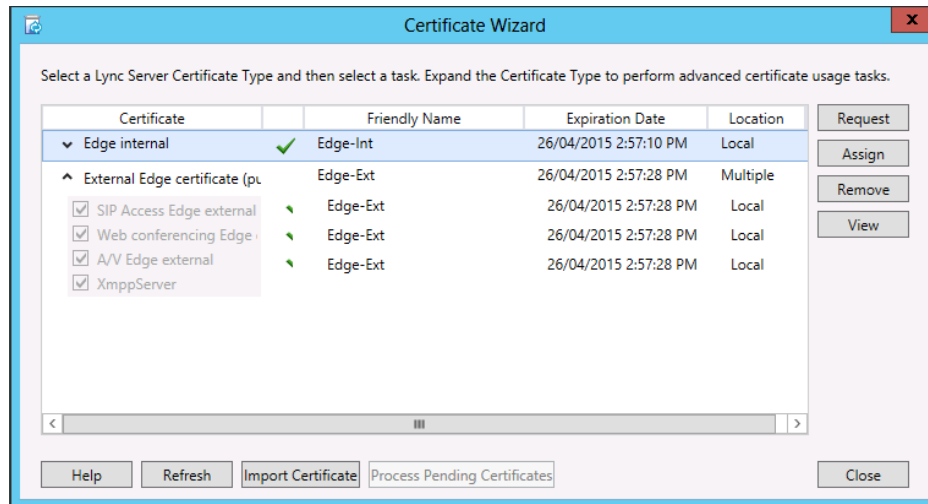
10.9.4.3 Installing the Certificate on the CloudBond 365 Server

The procedure below describes how to install the certificate on the CloudBond 365 Server.

➤ **To install the certificate on the CloudBond 365 Server:**

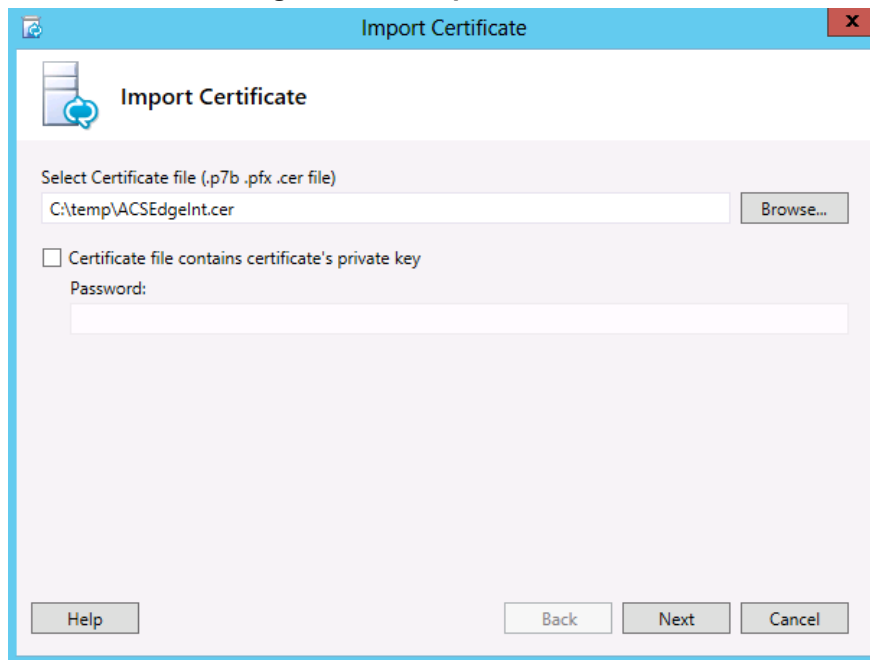
1. Copy the generated .cer file back to the CloudBond 365 system.
2. In the **Skype for Business Certificate Wizard**, select **Import Certificate** to import the just created Certificate file.

Figure 10-67: Certificate Wizard

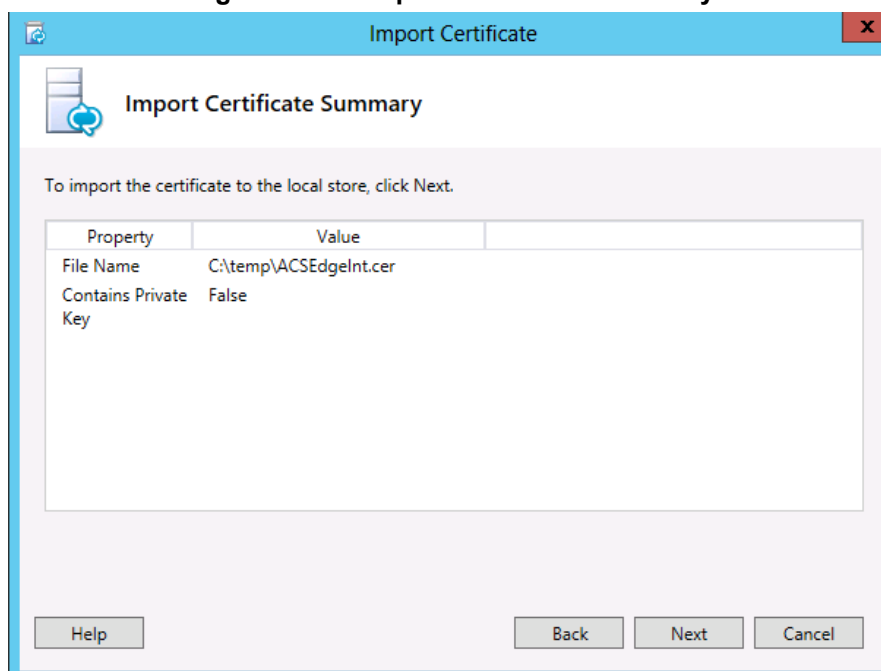


3. Specify the certificate file copied from the CA, and then click **Next**.

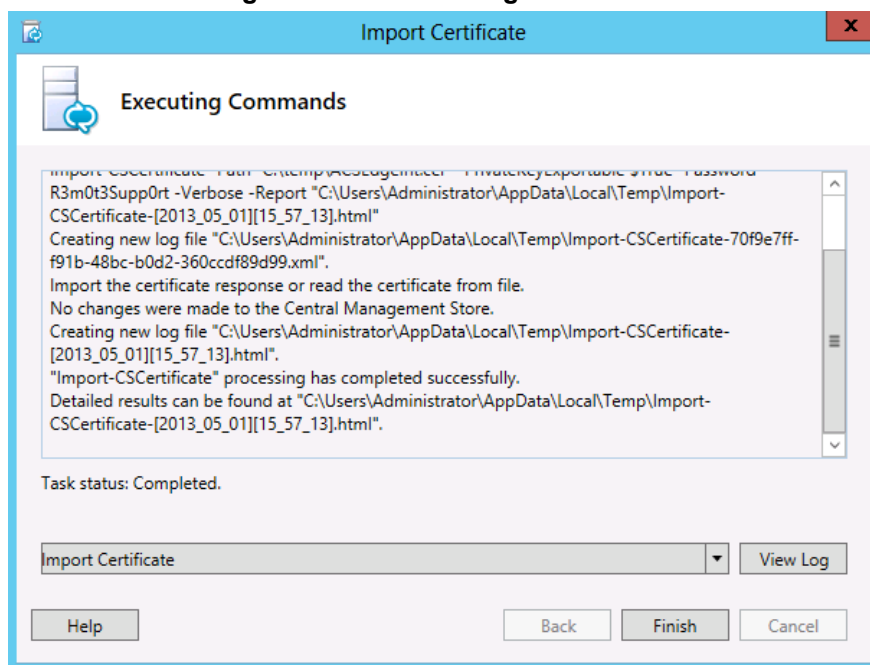
Figure 10-68: Import Certificate



4. Click **Next**.

Figure 10-69: Import Certificate Summary

5. Click **Finish**.

Figure 10-70: Executing Commands

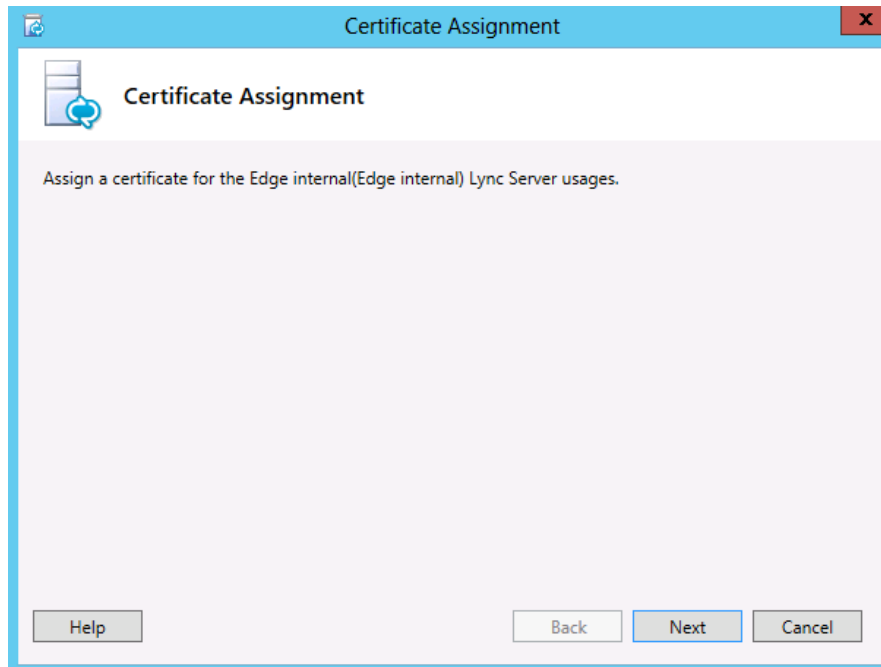
10.9.4.4 Assign the Certificate to a Skype for Business Role

The imported certificate must now be assigned to a Skype for Business Role.

➤ **To assign the Certificate to a Skype for Business Role:**

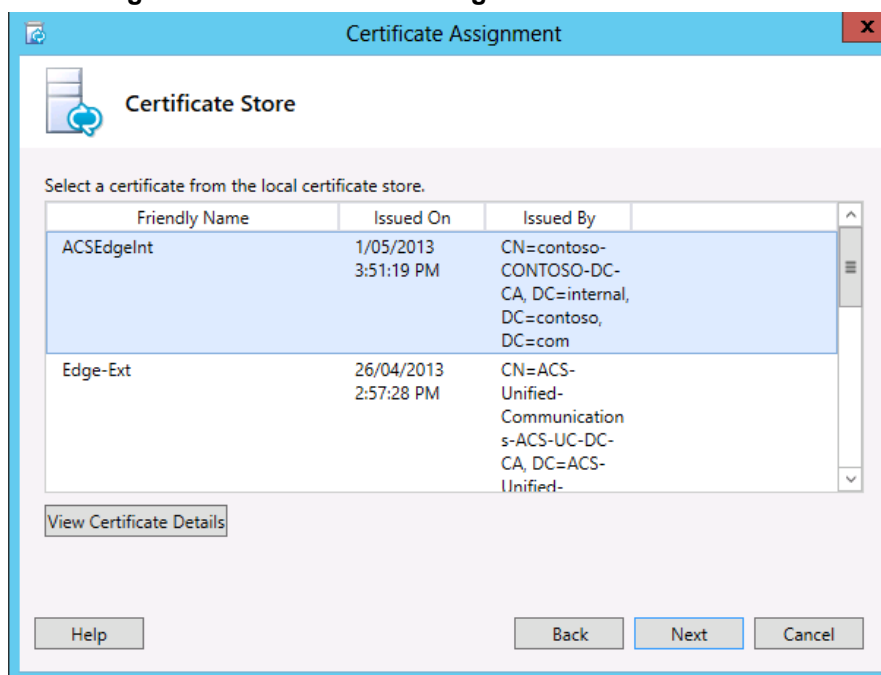
1. Once the certificate has been imported, highlight the Skype for Business role for the certificate (Edge Internal) then select **Assign**.

Figure 10-71: Certificate Assignment



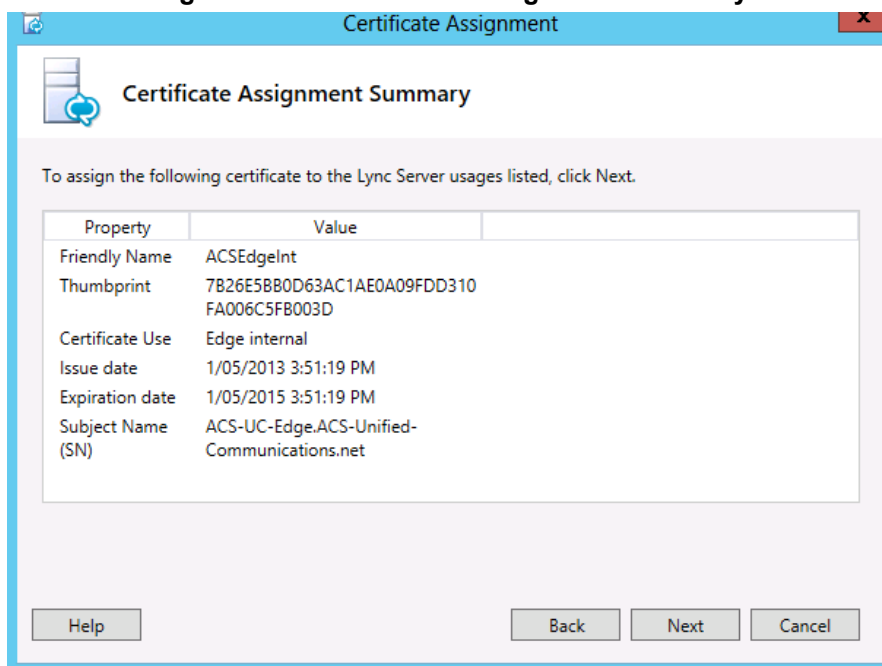
2. Select the certificate just imported to the certificate store.

Figure 10-72: Certificate Assignment – Certificate Store



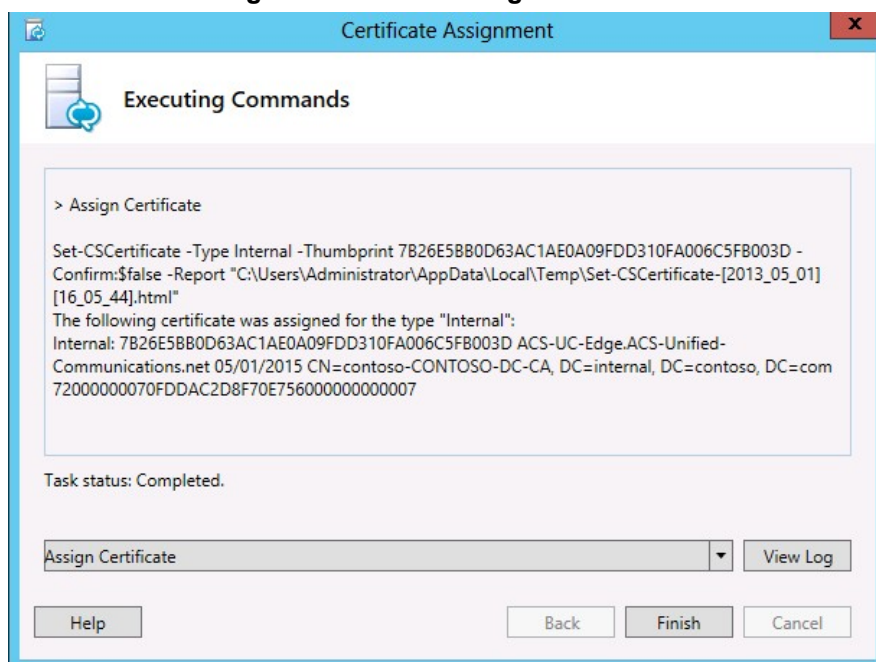
3. If your certificate does not appear in the list, then the certificate is not suitable for assigning to the chosen roles.
4. Click **Next**.

Figure 10-73: Certificate Assignment Summary



5. Click **Finish**.

Figure 10-74: Executing Commands



6. Click **Close** to close the certificate wizard, followed by **exit** to close the deployment wizard.
7. Ensure the steps above have been performed for both the CloudBond 365 Frontend and for the CloudBond 365 Edge server for the Edge internal certificate.

10.10 Requesting External Certificates

Depending upon your chosen Public Certificate vendor, you may be able to provide Certificate Request files in their application process. Many vendors however require you to use their proprietary Certificate Request data entry tools.

Regardless of the vendors requirements, it is often useful to use the Skype for Business Certificate Wizards to at least confirm the required contents of your public certificates. The certificate wizards use the completed topology to generate certificate requests, and also to install the certificate and assign it to roles within Skype for Business.

The certificate wizard must be run on both FE and Edge servers, and will create two separate certificate requests, one for each of the servers.



Warning: You cannot create a request for the minimum SAN certificate using the certificate wizard.

- The wizard, when run on the FE server will automatically include SAN entries for LyncDiscover for each SIP domain.
- The wizard, when run on the Edge server, will automatically include SAN entries for each SIP domain required for XMPP (PIC) integration unless specifically excluded.

The certificate requests cannot be combined into a single request.

Figure 10-75: Front-End certificate for External (Public) use via Reverse Proxy

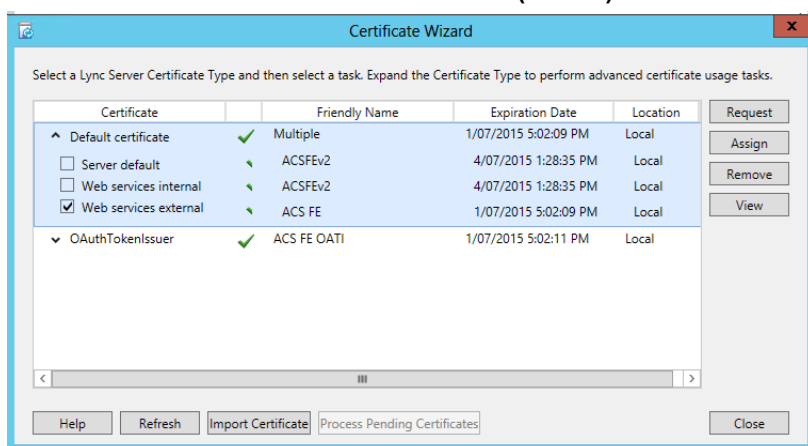
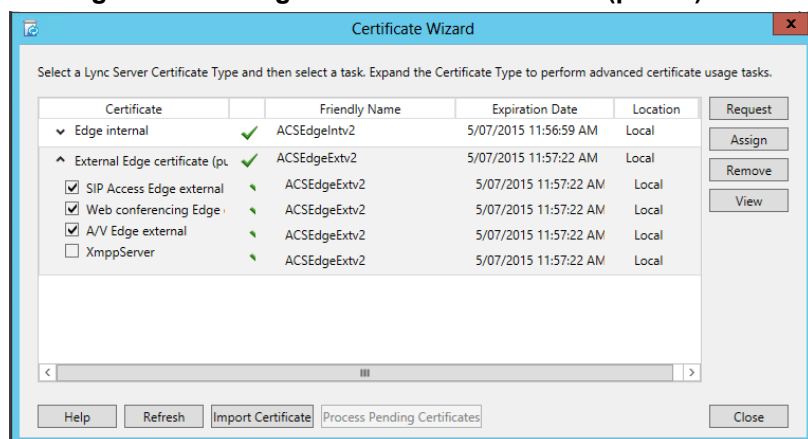


Figure 10-76: Edge Certificate for External (public) use



The process for creating certificate requests is detailed in the preceding sections.



Note: The process for creating certificate requests, importing certificates, and assigning certificates to Skype for Business roles is similar for both Internal and External certificates. The difference is which selections (roles) you chose on the first screen of the Wizard.

Once your chosen Public Certificate vendor has supplied you with the requested certificates, copy the certificate files to the Front End and Edge servers, then use the Skype for Business Certificate Wizards to import the certificates, and assign them to Skype for Business Roles.

The process for importing and assigning certificates is detailed in the preceding sections.

10.11 Certificate Summary

Update: Public certificate authorities will no longer issue public certificates valid from 1 Nov 2015, which contain private DNS name spaces or reserved IP address ranges. Additionally, any name or IP address entered in the Subject common name field must also appear as an entry in the Subject Alternate Name (SAN) list. The intent is to depreciate the Subject common name at some point in future.

The certificates listed in the following table are required to support the edge topology shown in the Single Consolidated Edge Topology figure.

There are three certificates shown for the reverse proxy server to highlight the certificate requirements for dedicated simple URLs (for example, <https://dial-in.contoso.com>).

For deployments that have a single pool or where multiple pools share the same dial-in conferencing and meeting simple URLs, you could create a single publishing rule and corresponding certificate.

For example, URLs defined in topology builder as `lync.contoso.com/dialin` and `lync.contoso.com/meet` could share a single publishing rule and certificate with a subject name of `lync.contoso.com`.



Note: The following table shows a second SIP entry in the subject alternative name list for reference. For each SIP domain in your organization, you need a corresponding FQDN listed in the certificate subject alternative name list.

Table 10-1: Certificates Required for Single Consolidated Edge Topology

Component	Subject Name	Subject Alternative Name Entries/Order	Certification Authority (CA)	Enhanced key usage (EKU)	Comments
Single consolidated Edge	access.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com	Public	Server*	Assign to the following Edge Server roles: External interface: SIP Access Edge Web Conferencing Edge A/V Edge

Component	Subject Name	Subject Alternative Name Entries/Order	Certification Authority (CA)	Enhanced key usage (EKU)	Comments
Single consolidated Edge	lsedge.contoso.net	N/A	Private	Server	Assign to the following Edge Server roles: Internal interface: Edge
Single consolidated Edge	lsedge.contoso.net	N/A	Private	Server	Assign to the following Edge Server roles: Internal interface: Edge
Reverse proxy	lsrp.contoso.com	lswebext.contoso.com dialin.contoso.com meet.contoso.com	Public	Server	Address Book Service, distribution group expansion and Skype for Business IP Device publishing rules. Subject alternative name includes: External Web Services FQDN
					Dial-in conferencing Online meeting publishing rule
Next hop pool (on Front End)	fe01.contoso.net (on Front End)	sip.contoso.com sip.fabrikam.com lsweb.contoso.net lswebext.contoso.com admin.contoso.com dialin.contoso.com meet.contoso.com fe01.contoso.net	Private	Server	Assign to the following servers and roles in the next hop pool: Front End 01



Note: Client ECU is required if public Internet connectivity with AOL is enabled.

10.12 Setting Up a Certificate Authority

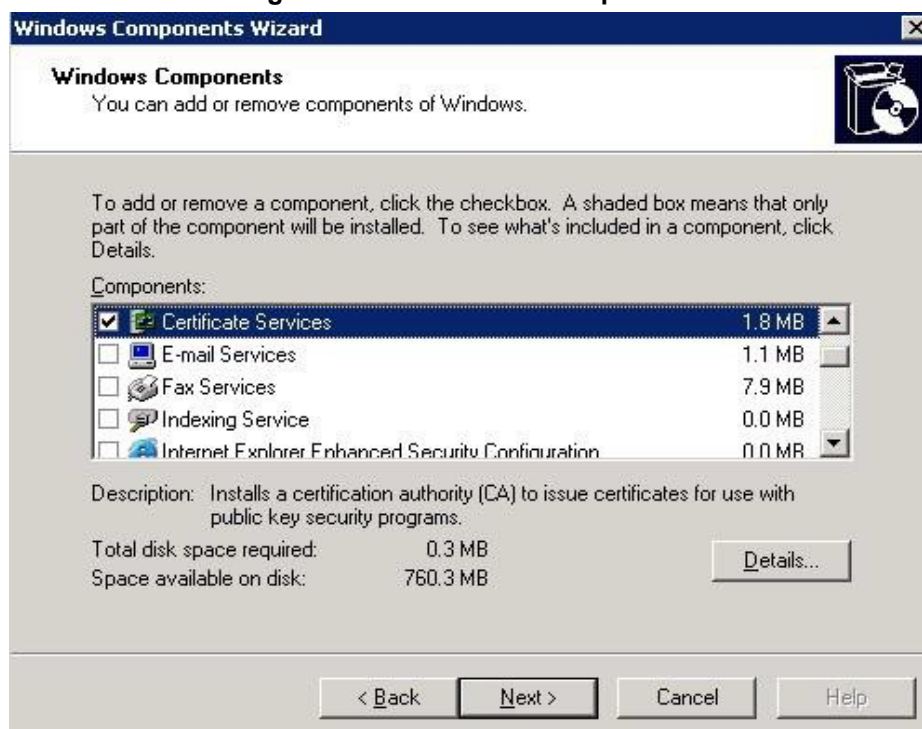
This section describes how to setup a certificate authority.

10.12.1 Setting Up a Certificate Authority on Windows Server 2003

➤ To set up a Certificate Authority on a Microsoft Windows Server 2003 edition:

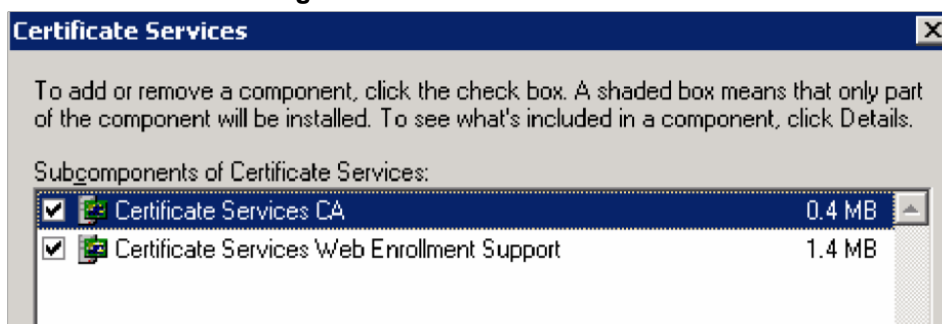
1. Open **Add or Remove Programs** in Windows Control Panel.
2. Select **Add/Remove Windows components**.
3. Select **Certificate Services**.

Figure 10-77: Windows Components



4. Click **Details** and make sure that both the Certificate Services CA and the Certificate Services Web Enrollment Support are enabled.

Figure 10-78: Certificate Services



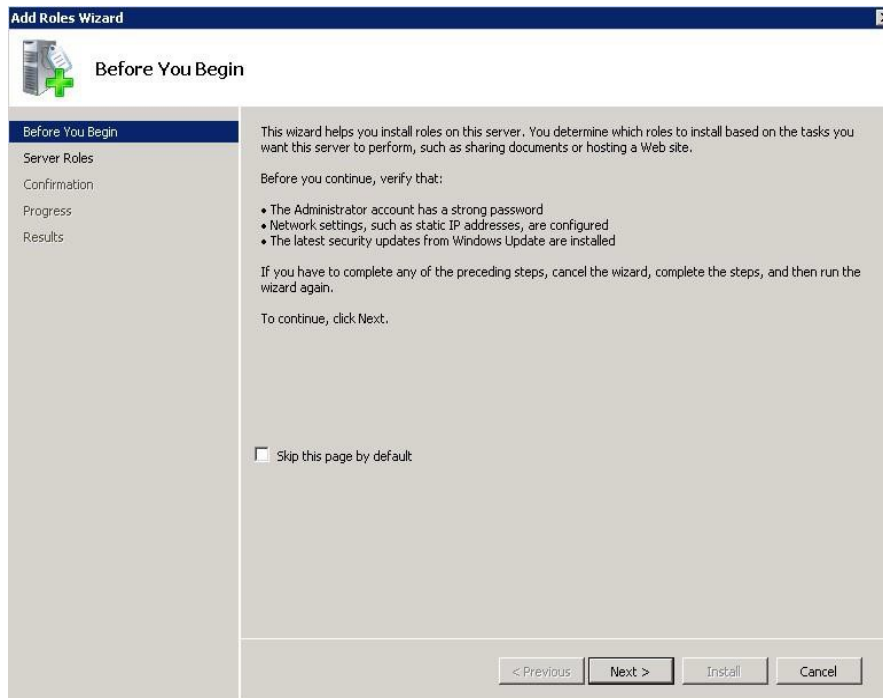
5. Click **OK** followed by **Next** to finish the installation.

10.12.2 Setting up a Certificate Authority on Windows Server 2008

- To set up a Certificate Authority on a Microsoft Windows server 2008 or 2008R2 edition:

 1. Open Server Manager through **Start -> All Programs -> Administrative Tools**.
 2. Select **Roles**, then Add Roles in the right screen of the Roles Summary section.
 3. Follow the screens as shown below:

Figure 10-79: Before You Begin



4. Select **Active Directory Certificate Services**:

Figure 10-80: Introduction to Active Directory Certificate Services

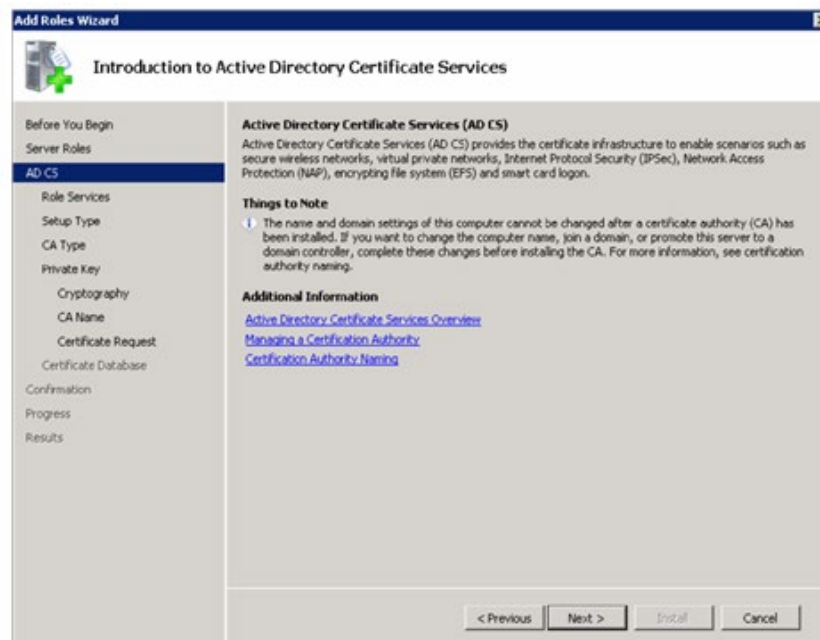
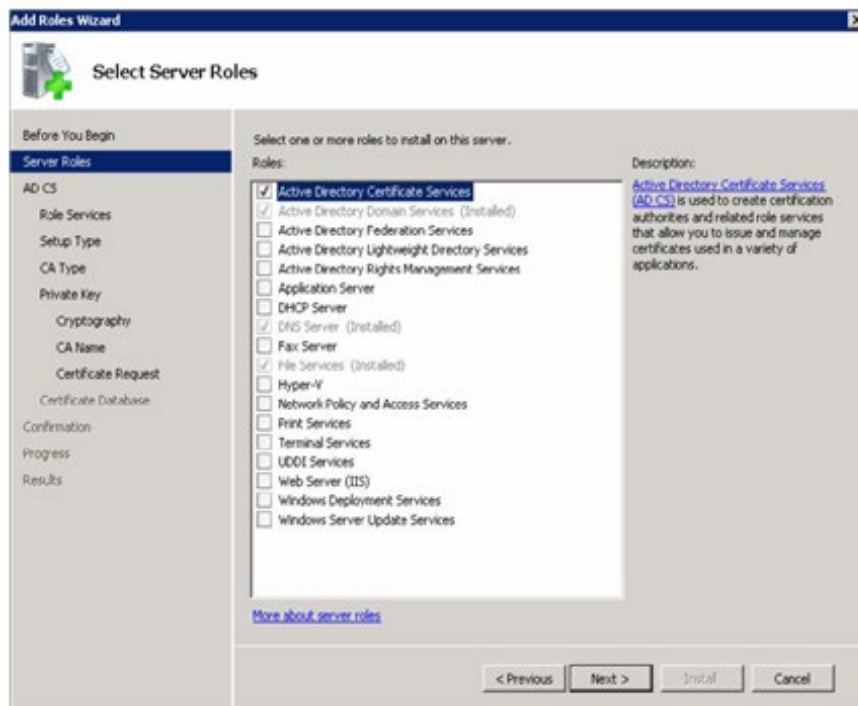
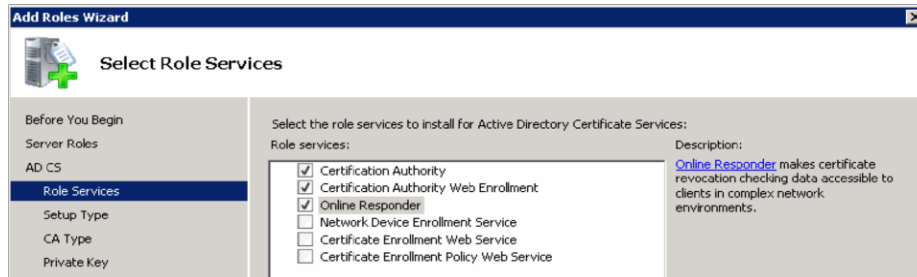


Figure 10-81: Select Server Roles



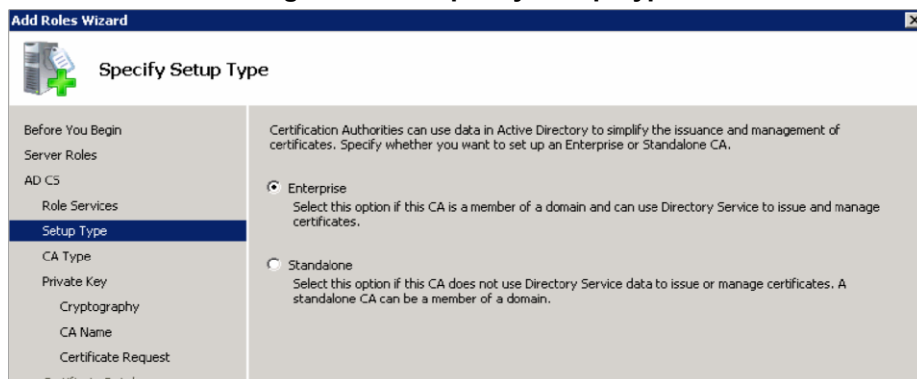
5. Select the **Certification Authority**, the **Certification Authority Web Enrolment** as well as the **Online Responder**.

Figure 10-82: Select Role Services



6. Select **Enterprise**.

Figure 10-83: Specify Setup Type



7. Select **Root CA**.

Figure 10-84: Specify CA Type

Add Roles Wizard

Specify CA Type

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

☒ **Root CA**
Select this option if you are installing the first or only certification authority in a public key infrastructure.

☐ **Subordinate CA**
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

8. Select **Create a New Private Key**.

Figure 10-85: Set Up Private Key

Add Roles Wizard

Set Up Private Key

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Web Server (IIS)

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

☒ **Create a new private key**
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

☐ **Use existing private key**
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ **Select a certificate and use its associated private key**
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ **Select an existing private key on this computer**
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

9. Use the default Cryptography, Common name and Distinguished name suffix in the next two pages.

Figure 10-86: Configure Cryptography for CA

Add Roles Wizard

Configure Cryptography for CA

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Web Server (IIS)
Role Services
Confirmation

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP):
RSA#Microsoft Software Key Storage Provider

Key character length:
2048

Select the hash algorithm for signing certificates issued by this CA:
sha1
md2
md4
sha256

☐ Use strong private key protection features provided by the CSP (this may require administrator interaction every time the private key is accessed by the CA)

Figure 10-87: Configure CA Name

The screenshot shows the 'Configure CA Name' step in the 'Add Roles Wizard'. The left sidebar lists the steps: Before You Begin, Server Roles, AD CS, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name (selected), Validity Period, Certificate Database, and Confirmation. The main area contains instructions: 'Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' There are three text input fields: 'Common name for this CA:' with the value 'jocshost-LYNCRIM-CA', 'Distinguished name suffix:' with the value 'DC=ocshost,DC=nl', and 'Preview of distinguished name:' with the value 'CN=jocshost-LYNCRIM-CA,DC=ocshost,DC=nl'.

10. Choose a Validity Period for the CA.

Figure 10-88: Set Validity Period

The screenshot shows the 'Set Validity Period' step in the 'Add Roles Wizard'. The left sidebar is the same as in Figure 10-87, with 'Validity Period' selected. The main area contains instructions: 'A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.' There is a dropdown menu for 'Select validity period for the certificate generated for this CA:' with '5 Years' selected. Below it, the 'CA expiration Date:' is '1/26/2016 1:37 PM'. A note states: 'Note that CA will issue certificates valid only until its expiration date.'

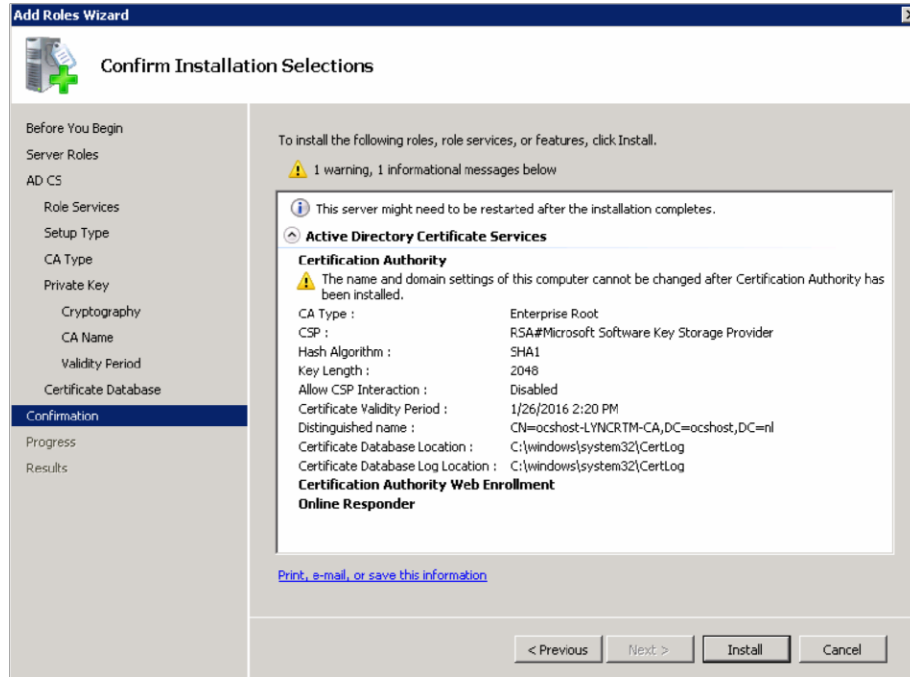
11. Keep the default data location.

Figure 10-89: Configure Certificate Database

The screenshot shows the 'Configure Certificate Database' step in the 'Add Roles Wizard'. The left sidebar lists the steps: Before You Begin, Server Roles, AD CS, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, and Configure Certificate Database (selected). The main area contains instructions: 'The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.' There are two text input fields: 'Certificate database location:' with the value 'C:\Windows\system32\CertLog' and a 'Browse...' button, and 'Certificate database log location:' with the value 'C:\Windows\system32\CertLog' and a 'Browse...' button. A checkbox labeled 'Use existing certificate database from previous installation at this location' is unchecked.

12. If IIS roles are added by the Add Roles Wizard, accept those by clicking next and finish the Wizard by clicking Install on the Confirmation page.

Figure 10-90: Confirm Installation Selections



10.12.3 Setting Up a Certificate Authority on Windows Server 2012

- To set up a Certificate Authority on a Microsoft Windows server 2012:
- 1. Follow the screens as shown below:

Figure 10-91: Add Roles and Features Wizard

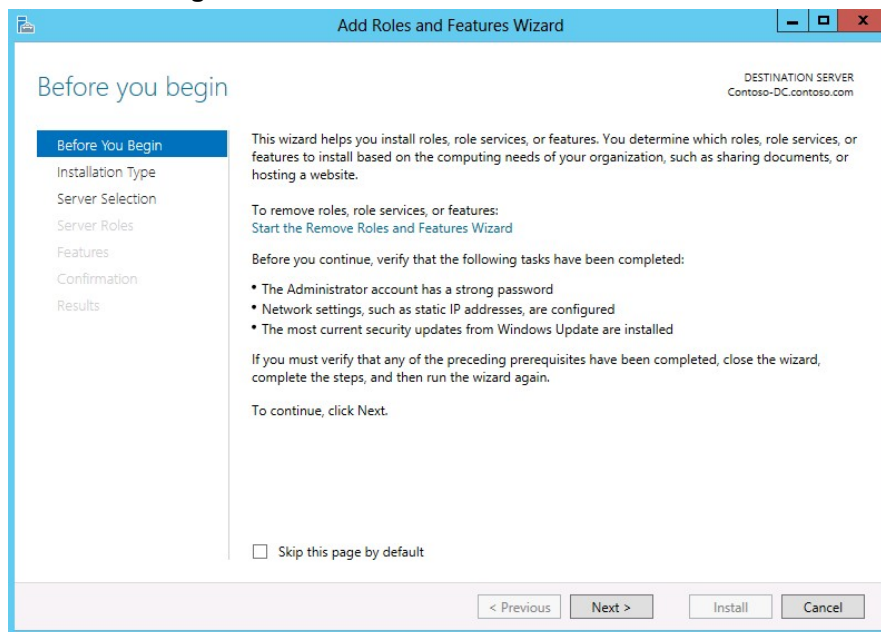
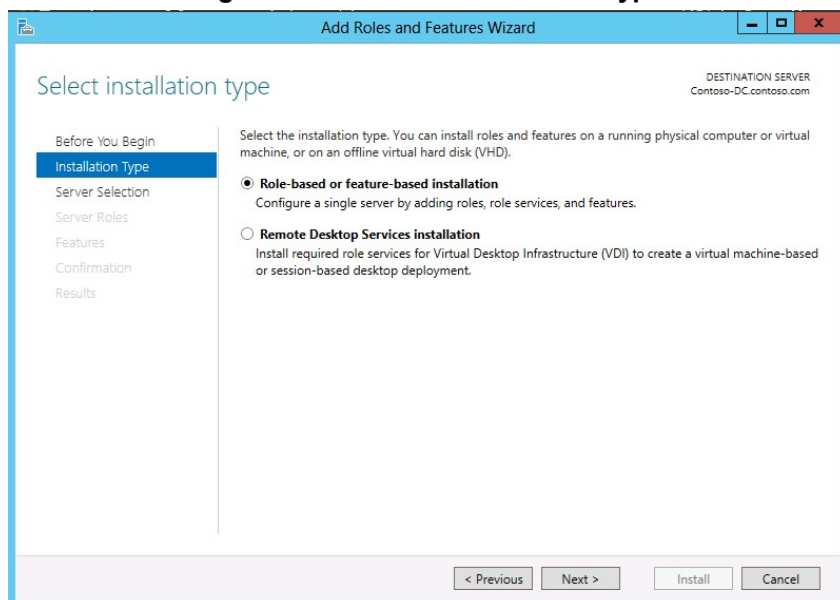
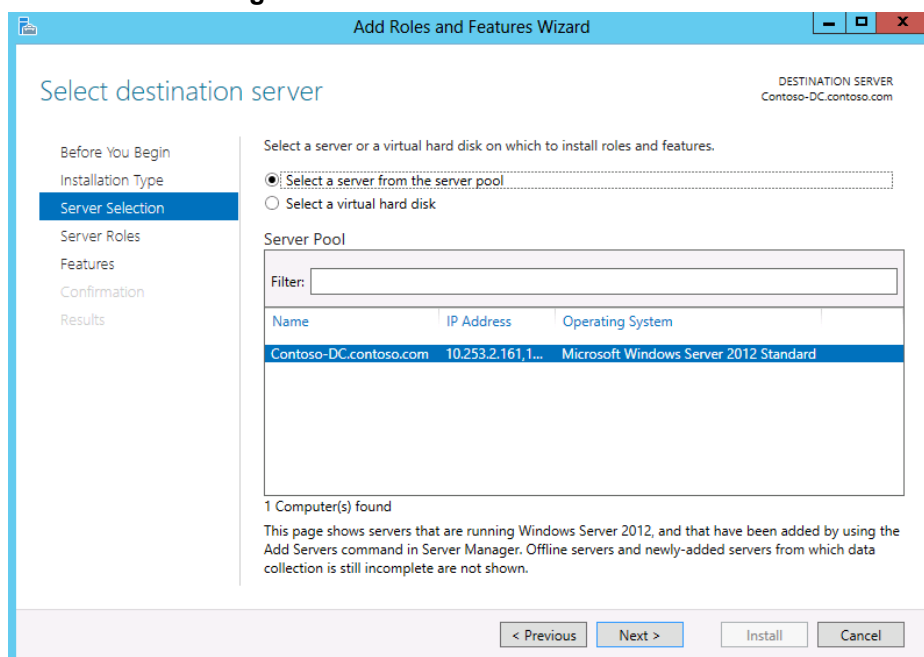
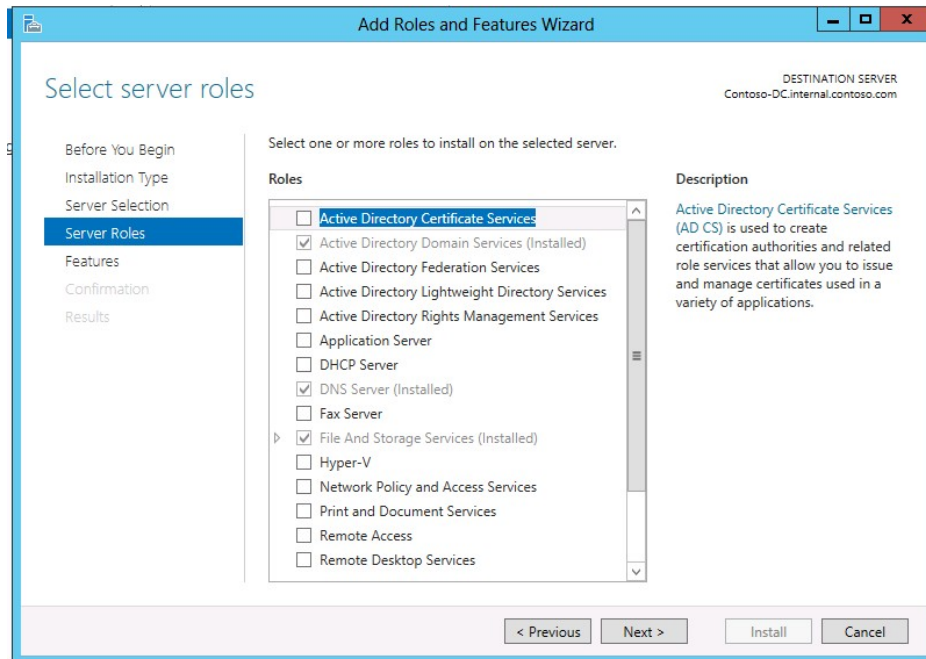


Figure 10-92: Select Installation Type**Figure 10-93: Select Destination Server**

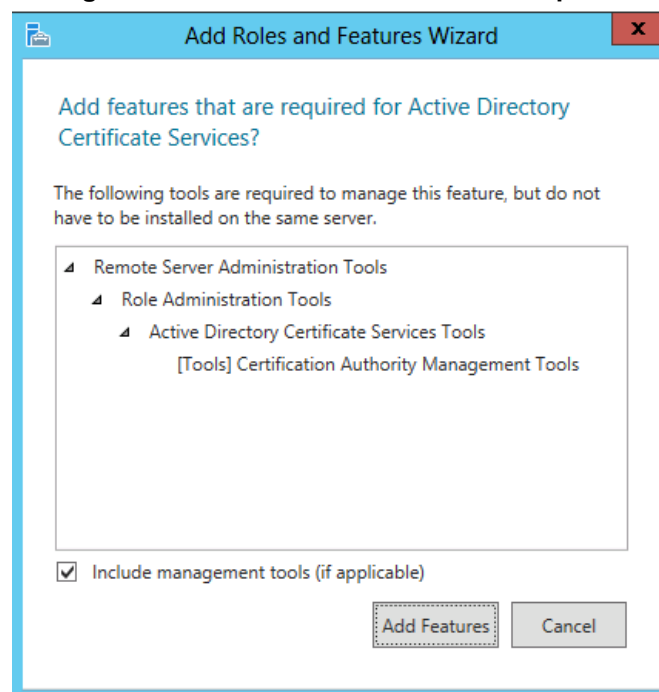
2. Select **Active Directory Certificate Services**:

Figure 10-94: Select Server Roles

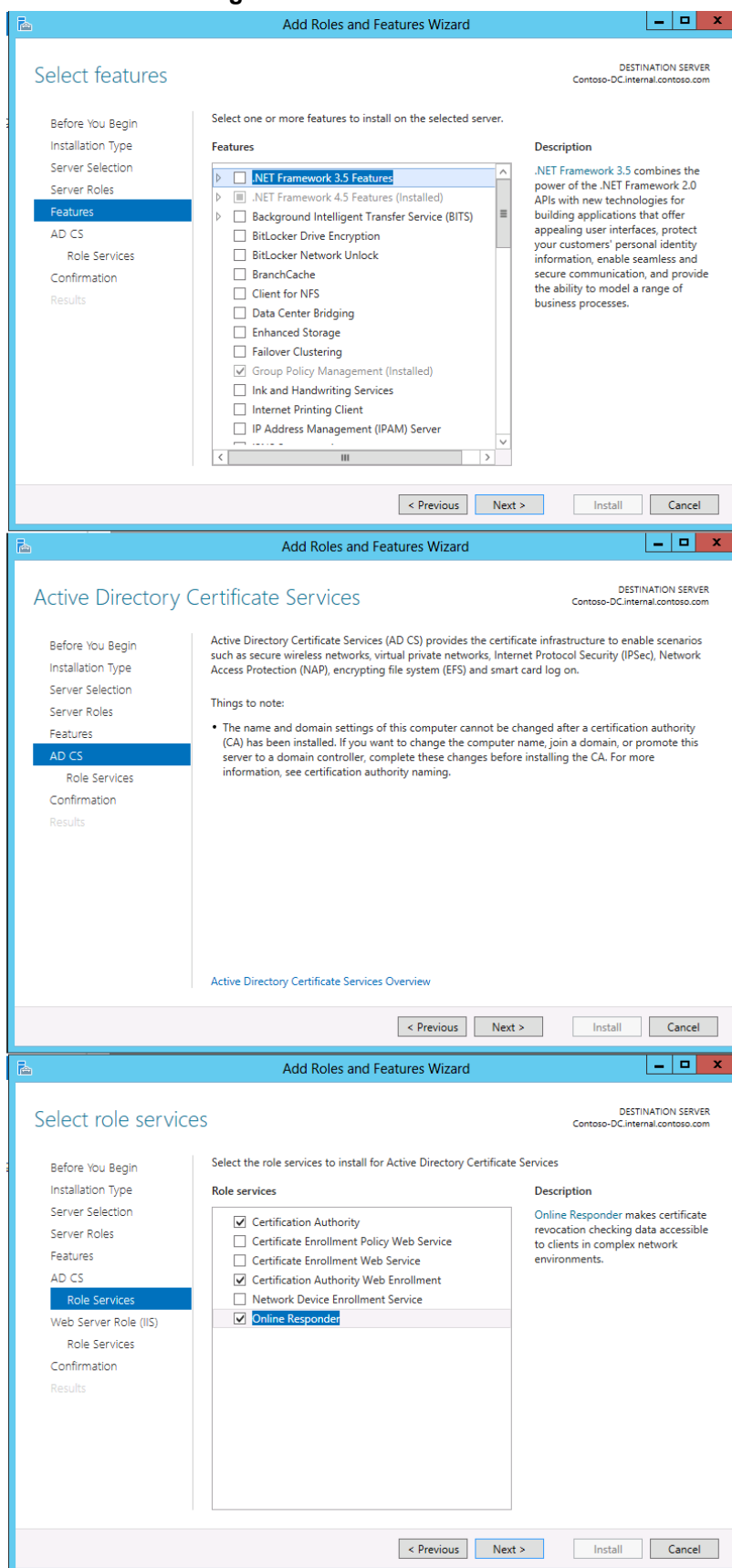


3. Click **Add Features**.

Figure 10-95: Add Features that are Required

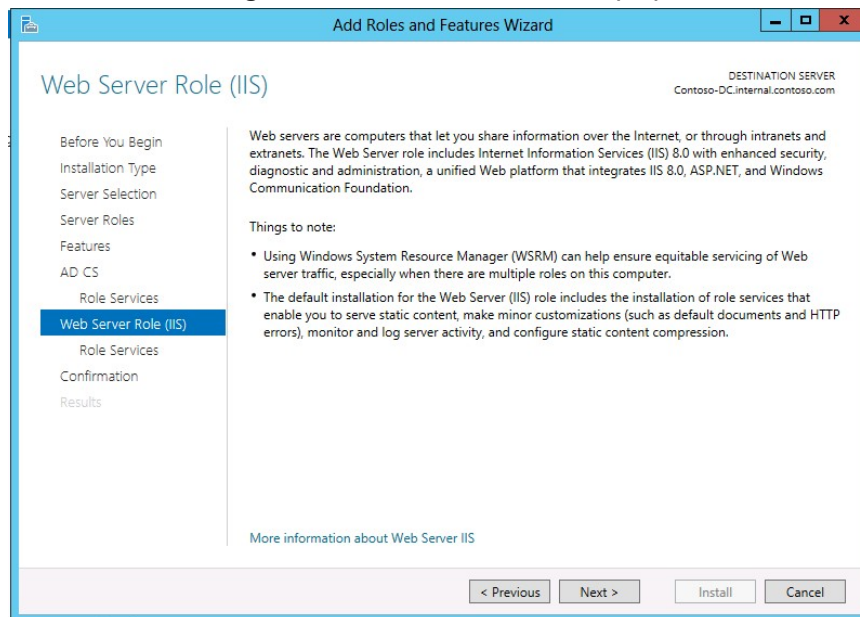


4. Follow the instructions on the screens as shown below.

Figure 10-96: Select Features

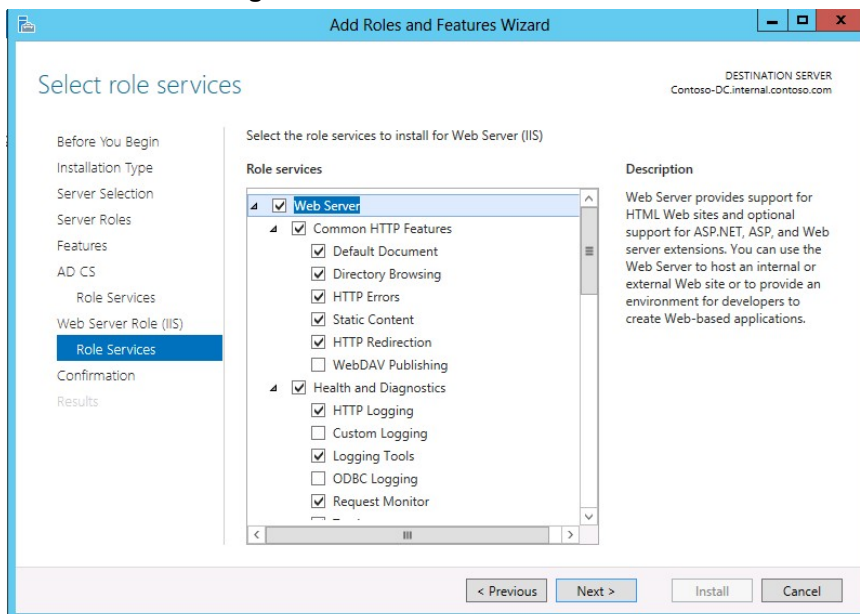
5. Click **Next**.

Figure 10-97: Web Server Role (IIS)



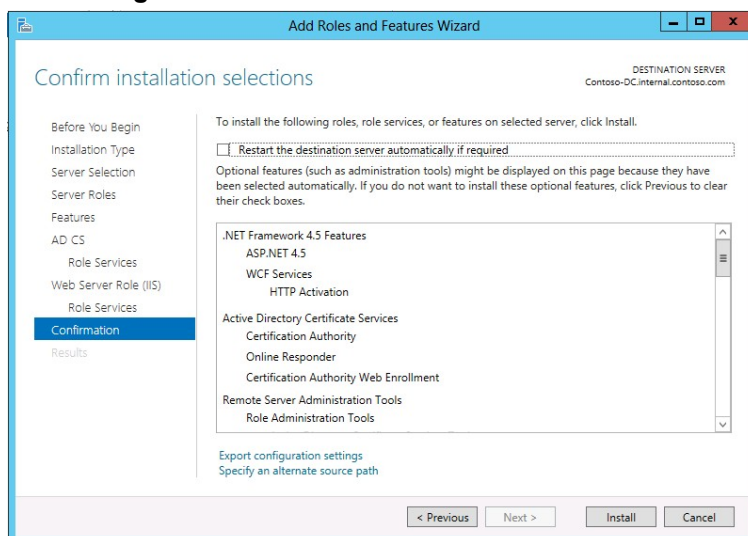
6. Click **Next**.

Figure 10-98: Select Role Services



- Click **Install** to complete the Wizard.

Figure 10-99: Confirm Installation Selection

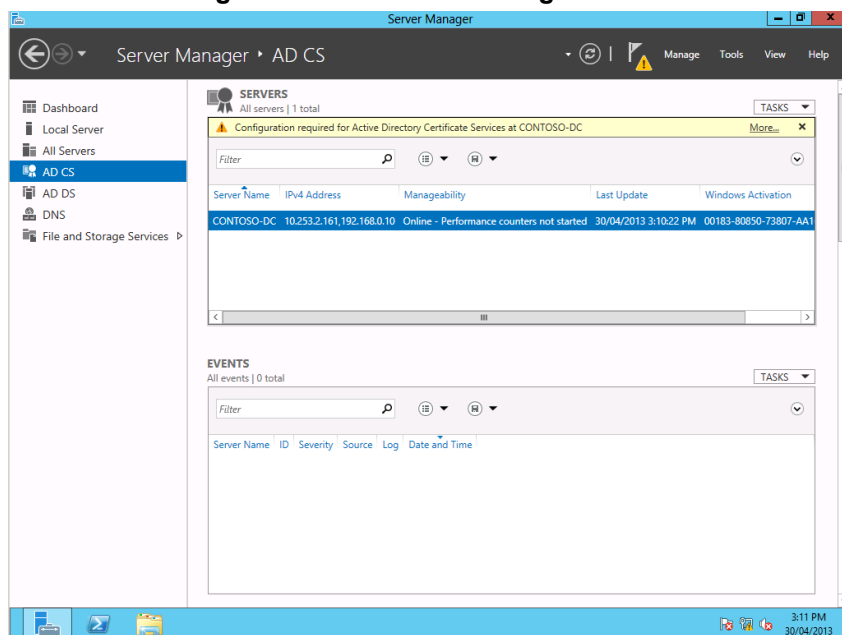


10.12.3.1 Configure the Certificate Services

You must now configure the Active Directory Certificate Services for correct operation.

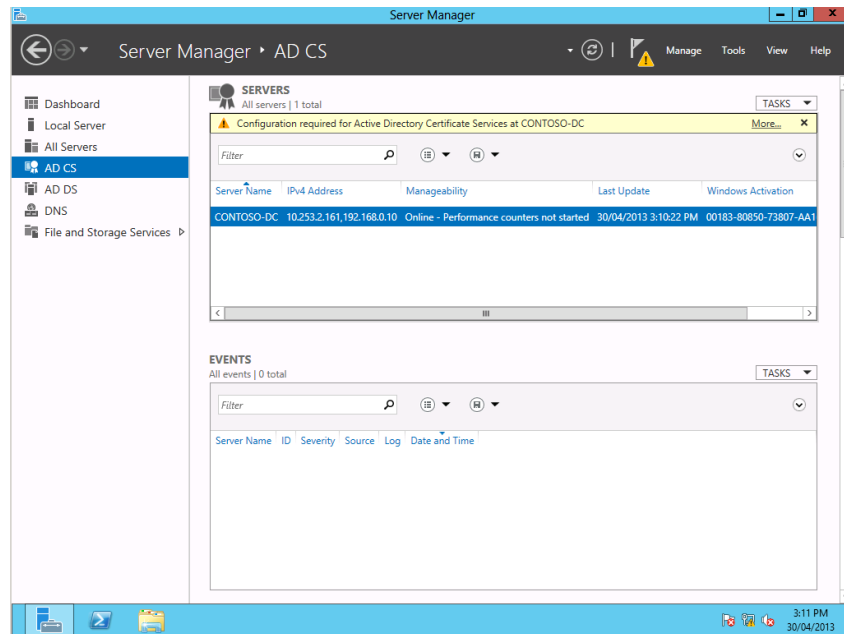
- In the Server Manager, select **AD CS**.
- Click **More...** in the top right corner.

Figure 10-100: Server Manager AD CS



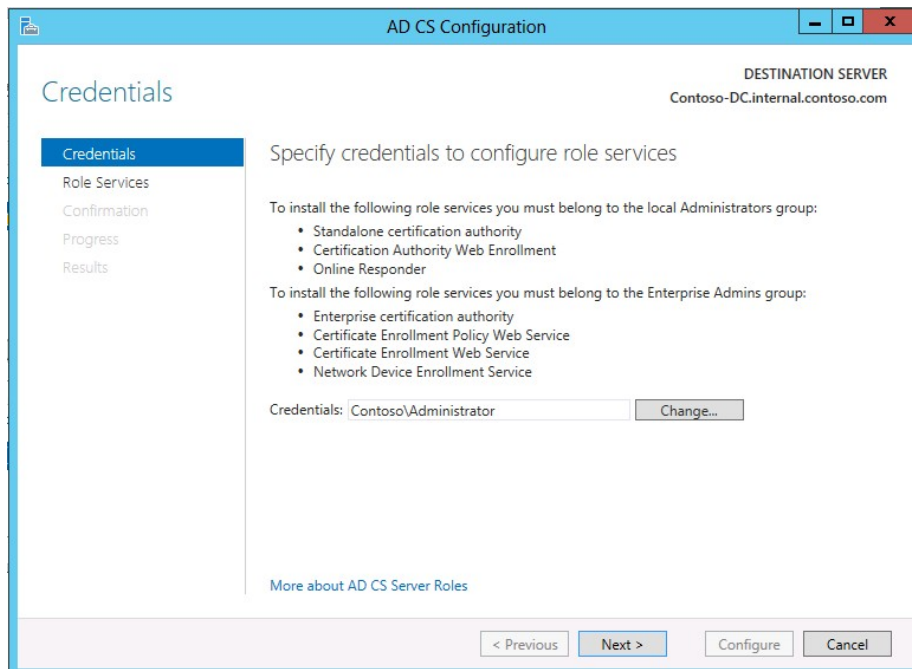
3. Click **Configure Active Directory Certificate Services...** in the action column

Figure 10-101: Server Manager AD CS - Servers



4. Follow the instructions on the screens below.

Figure 10-102: AD CS Configuration - Credentials



5. Select **Certification Authority**, **Web Enrollment**, and **Online Responder**.

Figure 10-103: AD CS Configuration – Role Services

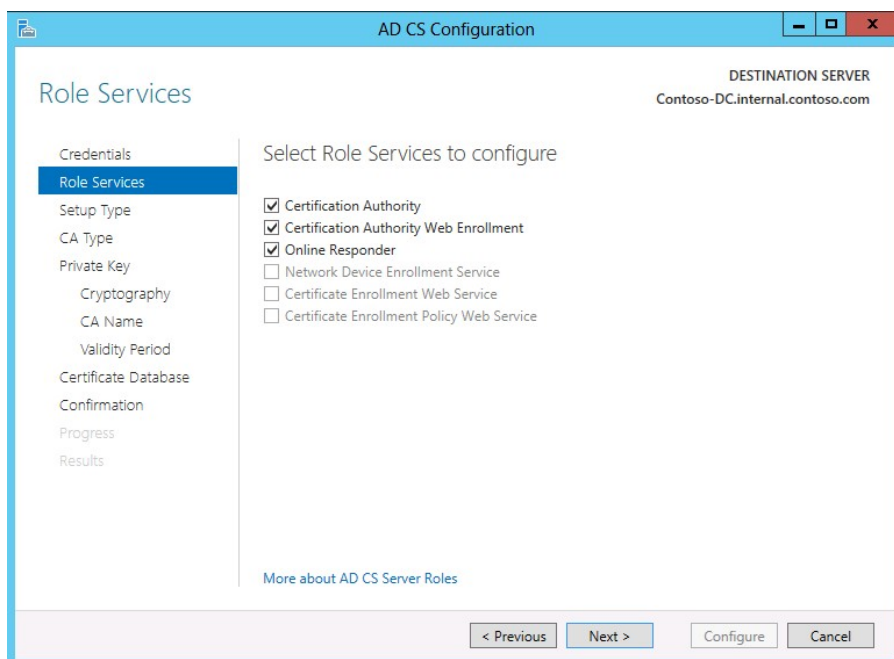


Figure 10-104: AD CS Configuration – Setup Type

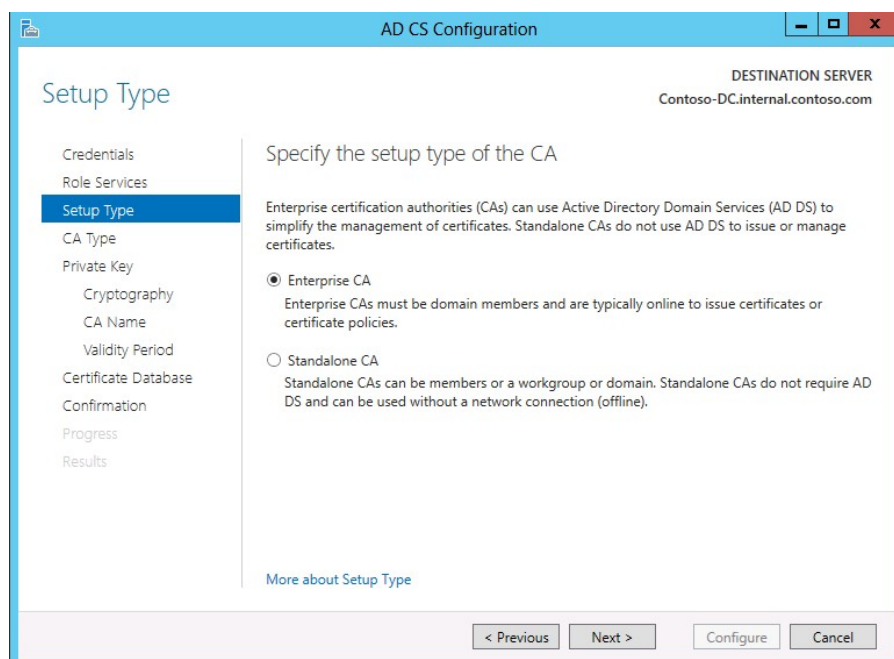


Figure 10-105: AD CS Configuration – CA Type

AD CS Configuration

DESTINATION SERVER
Contoso-DC.internal.contoso.com

CA Type

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

Figure 10-106: AD CS Configuration – Private Key

AD CS Configuration

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Private Key

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ Create a new private key
Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous Next > Configure Cancel

Figure 10-107: AD CS Configuration – Cryptography for CA

The screenshot shows the 'Cryptography for CA' window in the AD CS Configuration console. The left-hand navigation pane lists several steps: Credentials, Role Services, Setup Type, CA Type, Private Key, **Cryptography** (highlighted), CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main pane is titled 'Specify the cryptographic options'. It contains two dropdown menus: 'Select a cryptographic provider:' set to 'RSA#Microsoft Software Key Storage Provider' and 'Key length:' set to '2048'. Below these is another dropdown menu 'Select the hash algorithm for signing certificates issued by this CA:' with a list of options: SHA256, SHA384, SHA512, SHA1 (highlighted), and MD5. A checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' is currently unchecked. At the bottom of the main pane is a link 'More about Cryptography'. The bottom of the window features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

Figure 10-108: AD CS Configuration – CA Name

The screenshot shows the 'CA Name' window in the AD CS Configuration console. The left-hand navigation pane is identical to the previous window, with 'CA Name' highlighted. The main pane is titled 'Specify the name of the CA'. It includes a descriptive text: 'Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' Below this text are three input fields: 'Common name for this CA:' containing 'internal-CONTOSO-DC-CA', 'Distinguished name suffix:' containing 'DC=internal,DC=contoso,DC=com', and 'Preview of distinguished name:' containing 'CN=internal-CONTOSO-DC-CA,DC=internal,DC=contoso,DC=com'. A link 'More about CA Name' is located at the bottom of the main pane. The bottom of the window features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

Figure 10-109: AD CS Configuration – Validity Period

AD CS Configuration

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Validity Period

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 30/04/2018 3:16:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

More about Validity Period

< Previous Next > Configure Cancel

Figure 10-110: AD CS Configuration – CA Database

AD CS Configuration

DESTINATION SERVER
Contoso-DC.internal.contoso.com

CA Database

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the database locations

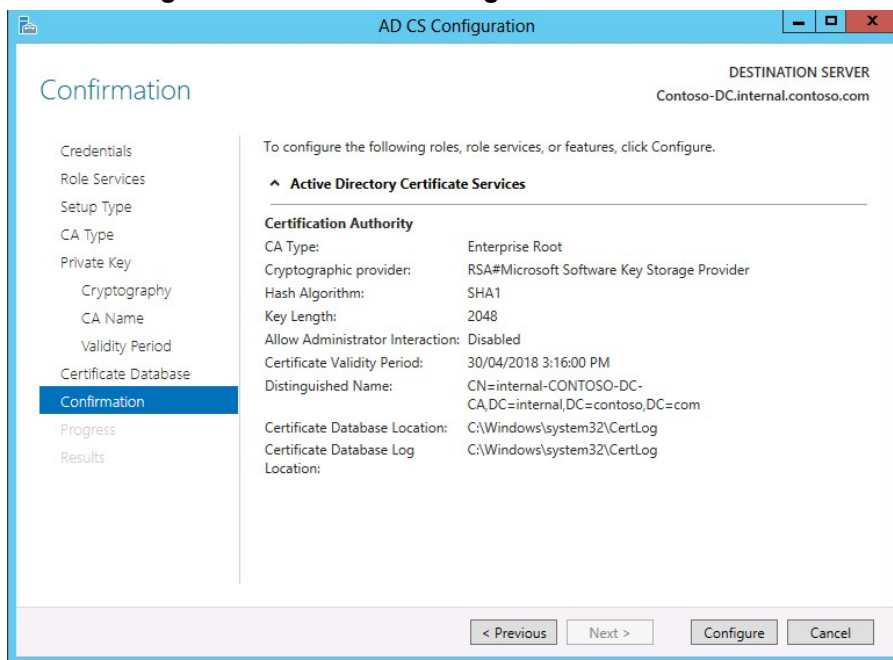
Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

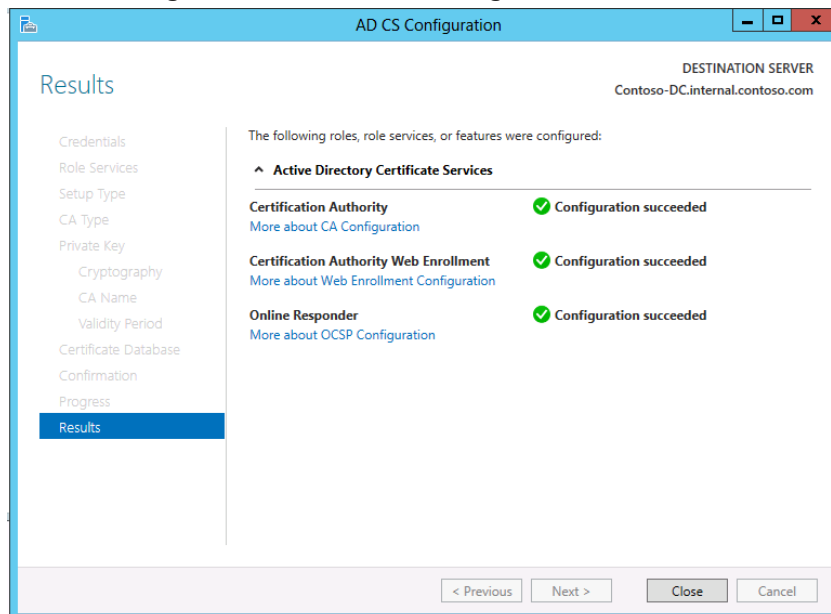
More about CA Database

< Previous Next > Configure Cancel

- Click **Configure** to complete the wizard.

Figure 10-111: AD CS Configuration - Confirmation

- Click **Close**.

Figure 10-112: AD CS Configuration - Results

This page is intentionally left blank.

11 Miscellaneous Actions

The following actions are described below:

- Installing the Product License
- Activating Windows
- Running Windows Updates
- Running Skype for Business Cumulative Update
- Understanding CloudBond Support and Responsibility Program
- Running Antivirus Application
- Running the Skype for Business Deployment Wizard
- Forwarding DNS Requests

11.1 Installing the Product License

X-UM Standard has two licenses – one for the CloudBond 365 and one for the X-UM Connector. The CloudBond 365 uses an Enterprise License model i.e. a single CloudBond 365 license is used for one or more CloudBond 365 servers that are installed in the same company domain and share the same Active Directory (AD). The Enterprise License will store the total number of users of all CloudBond 365 servers that share the same AD.

The X-UM Standard License is per X-UM Connector server.

Both license are based on a unique “System ID” (Fingerprint) which is based on an AD fields. The “System ID” key is available the first time you try to login to the CloudBond 365 using the CloudBond 365 sysadmin.

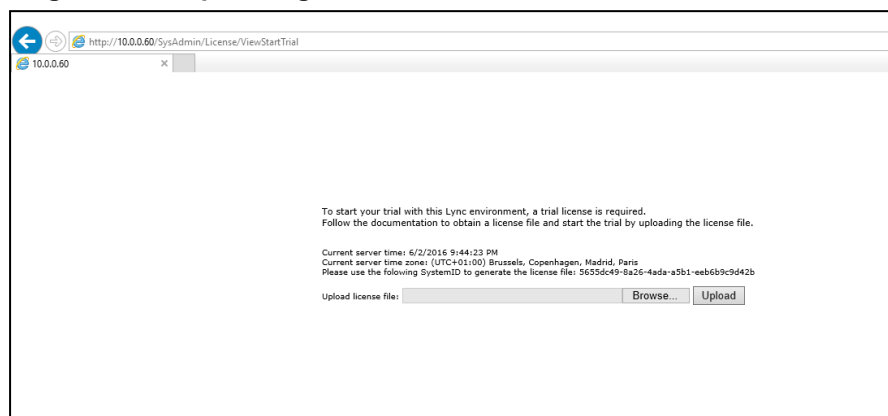
For the X-UM Standard, you need to open the Swagger Web interface to obtain the ID.

11.1.1 Uploading the CloudBond 365 License

The procedure below describes how to upload the CloudBond 365 License.

➤ **To upload the CloudBond 365 License:**

Figure 11-1: Uploading License File to the CloudBond 365



The “System ID” is also available in the CloudBond 365 management tool **System Configuration > Licensing Info** page.

The first time a CloudBond 365 system is ordered for an enterprise the AudioCodes system generated a unique “Product Key” that represents the customer enterprise system. The Product key is sent to the customer/channel upon system ordering via email.

To activate your CloudBond 365 system you will need both a “Product Key” and a “System ID” (Fingerprint). Once you have both keys you can activate your product through AudioCodes License Activation tool at <http://www.audiocodes.com/swactivation>. An e-mail will subsequently be sent to you with your Product License.

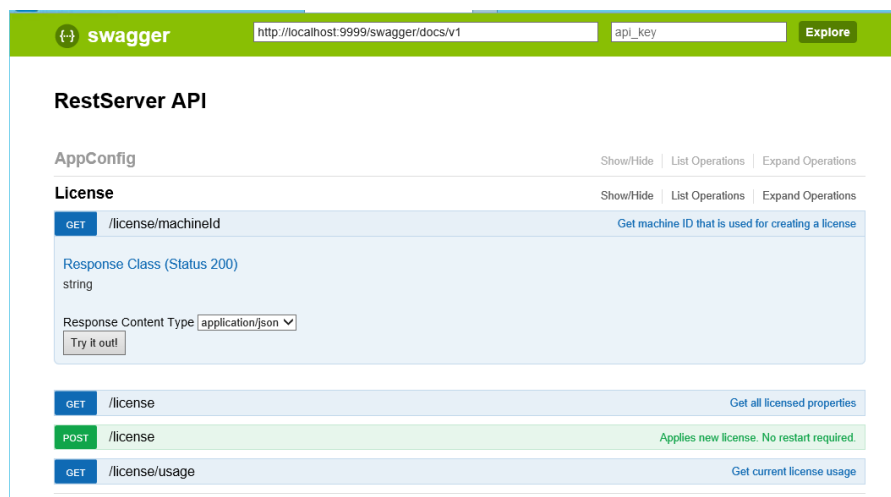
11.1.2 Uploading the X-UM Standard License

The procedure below describes how to upload the X-UM Standard License.

➤ To upload the X-UM Standard License:

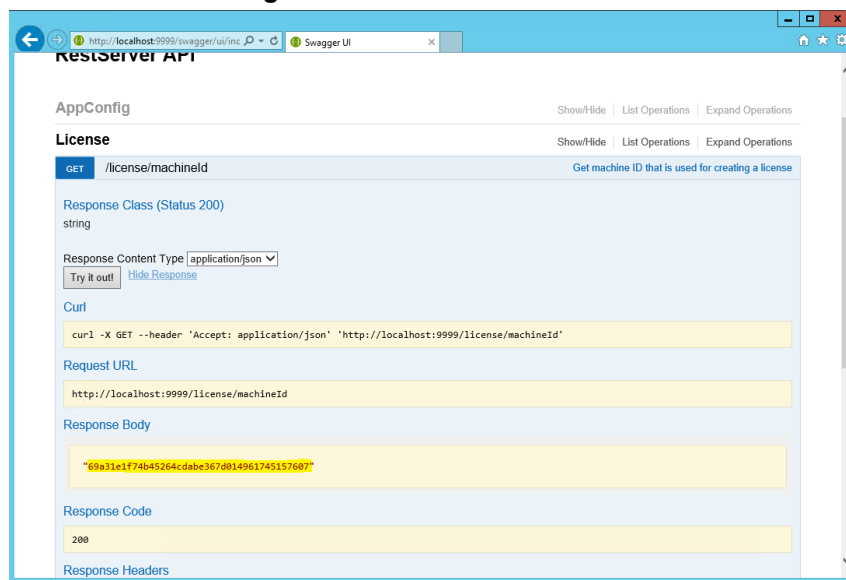
1. From the X-UM Standard open the browser and browse to <http://localhost:9999/swagger/>.
2. To get the System ID go to **License > GET /License/machineId > Try it out!..**

Figure 11-2: RestServer API



3. After clicking 'Try it out!' you will get the below page – the machine ID is the string mark in yellow (without the quotes).

Figure 11-3: RestServer API - 2



4. To upload the license go to **License > POST /License**.
5. Copy the license key to the licenseString edit box (Add quotes if your string don't include one).
6. Click **Try it out!**.
7. Validate that the license is valid by going to **License > POST /License**.

11.2 Activating Windows

X-UM Standard is supplied with Windows 2012 R2 Standard Edition OEM licenses, with the Microsoft Product License code stickers attached to the server hardware.

If you are performing a Bare Metal installation, or rebuilding an existing X-UM Standard system, you may need to activate windows when the software installation is complete.

You will need to Activate the Host server, as well as each Virtual Machine.

To activate windows, you may start the Activation process by running *slui.exe*, or opening the Sever Manager utility and clicking the **Product ID** field.



Note: Make sure your host server and all virtual machines have Internet access when activating the Windows license.

The Windows activation key is a 25 character key available on the Windows license sticker attached to the server and named 'Product Key' e.g., *abcd-12345-efghi-6789-jklmn*.

Each Windows 2012 R2 OEM sticker is allowed to activate one physical server (i.e., Host) and two additional virtual machines running on the same physical sever.

Figure 11-4: Sticker Location



The CloudBond 365 Standard+ Box Edition contains two Windows 2012 R2 OEM license stickers that allows you to license the Host, FE and Edge servers with the first sticker product key. The second sticker product key is for licensing the X-UM Connector server.

Figure 11-5: Activation using Server Manager

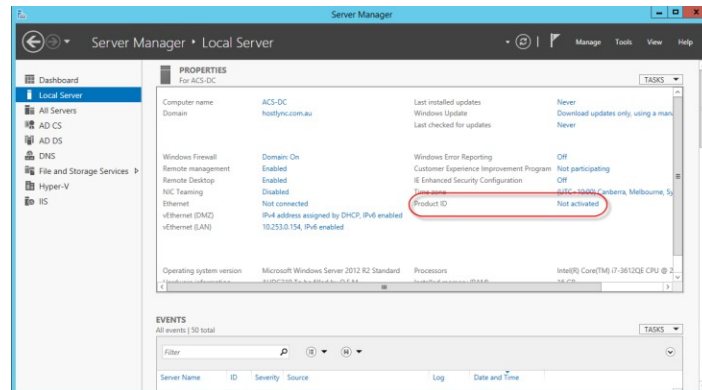


Figure 11-6: Entering the Product Key



Note: It is recommended that you photograph or copy the Windows product key stickers and save them in a safe place to be used in the future, for a system re-installation or if your server is physically placed in a rack where it may be difficult to access the Windows sticker during installation.

11.3 Running Windows Updates

Microsoft periodically releases new hotfixes for the Windows operating system to solve security issues and bug fixes.

It is recommended to follow the Microsoft recommendation and have your X-UM Standard Windows operating system up-to-date with the latest hotfixes.

Refer to the Microsoft best practice guidelines regarding Windows Update:

<https://technet.microsoft.com/en-us/library/dn518328.aspx>



Note: If any unsupported or unapproved hotfix is found by the AudioCodes team, AudioCodes will officially publish a Product Notice regarding this issue.

Windows Update settings should be modified to suit your requirements, or manually install updates at a convenient time on all Windows Servers (Management server, Front End, and Edge) installed as part of a X-UM Standard 365 system.

To manually install updates, open the Server Manager Utility, then select the Last Installed Updates field.



Note: Ensure that DNS forwarding has been set correctly prior to attempting a Windows Update. See Section 11.8 for more details.

Figure 11-7: Accessing Windows Updates

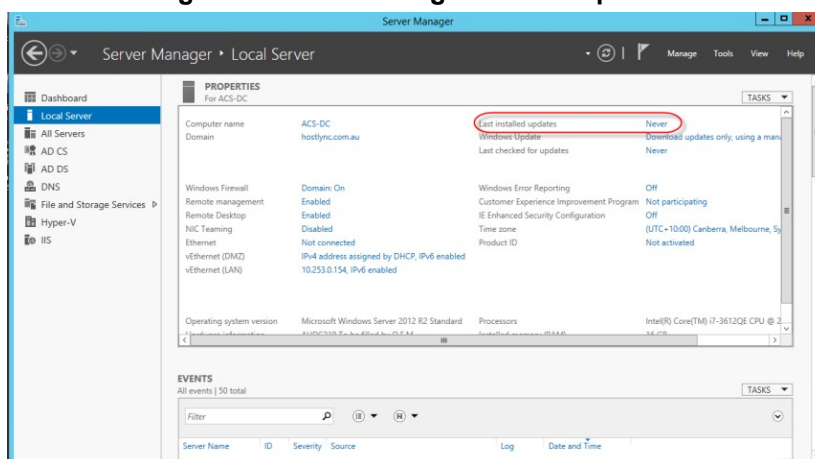


Figure 11-8: Checking for New Updates

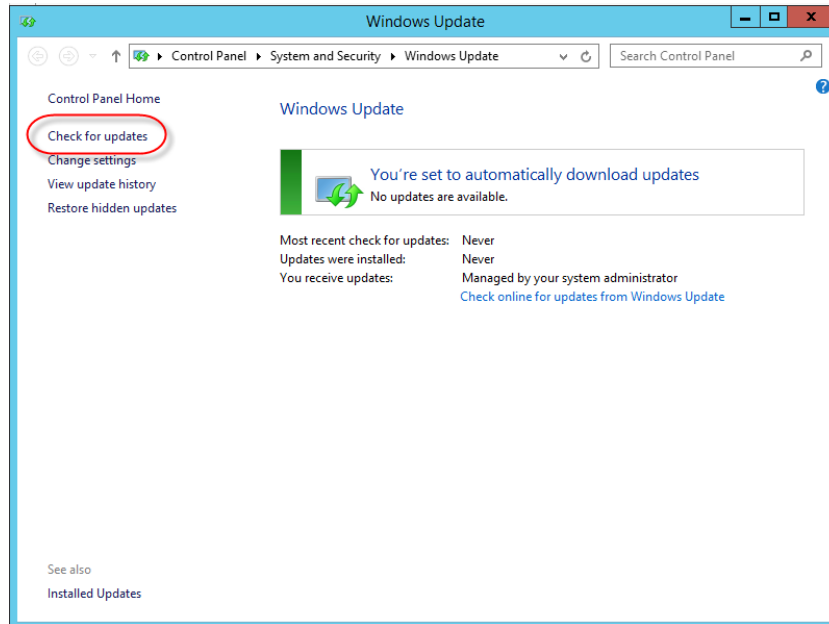


Figure 11-9: Checking for New Updates

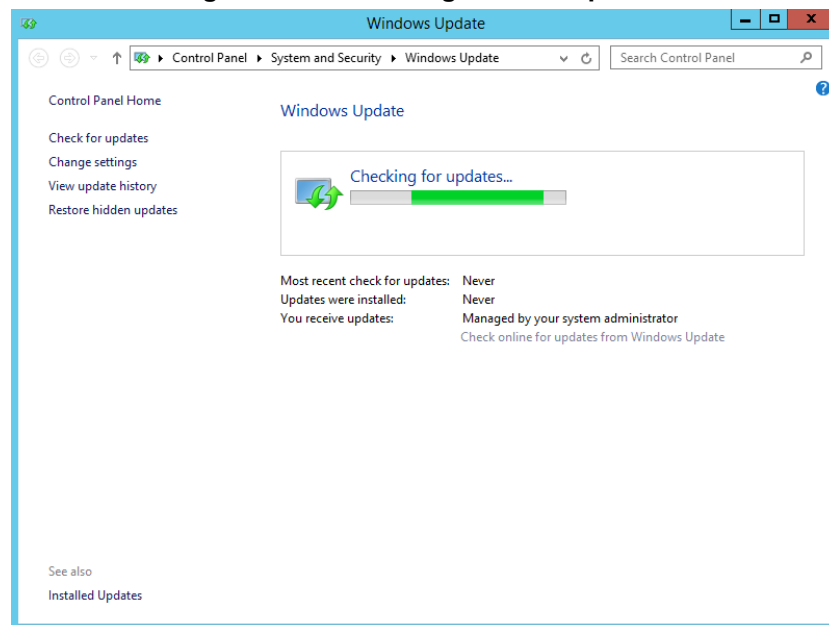


Figure 11-10: New Updates Found

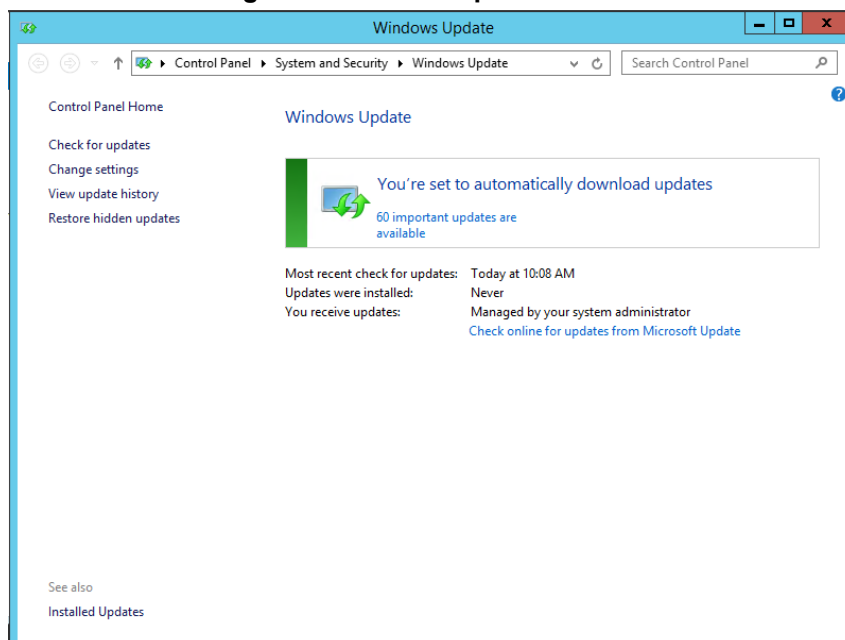
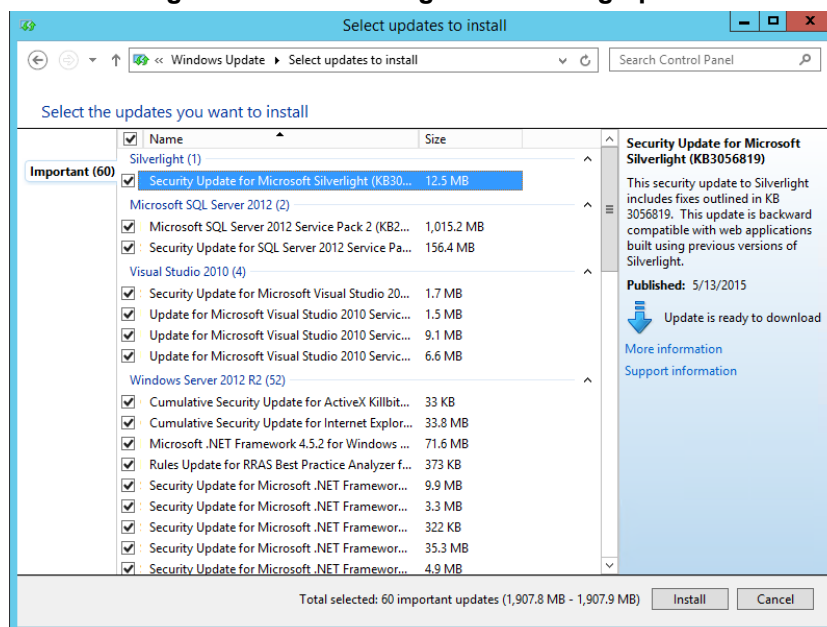


Figure 11-11: Selecting and Installing Update



Unless you wish to avoid a specific update, it is generally easiest to accept the default selections and click **Install**.

11.4 Skype for Business Cumulative Update

Microsoft periodically releases a Cumulative Update (CU) of fixes for the Skype for Business different roles. AudioCodes periodically tests and verifies each released CU and publishes its recommendation, whether or not a new CU is approved for the X-UM Standard system.

It is recommended not to install a CU on the X-UM Standard unless it has been approved by AudioCodes.

11.5 CloudBond Support and Responsibility Program

The CloudBond 365 Support and Responsibility Program is based and defined in the AudioCodes Partner Solution Support (APSS) program. For more information, refer to the APSS-Policy.

11.6 Antivirus Application

No antivirus application is installed with X-UM Standard. To protect your X-UM Standard system, it is advised to install an antivirus application. Make sure you install a Microsoft-verified antivirus application for Skype for Business.

Antivirus applications may influence and degrade system performance. Refer to Microsoft instructions for installing the antivirus application on Skype for Business servers at <https://technet.microsoft.com/en-us/library/mt629173.aspx>.

11.7 Running the Skype for Business Deployment Wizard

Normally, the Software Install Wizard will perform all Skype for Business Deployment steps for you automatically.

If creating a paired pool for resiliency purposes, this can only be done after the software install has been completed. For Paired Pools, it is necessary to run the Skype for Business Deployment wizard on each server, so that Topology Changes (paired pools) take effect.

To run the deployment wizard (on each FE and Edge server), locate the Skype for Business Deployment Wizard on the Start menu, and open the Utility.

Figure 11-12: Skype for Business Deployment Wizard

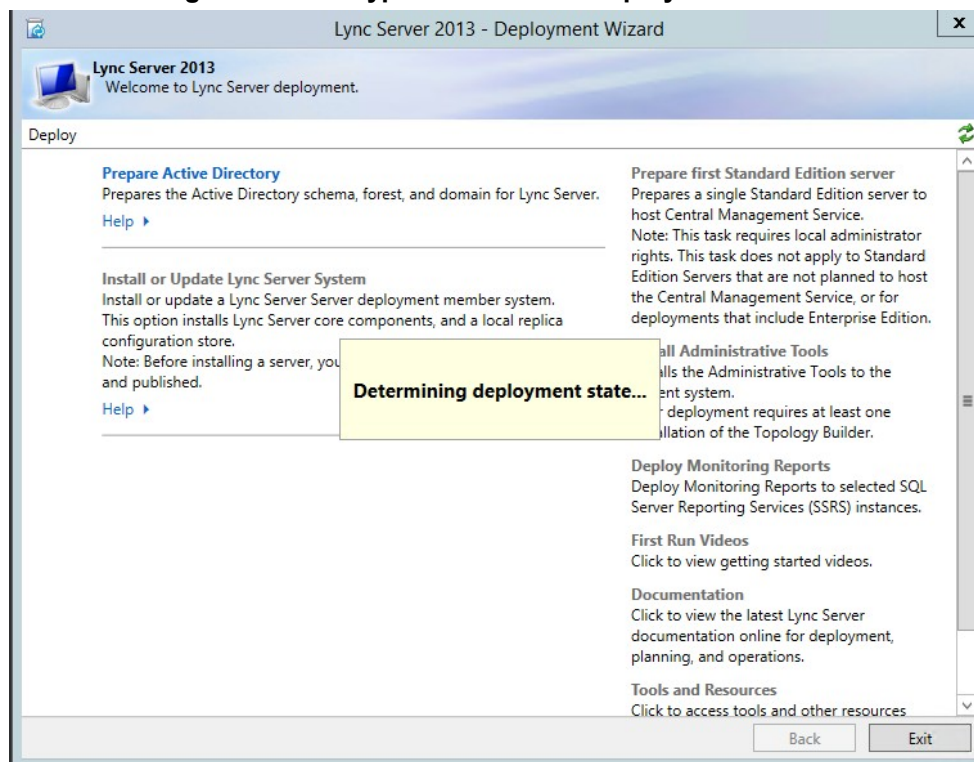


Figure 11-13: Setup or Remove Components

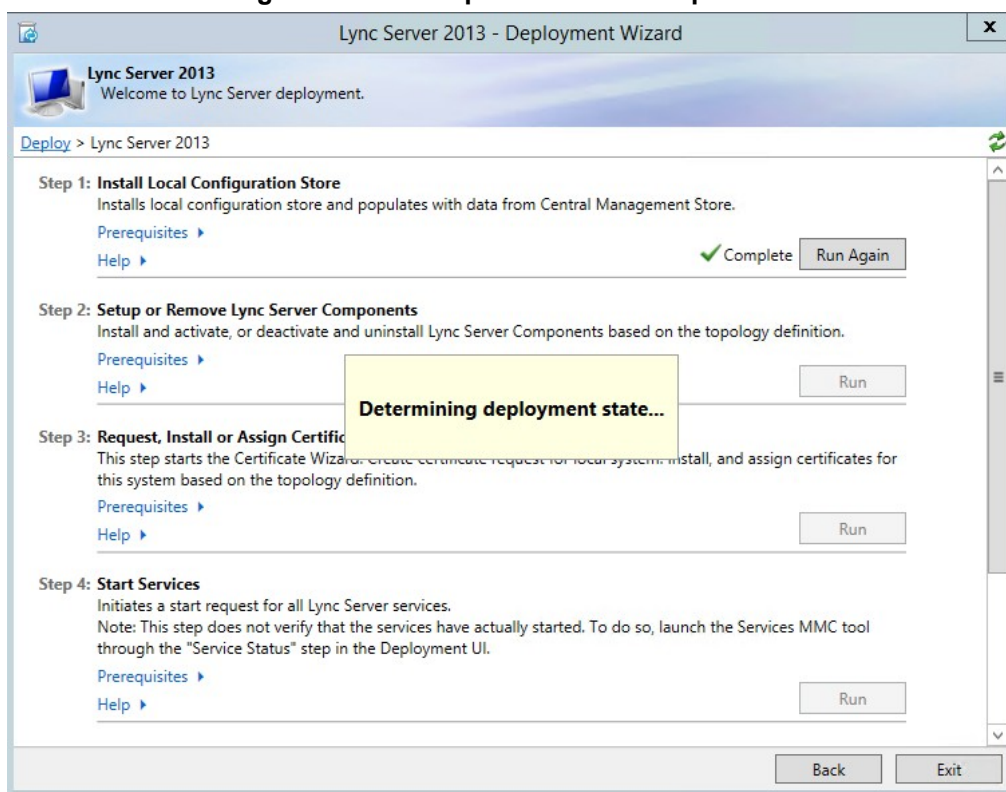


Figure 11-14: Updating the Skype for Business Deployment

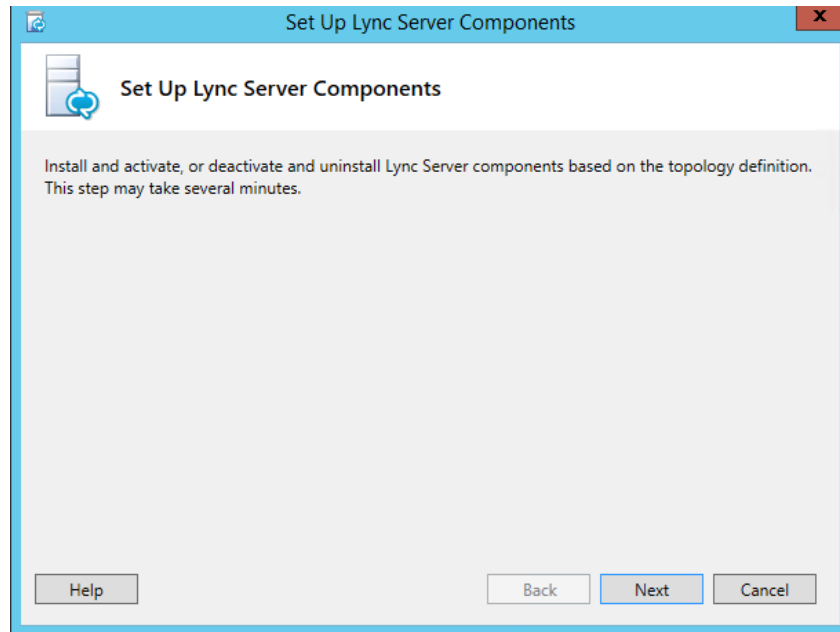
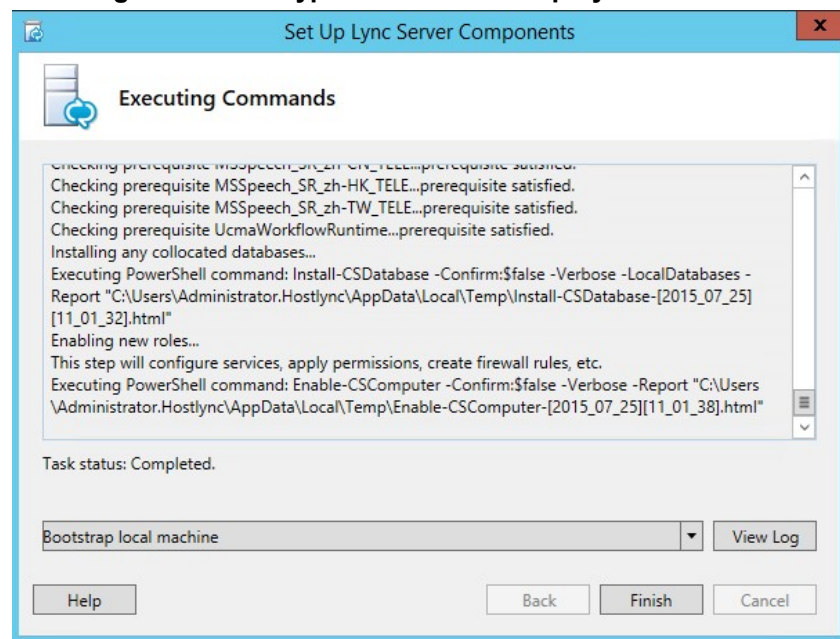


Figure 11-15: Skype for Business Deployment Results



11.8 Forwarding DNS Requests

The X-UM Standard controller (UC-DC) acts as the DNS master for the X-UM Standard system. It can resolve all necessary DNS lookup requests within the X-UM Standard system. However, the DNS server on UC-DC is unable to resolve external DNS requests by itself. The DNS server must forward any unknown request to another, more authoritative DNS server.

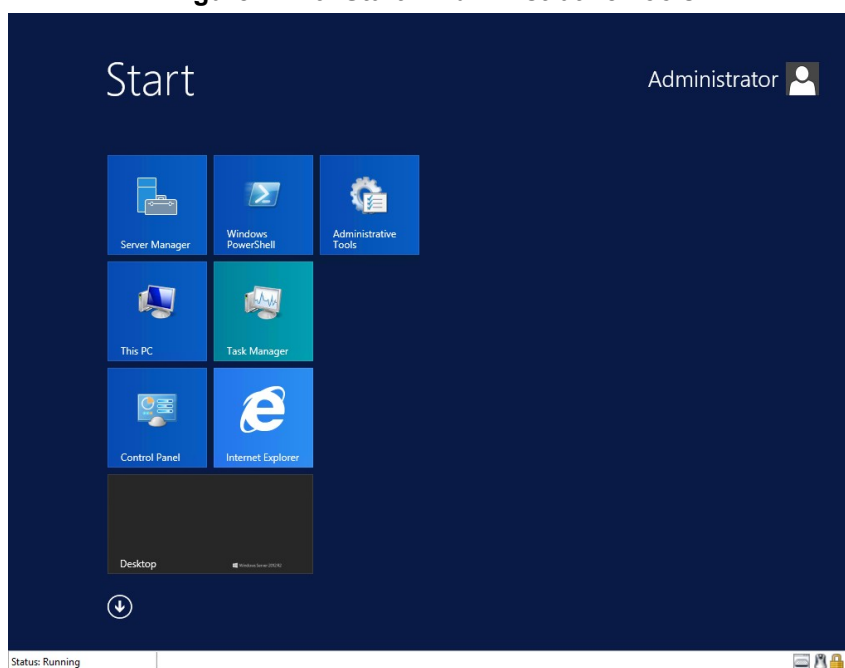
If following the Deployment Guide, and establishing a Forest Trust with your corporate domain, DNS requests would normally be forwarded to the corporate DNS server as the more authoritative server.

If you are deploying the X-UM Standard system in a standalone mode, with no forest trust, DNS requests would normally be forwarded to the Internet (DNS specified by your ISP), as the more authoritative server.

➤ **To forward DNS requests:**

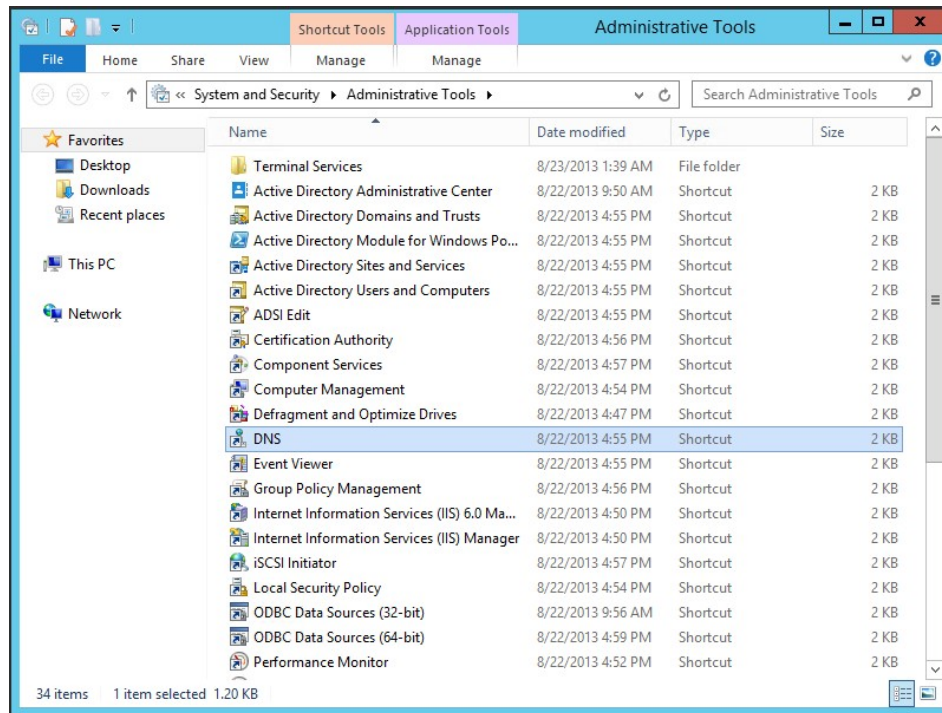
1. Log on to UC-DC using **Remote Desktop**.
2. Open the **Administrative Tools** menu and select the **DNS Management Console**.

Figure 11-16: Start > Administrative Tools



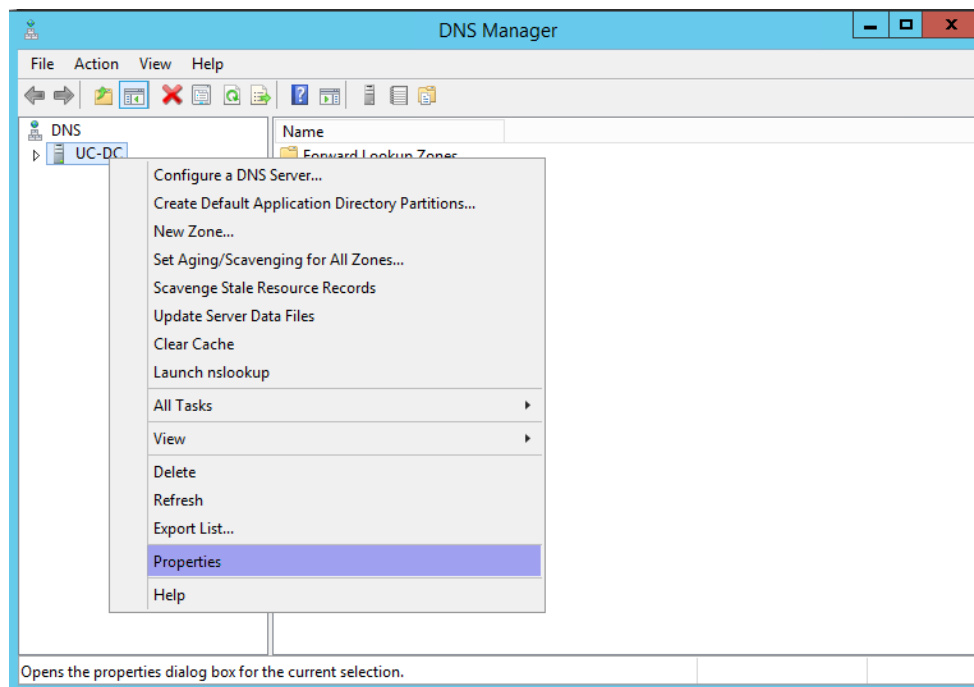
3. Right-click the DNS server name.

Figure 11-17: DNS MMC Tool



4. Select **Properties**.

Figure 11-18: Setting DNS Server Properties



5. Select the **Forwarders** tab and add the IP address of the more authoritative DNS server
6. Close the **DNS mmc**.

DNS requests from the X-UM Standard servers will now be passed to the X-UM Standard Controller (UC-DC) as normal. If the request is for an external name, the UC-DC DNS server will be unable to resolve the request, and will relay the request to the more authoritative DNS server for resolution.



Note: Failure to set DNS forwarding correctly will cause Windows Updates to fail.

Figure 11-19: Adding Corporate DNS to Forwarders

UC-DC Properties

Debug Logging | Event Logging | Monitoring | Security

Interfaces | **Forwarders** | Advanced | Root Hints

Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
fec0:0:0fff::1	<Unable to resolve>
fec0:0:0fff::2	<Unable to resolve>
fec0:0:0fff::3	<Unable to resolve>
192.168.0.10	Contoso-DC

☒ Use root hints if no forwarders are available Edit...

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

OK Cancel Apply Help

This page is intentionally left blank.

12 X-UM Connector Configuration

The procedure below describes how to configure the X-UM Connector by doing the following:

- Set the X-UM Connector configuration for customer environment.
- Create users in CloudBond 365 using the CloudBond 365 GUI – or use the life cycle management capability to create the users automatically.
- Add users to X-UM Connector (manually for now)

12.1 Set X-UM Connector configuration

1. Connect to X-UM Connector server via remote desktop
2. Edit C:\Program Files\Audiocodes\XUMConnector\Config\System.config
3. The full list of available parameters + detailed explanation can be found in C:\Program Files\Audiocodes\XUMConnector\Config\README-configuration
4. Below you can find the important parameters that in most of the installation the default value must be change:
 - **outboundHost** - The host or IP address for outbound connections – SBC/GW IP
 - **outboundPort** - The port for outbound connections
 - **proxyListenPort** - X-UM Connector listen port – You must open this port for incoming traffic on the X-UM FireWall
 - **exchUmNumber** - Number to dial to log to your Exchange UM mailbox (no need to enter the mailbox number when dialing via this number via the X-UM Connector)
 - **exchUmNoPin** - If true then no user PIN is required when dialing to Exchange UM.



Note: For more information about the System Configuration file, read C:\Program Files\AudioCodes\XUMConnector\Config\XUMConnectorConfiguration.rtf.



Note: Make sure you restart the XM service after changing the config file.

12.2 Create Users in CloudBond 365

You need to create the users on CloudBond to be able to use the X-UM solution.

There is manual creation one or many via import and automatic via Lifecycle Management that take the correct users from the Corporate AD.

For more information regarding working with the CloudBond Web Admin use the *LTRT-26319 CloudBond 365 and User Management Pack 365 Administration Guide Ver 7.6.*

12.3 Adding Users to X-UM Connector

The procedure below describes how to add users to X-UM server. The users must be enabled for Skype Enterprise Voice. There are three options for managing the users:

- Manual procedure using a csv file
- Active Directory Sync schedule script
- REST API

➤ **to add users to X-UM Connector:**

1. Connect to X-UM Connector server via remote desktop.
2. Edit the C:\Program Files\AudioCodes\XUMConnector\Users\users.csv file.



Note:

- Changes made to the file are immediately applied. There is no need to restart the service.
- For X-UM HA, the users file must be on network storage and accessible for all X-UM servers.

```
#
# This file contains the list of users for the application
# The file must be in CSV format with a header line containing
# field 'SipUri' and 'Extension'
# SipUri must be the full SIP URI of the user to register, for
# example 'sip:user1@example.org'
#
# The Extension field is used to map a phone extension
# registration and its SIP URI.
# Multiple extensions per user are supported by separating
# them with '|'. For example '4001 | 4002'.
# Sample file contents:
#
# SipUri,Extension
# sip:user1@example.net , 4001
#
# Empty lines, and lines beginning with '#' are ignored
#

SipUri,Extension
```

➤ **To run the Active Directory Sync script:**

1. Connect to X-UM Connector server via remote desktop.
2. Under C:\Program Files\Audiocodes\XUMConnector\UsersSync folder you can find the AD sync files:
 - ReadMe.txt – instruction how to set the AD sync
 - XumUsersSync.ps1 - This is the main powershell script, IT SHOULD NOT BE MODIFIED.
 - Config.ps1.DIST - This is the default distribution configuration file.
 - XumUsersSync.bat - This is a batch file convenience wrapper for running the synchronization script.

By default, synchronization is disabled (because it doesn't know the custom AD group name).

To enable synchronization, Save Config.ps1.DIST as Config.ps1 and edit it as follows:

- a. Change Enabled to \$true (Enabled = \$true)
 - b. Set GroupName to the AD group containing XUM users
 - c. Optional, set ExtensionAttribute to the attribute name containing the user extension. In Powershell, run 'Get-ADUser <user> -Properties *' to view all user property names and values.
Optional, Change CsvFilePath to CSV file path. By default it is the users.csv file in users folder in installation directory, and usually should not be modified.
If using XUM HA then you must change it to the network shared CSV users file.
 - d. Optional, change XUM Windows task scheduler schedule as needed. By default, it will run every night. The entry is under the "Audiocodes" folder in the task scheduler.
3. Testing Synchronization:

It is possible to run the synchronization task immediately from the task scheduler (under "Audiocodes" folder). This should generate a "log" directory and a log file in this directory with details of the last synchronization results. Verify that the users CSV file is updated accordingly.

12.3.1 Using REST API

You can manage users basic operations of Add, Delete, Edit user information using the REST API. The REST API format can be displayed in the Swagger Web interface, where you can view the API calls, parameters per API and the format of the result.

By default REST API is block from external, to allow the REST API from remote need to change it on the XUM configuration file.

This page is intentionally left blank.

13 Configure the SBC in X-UM Solution

The telephony connection between the PBX/IP PBX or PSTN to X-UM Standard is done via the SBC/gateway. In the example shown below, the PBX/IP PBX or PSTN is referred to as IP-PBX, where "A" is an IP-PBX extension or external number, and "B" is an IP PBX extension. For detailed flows see 2.3Section 2.3 Call Flows.

The following scenario will go via the SBC:

- **"A" call "B" on the IP PBX, and call is forward to Exchange UM to leave a voice message**

In this scenario the SBC will route the call to the Mediation server running on the Front End Server on the X-UM Standard.

SBC will have to manipulate the numbers to match the users numbers format.

- **"A" call to login to Exchange UM**

In this scenario the SBC will route the call to the X-UM Connector.

X-UM will convert "A" to user SIP URI and will use it to login to the mailbox

SBC will have to manipulate the number to match the users numbers on the X-UM Connector user file. In this flow by default the direct login without enter the mailbox number and PIN.



Note: This scenario can be routed to the Mediation server instead of the special Exchange login number. In this case, the Exchange will ask you to enter mailbox "A" and the PIN.

- **MWI Interrogate (MWI Subscribe)**

In this scenario, the IP PBX checks the MWI state per extension (its used most of the time after phone/IP PBX reset) or if solicited MWI is used by IP PBX it is used to subscribe for the MWI presence.

The SBC will route these messages to the X-UM Connector.

SBC will have to manipulate the number to match the users numbers defined in the X-UM Connector user file.

13.1 MWI Notify

In this scenario the X-UM Connector send MWI SIP Notify to IP PBX

The SBC will route these messages from X-UM Connector to IP PBX

SBC will have to manipulate the number to match IP PBX extensions.

X-UM Connector supports solicited MWI and unsolicited MWI.

- **Play on Phone**

In this scenario the user can use the play- on phone feature on Exchange UM – when the user wishes to listen to a voice message, they can replay the message on the phone instead of using the computer.

In case the user enters the SIP URI or User Tel URI as a destination, the call will be sent via the X-UM Connector to the SBC and to the IP PBX.

In case the user enters a non-user number, the call is sent via the Mediation server to the SBC and to the IP PBX.

The SBC needs to route these calls correctly.

■ Callback

One of the following scenarios:

- The user logs into the mailbox and dials to the person who left the voice message.
- When calling to a user SIP URI or User Tel URI via the X-UM Connector to the SBC and to the IP-PBX.
- In case, the user enters a non-user number, the call is sent via the Mediation server to the SBC and then to the IP-PBX.

13.2 X-UM Connector SIP Interface

The X-UM SIP interface supports TCP only. The default listening port is 5070, however can be changed via the Configuration file.

X-UM answers to SIP Option messages – the SBC can check that the X-UM connector is up via the Option messages.

13.3 SBC Configuration Important points

The SBC must be set to work in Skype for Business according to SBC documentation (for example: Handle refer locally, security settings). According to the above scenarios, set the routing between the IP PBX and the X-UM Connector and Mediation server.

Number manipulation should be done according to the Skype user Tel URI and according to the X-UM users file that holds phone numbers for mapping between SIP URI and IP PBX phone numbers.

14 Using X-UM Connector Debugging tools

This section describes the following X-UM Connector debugging tools:

- X-UM Log
- X-UM Connector Running in Console Mode
- Syslog
- OCS Logger and Wireshark

14.1 X-UM Log

The X-UM Connector writes logs to "C:\Program Files\AudioCodes\XUMConnector\log .

14.2 X-UM Connector Running in Console Mode

When you run X-UM Connector in Console mode, it will provide an online console containing the log messages.

➤ **To run the X-UM Connector in console mode:**

1. Stop the AudioCodes XUM Connector service.
2. Search for 'Run XUMConnector' in Console mode and run it as the Administrator.
3. When you complete the debug, stop the console by pressing "q" and run the service again.

14.3 Syslog

The X-UM Connector supports Syslog.

➤ **To configure Syslog :**

1. Connect to X-UM server using Remote Desktop.
2. Edit the C:\Program Files\AudioCodes\XUMConnector\Config\System.config file.
3. Add and configure the following parameters:
 - **syslogEnabled** - Enables logging to the Syslog server. The default value is 'False'.
 - **syslogServer** – Defines the Syslog server IP address.



Note: The *syslogServer* value must be an IPv4 address. Names are not allowed because IPv6 is not supported. The default value is "127.0.0.1".

- **syslogPort** - Syslog server port DefaultValue = "514"

14.4 OCS Logger and Wireshark

OCS Logger and Wireshark can be used to take traces of the SIP messages.

The tools can be found under C:\Program Files\AudioCodes\XUMConnector\Tools.

15 Re-Image X-UM Standard

Sometime Re-Image of the the X-UM Standard system is required. Thisis done by using a dedicated USB that comes with the product.

Refer to Section 11 in LTRT-26599 CloudBond 365 Installation Manual Ver 7.6. for detailed instruction on how to Re-Image – this document is general for all CloudBond365 products, the X-UM is based on the Standard Plus platform.

When the CB365 is ready, users must add an extra VM for the X-UM (in the next major version CB365 uninstallation will create and set the X-UM Connector VM).

15.1 Download Latest Version

Download a clean Windows 2012R2 VHDX from:

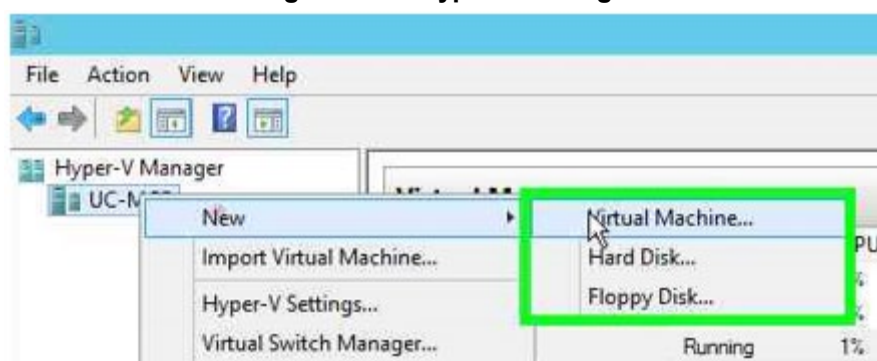
https://s3.eu-central-1.amazonaws.com/downloads-audiocodes/Download/AC_CCE_VHDX.html

Unzip it to X-UM Standard host: 'D:\Hyper-V\Virtual Hard Disks' and rename it to xUM

15.2 Create the X-UM Connector VM

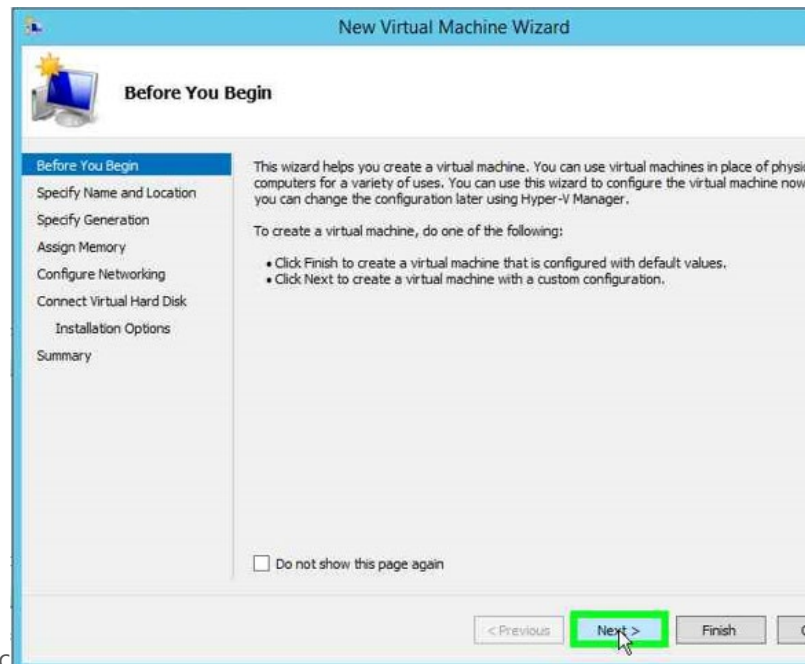
1. Open the **Hyper-V Manager**.
2. Right-click on **UC-MGR** (tree item); the following screen appears:

Figure 15-1: Hyper-V Manager



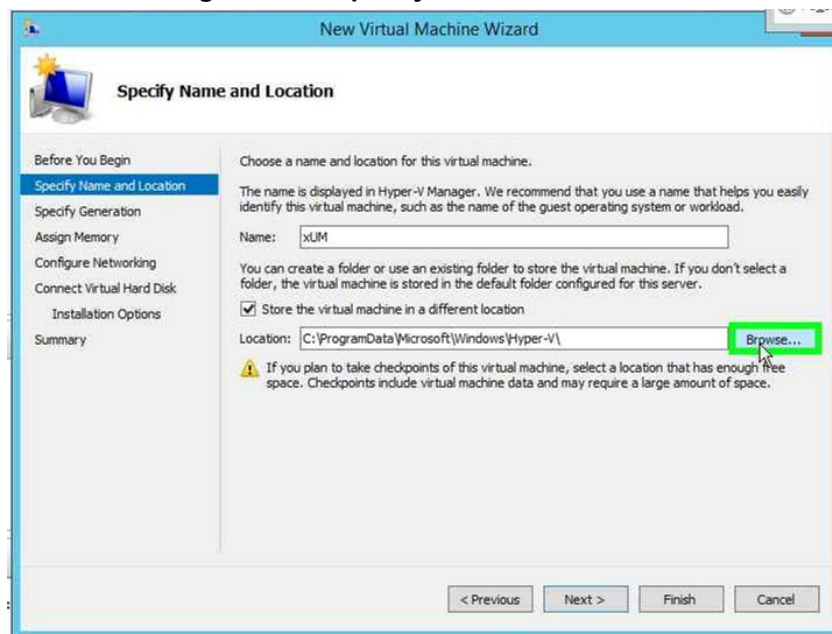
3. Click **New**; and then select **Virtual Machine**; the following screen appears:

Figure 15-2: Before You Begin



4. Click **Next**; the following screen appears:

Figure 15-3: Specify Name and Location



5. In the 'Name' field, enter "XUM".
6. Select the 'Store the virtual machine in a different location' check box.
7. Click **Browse**.
8. In the 'Location' field, enter "d:\Hyper-V".
9. Click **Next**.

Figure 15-4: Specify Name and Location

The screenshot shows the 'Specify Name and Location' step of the 'New Virtual Machine Wizard'. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location' (selected), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', and 'Summary'. The main area contains instructions to choose a name and location. The 'Name' field is set to 'XUM'. The 'Location' field is set to 'D:\Hyper-V\'. A checkbox labeled 'Store the virtual machine in a different location' is checked. A warning icon and text state: 'If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.' At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

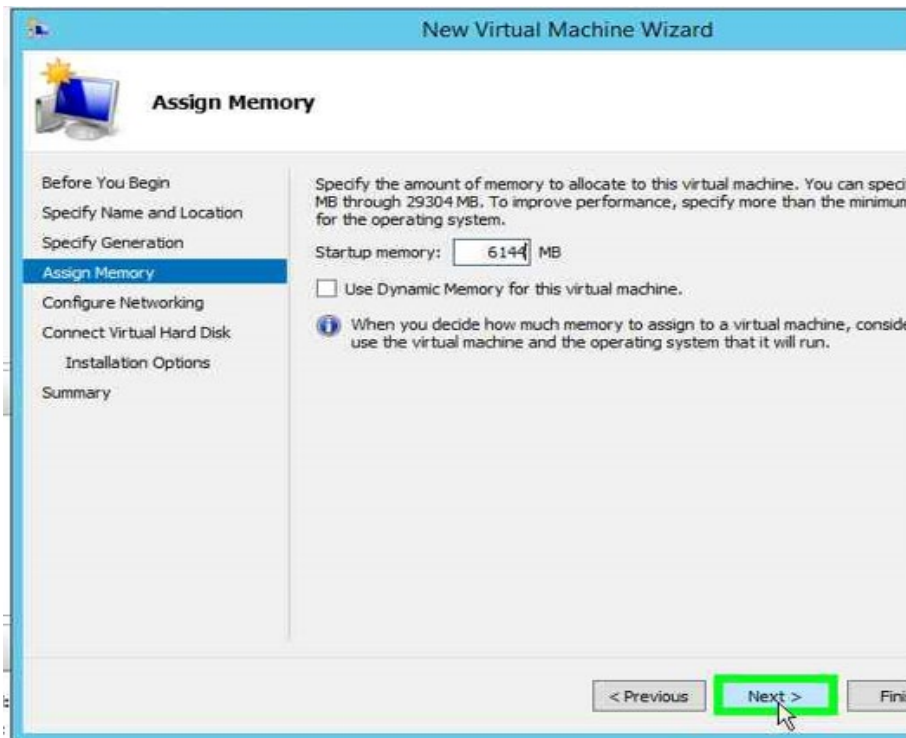
10. Click **Next**; the following screen appears:

Figure 15-5: Specify Generation

The screenshot shows the 'Specify Generation' step of the 'New Virtual Machine Wizard'. The left sidebar lists the steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation' (selected), 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions to choose the generation. Two options are listed: 'Generation 1' (selected with a radio button) and 'Generation 2'. A warning icon and text state: 'Once a virtual machine has been created, you cannot change its generation.' At the bottom are buttons for '< Previous', 'Next', and 'Finish'. The 'Next' button is highlighted with a green rectangle and a mouse cursor is pointing at it.

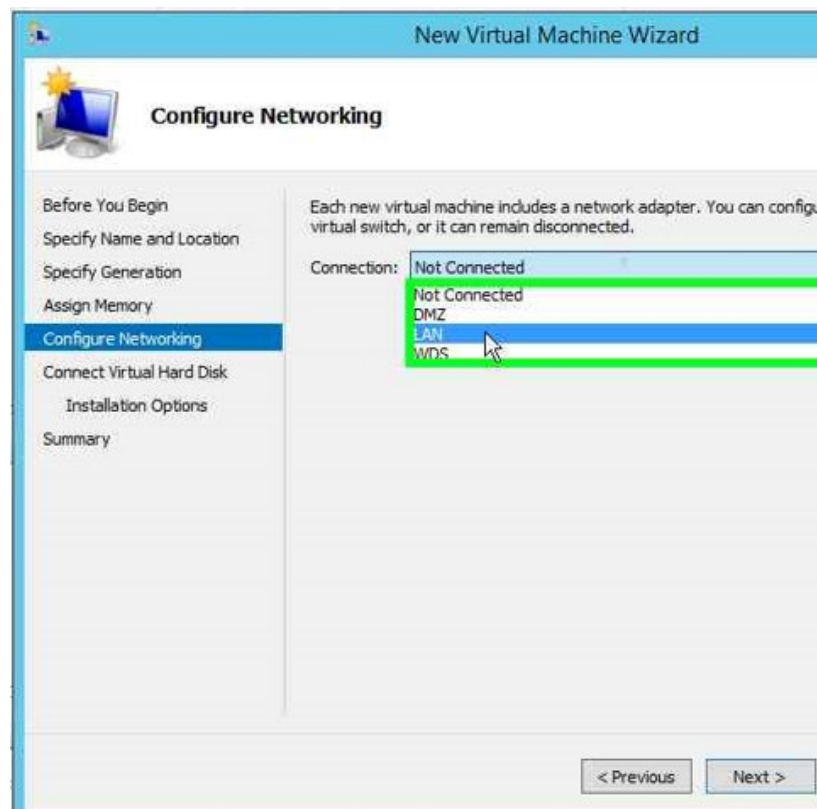
11. Click the **Generation 1** option, and then click **Next**; the following screen appears:

Figure 15-6: Assign Memory



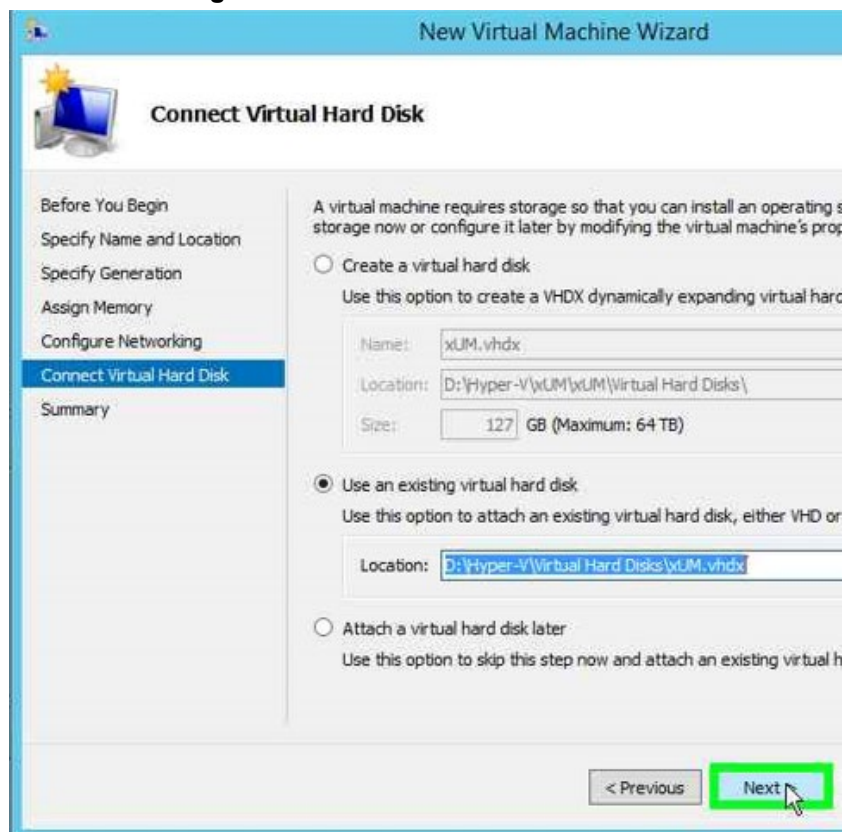
12. In the 'Startup memory' box, allocate **6144 MB** to the machine, and then click **Next**; the following screen appears:

Figure 15-7: Configure Networking



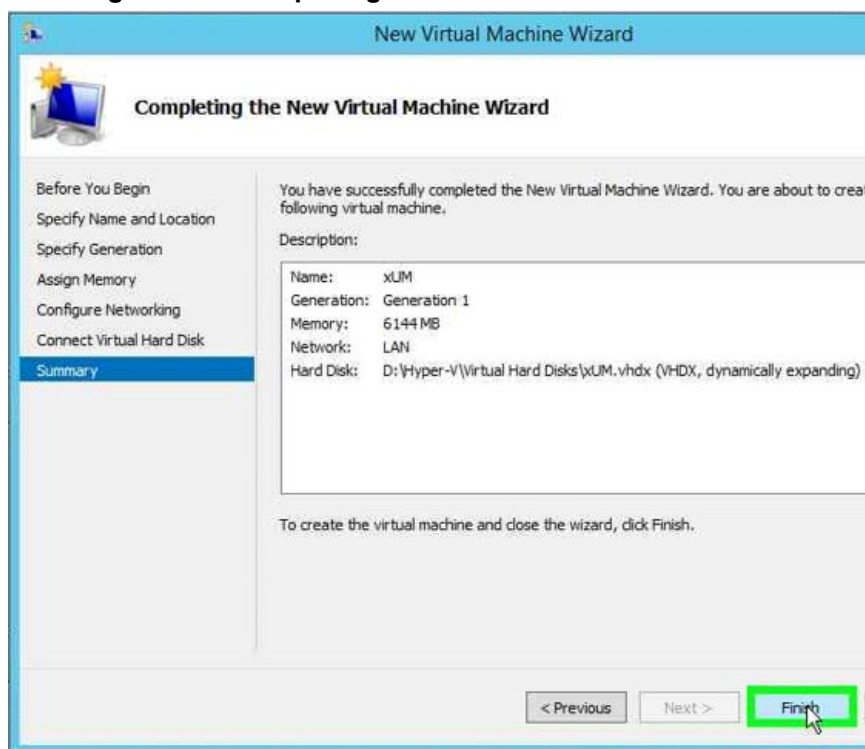
13. From the 'Connection' drop-down list, select **LAN**; and then click **Next**.

Figure 15-8: Connect Virtual Hard Disk



14. Click the **Use an existing virtual hard disk** option.
15. In the 'Location' field, browse to **D:\Hyper-V\Virtual Hard Disks\xUM.vhdx**.
16. Click **Next**.

Figure 15-9: Completing the New Virtual Machine Wizard



17. Click **Finish**.

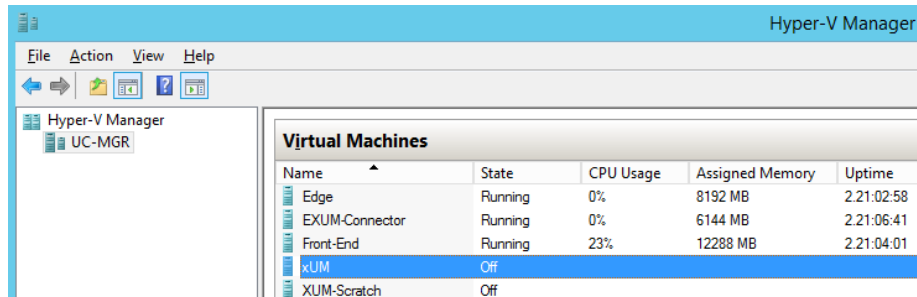
15.3 Configuring X-UM Connector VM

The procedure below describes how to configure the Virtual Machine.

- **To configure the X-UM Connector Virtual Machine:**

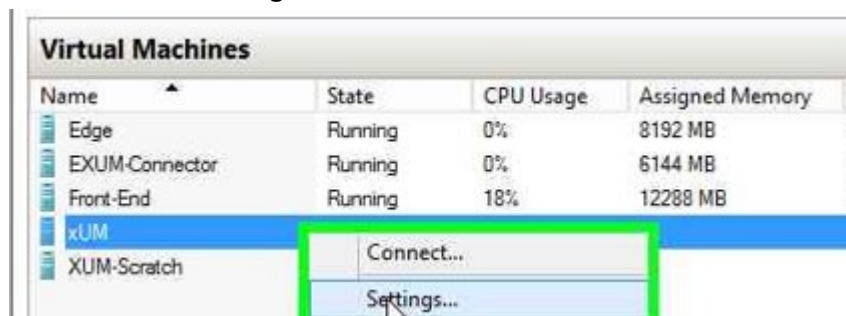
1. Start the **Hyper-V Manager**.

Figure 15-10:Hyper-V Manager



2. Right-click on 'xUM', and then select **Settings**.

Figure 15-11:Virtual Machines



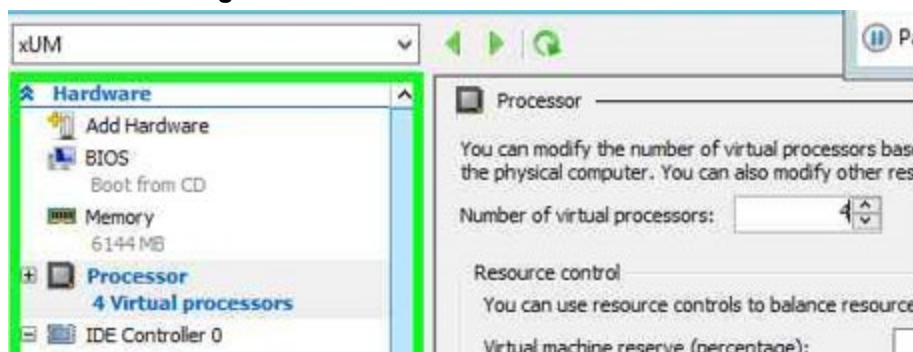
3. From the 'Settings' drop-down list, select **Processor**.

Figure 15-12:Processor Settings



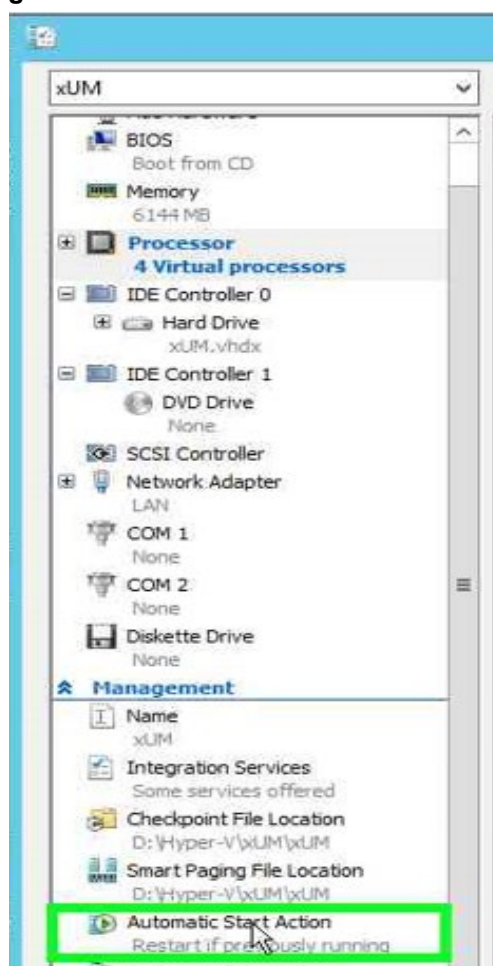
4. From the 'Hardware' drop-down list, modify the number of virtual processors to **4**.

Figure 15-13: Number of Virtual Processors



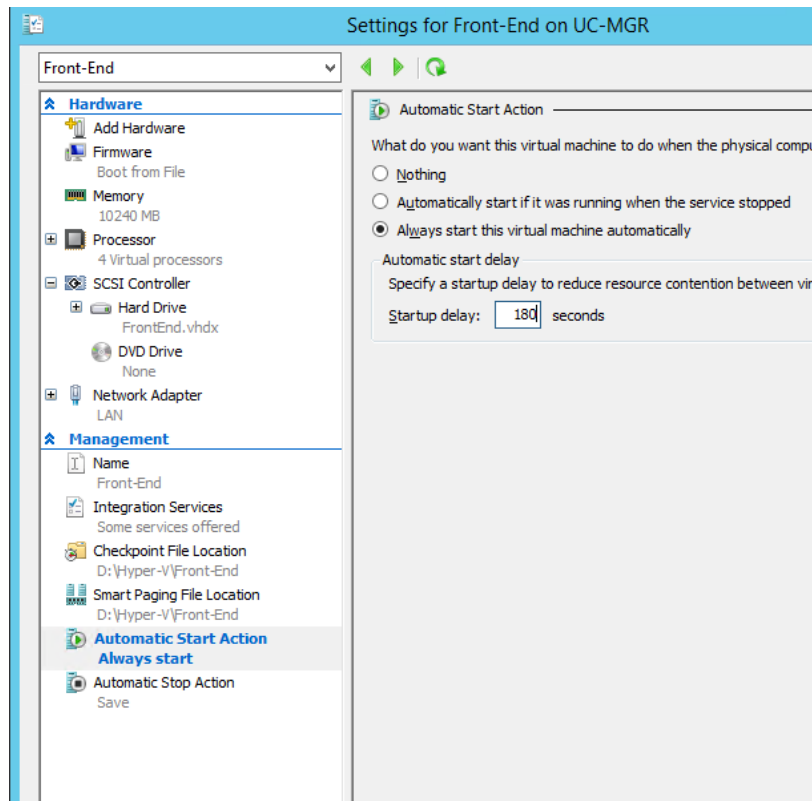
5. From the 'X-UM' drop-down list, select **Automatic Start Action**.

Figure 15-14: X-UM - Automatic Start Action



6. Select "Always start this virtual machine automatically", In the 'Startup delay' field, enter "180" seconds , and then click **OK**.

Figure 15-15:X-UM - Automatic Start Action – Startup Delay

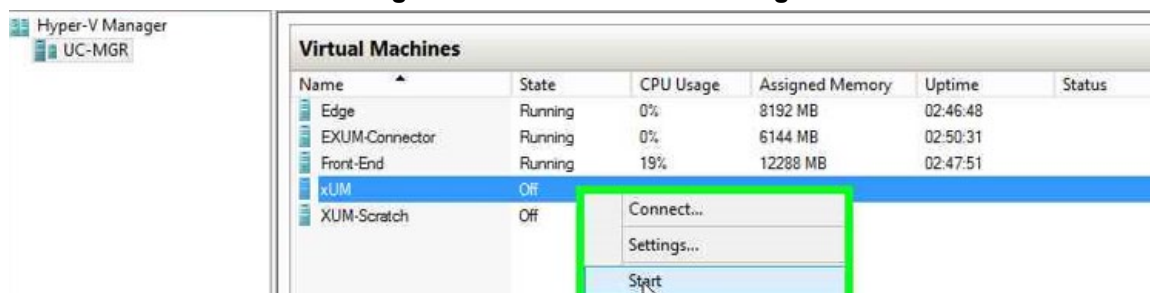


15.4 Starting the X-UM Connector Virtual Machine

➤ To Starting the X-UM Connector Virtual Machine:

1. On the Hyper-V Manager – Virtual Machines screen. right-click **X-UM**, and then select **Start**.

Figure 15-16:X-UM – Start Settings



2. Start the Virtual Machine, and then enter your local user name and password.

15.5 Windows 2012R2 Server Role & Features

Validate that all the below '**Server Role**' and '**Feature**' are enable via the Server Manager

- Server Role to enable:
 - File and Storage Services – File and iSCSI Services – File Server
 - File and Storage Services – Storage Services
- Feature to enable:
 - .Net Framework 3.5 Feature - .Net Framework 3.5
 - .Net Framework 4.5 Feature - .Net Framework 4.5
 - .Net Framework 4.5 Feature – WCF Service – TCP Port Sharing
 - Media Foundation
 - SMB 1.0/CIFS File Sharing Support
 - User Interface and Infrastructure – Graphical Management Tools and Infrastructure
 - User Interface and Infrastructure – Server Graphical Shell
 - Windows PowerShell – Windows PowerShell 4.0
 - Windows PowerShell – Windows PowerShell 2.0 Engine
 - Windows PowerShell – Windows PowerShell ISE
 - WoW64 Support

15.6 Set IP

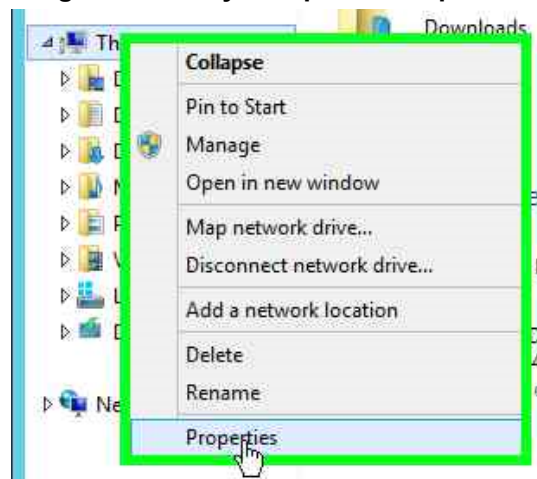
Set the X-UM Connector Network interface with the correct IP, Subnet, Default GW and DNS should be set to point to the X-UM Standard controller.

15.7 Add X-UM Connector to Domain

The procedure below describes how to add the machine to the domain.

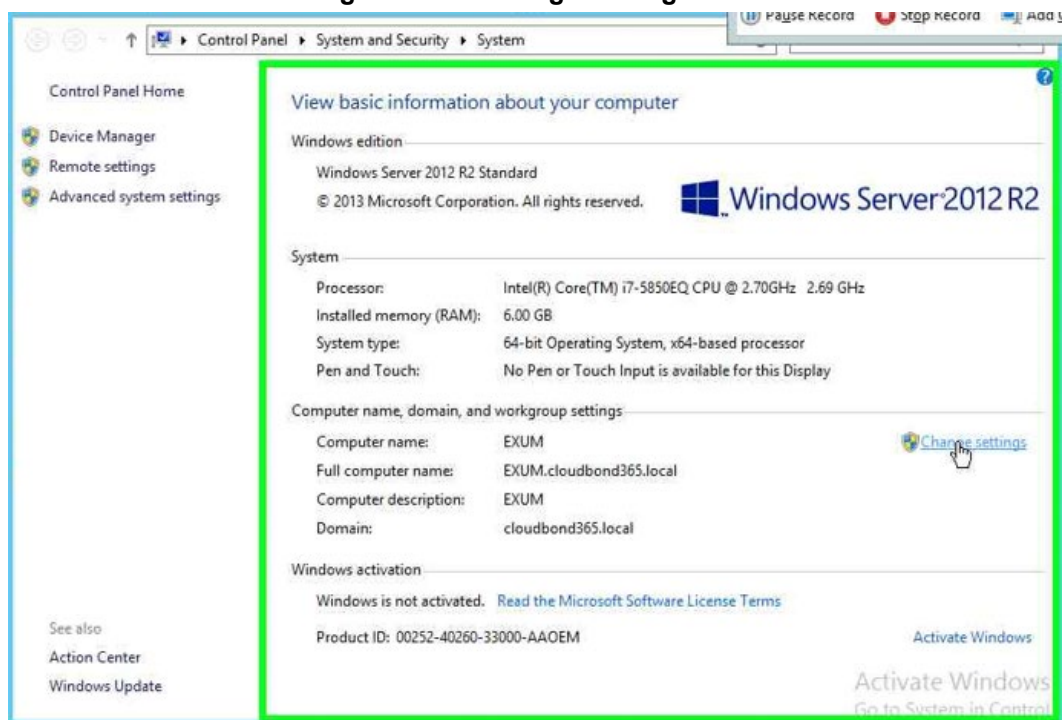
- **To add a machine to the domain:**
 1. Log in to the machine as a local user.
 2. From the Desktop, select the My Computer icon and right-click to view the settings.
 3. Select **Properties**.

Figure 15-17: My Computer - Properties



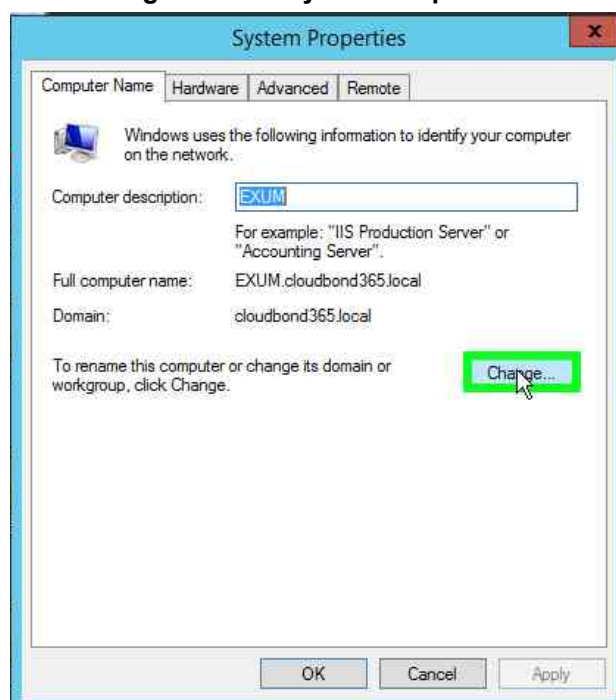
4. On the Windows Server 2012 R2 screen, click **Change settings**.

Figure 15-18:Change Settings Link



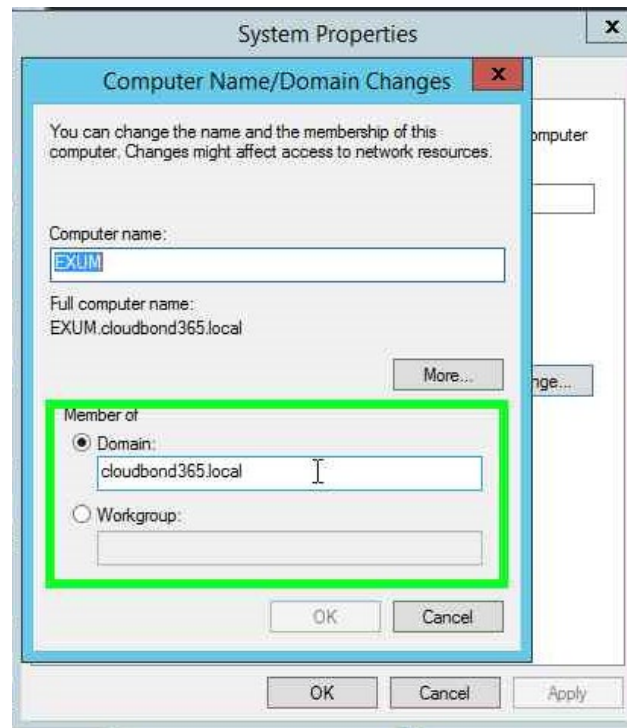
5. On the System Properties screen, click **Change**.

Figure 15-19:System Properties



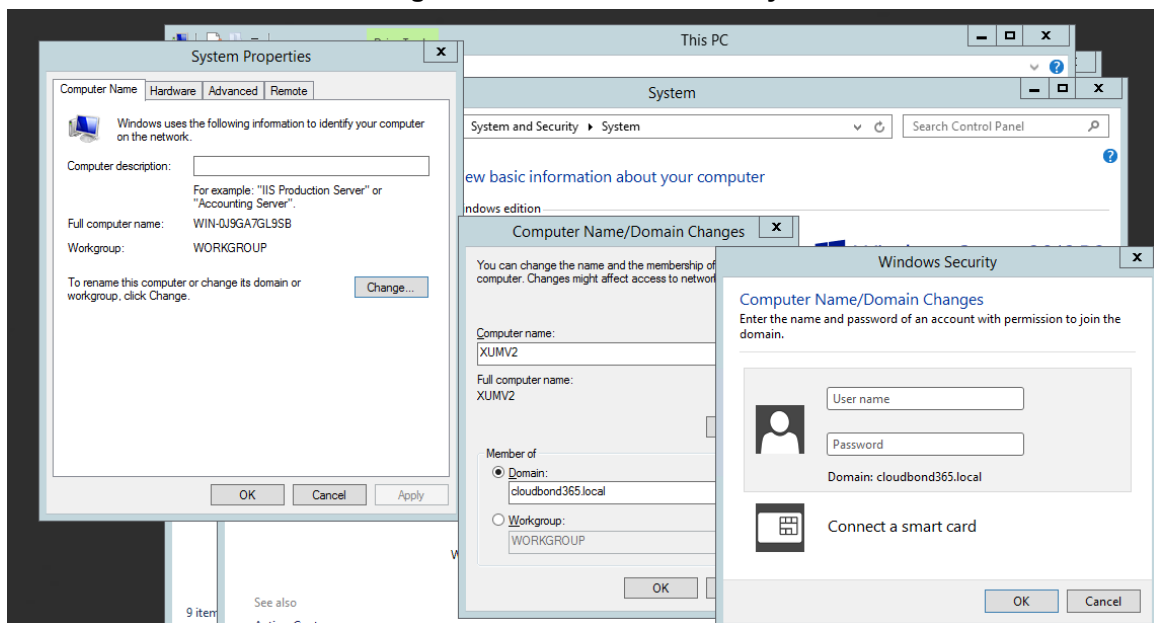
6. Change the **Computer Name** and **Domain**, and then click **OK**.

Figure 15-20: System Properties - Change



7. Insert the user name and password of the CloudBond domain, and then click **OK**.

Figure 15-21: Windows Security



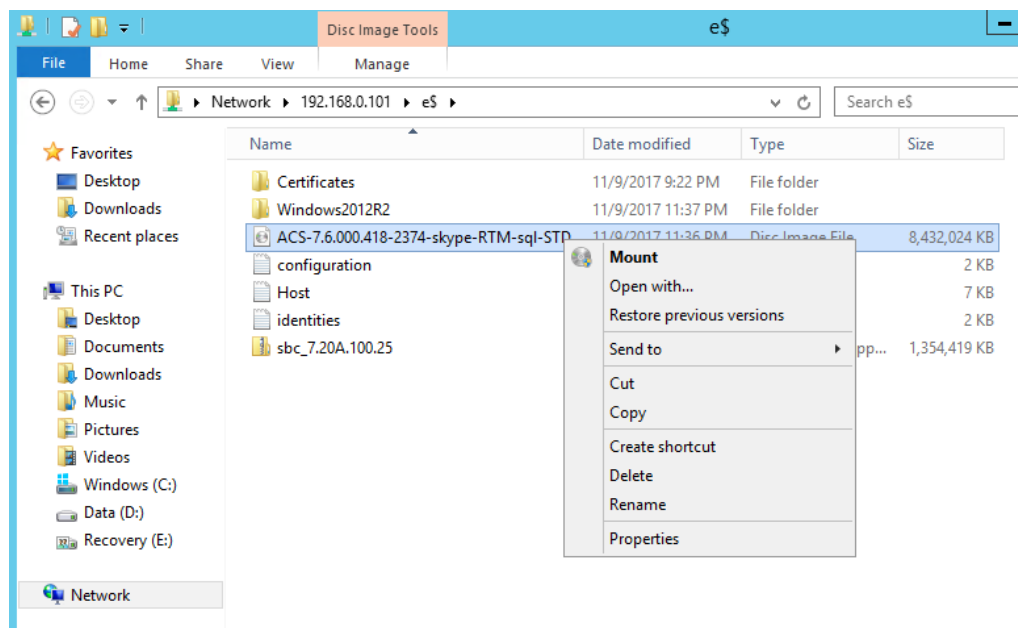
8. Restart the X-UM Connector VM.

15.8 Install UCMA 5

Log into X-UM Connector with domain credentials. The procedure below describes how to install the Unified Communications Managed API (UCMA) 5.0.

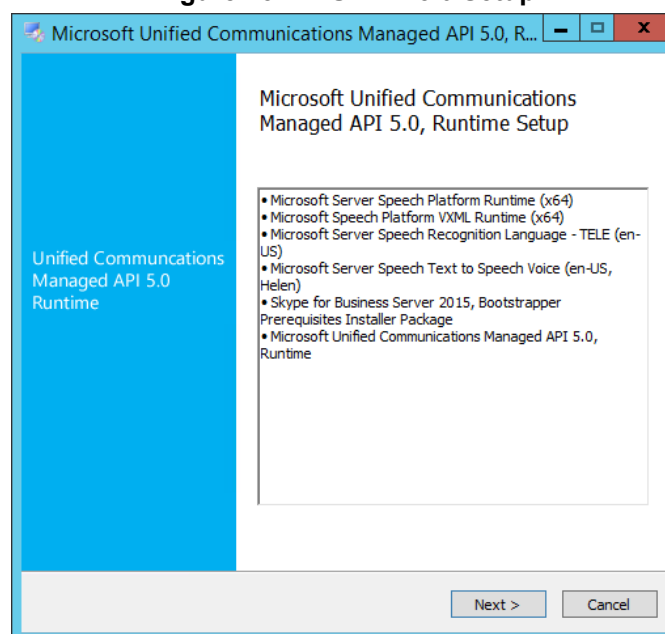
➤ **To install UCMA5:**

1. Open Network path: **Error! Hyperlink reference not valid. Standard Controller IP>\e\$**



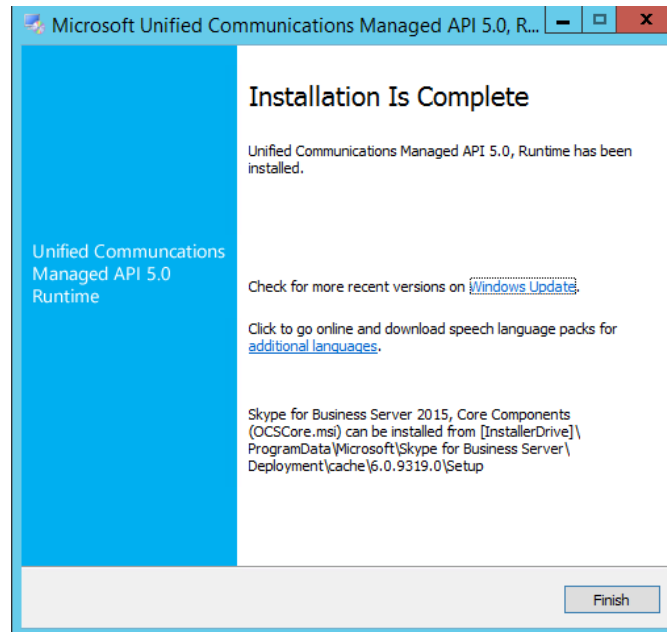
2. Mount the iso
3. Browse to <Mounted Disk>:\ThirdParty\UCMARuntime.
4. Run UcmaRuntimeSetup As administrator.

Figure 15-22: UCMA 5.0 Setup



5. When the installation has completed, the following screen appears:

Figure 15-23: Installation Complete



6. Click **Finish**.

15.9 Installing Skype for Business Component

The procedure below describes how to install the Skype for Business (Local Configuration Store) component using Skype for Business Deployment wizard, and the Skype For Business cumulative update (CU).

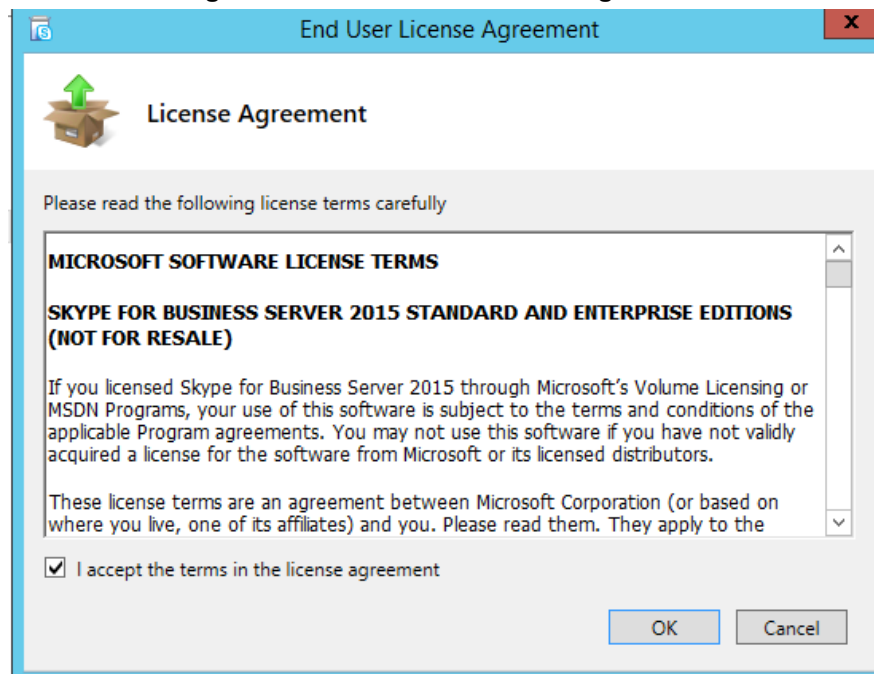
Log to X-UM Connector with domain credentials.

➤ To install Skype for Business local Configuration Store:

1. Open Network path: **Error! Hyperlink reference not valid.** *Standard Controller IP>\\e\$*
2. Mount the iso
3. Browse to <Mounted Disk>:\\SkypeRTM\\Setup\\amd64
4. Run as Administrator the Microsoft Deployment wizard *Setup.exe*

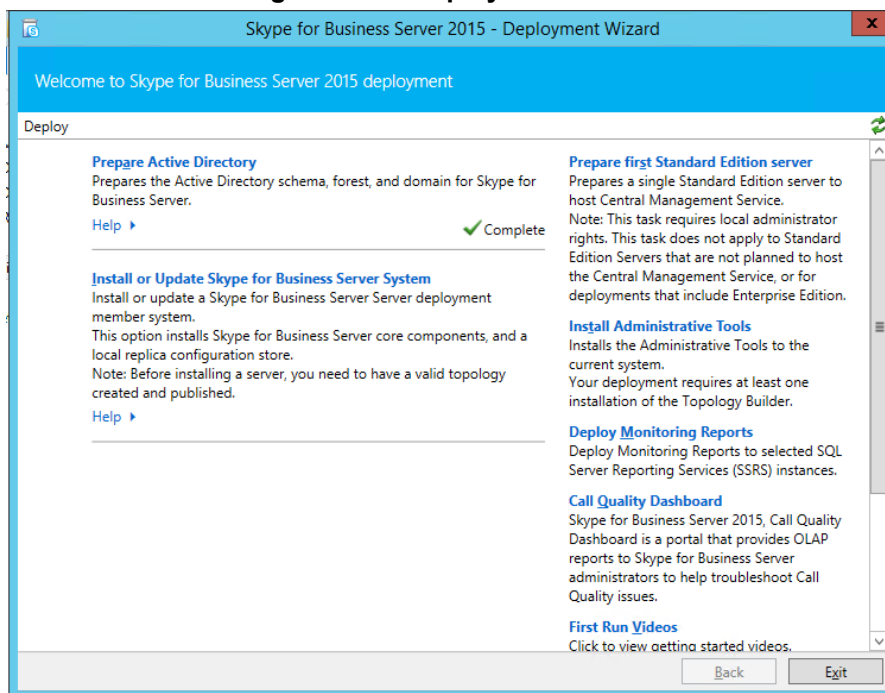
Figure 15-24: Skype for Business Server – Check Updates

5. Click the **Connect to the internet to check for updates** option, and then click **Install**.

Figure 15-25: End User License Agreement

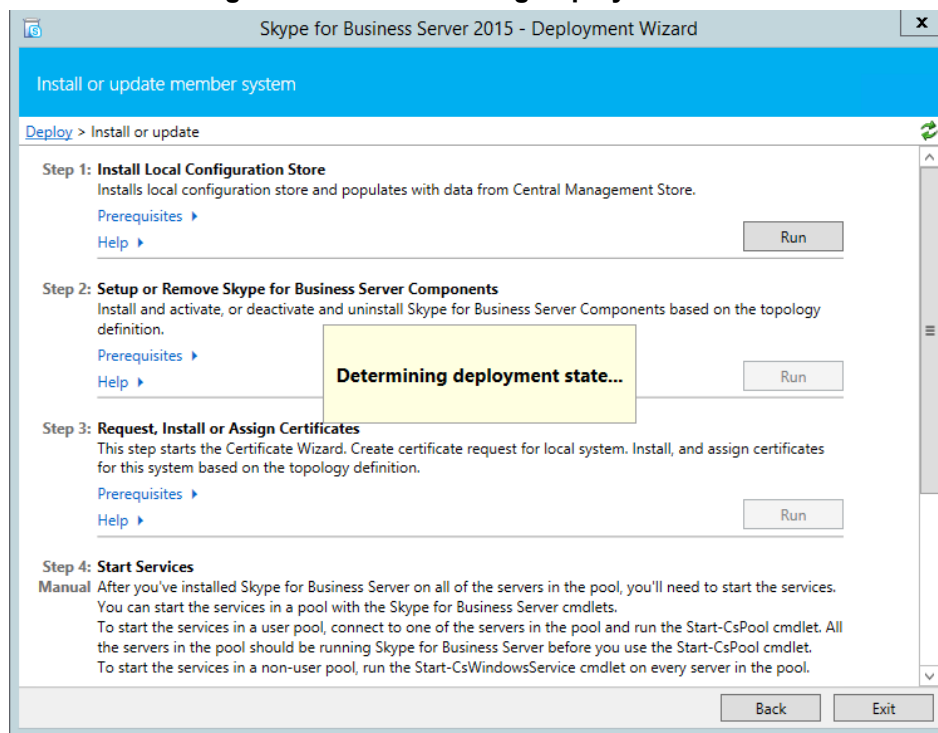
6. Accept the terms in the license agreement, and then click **OK**; the following screens appear:

Figure 15-26:Deployment Wizard



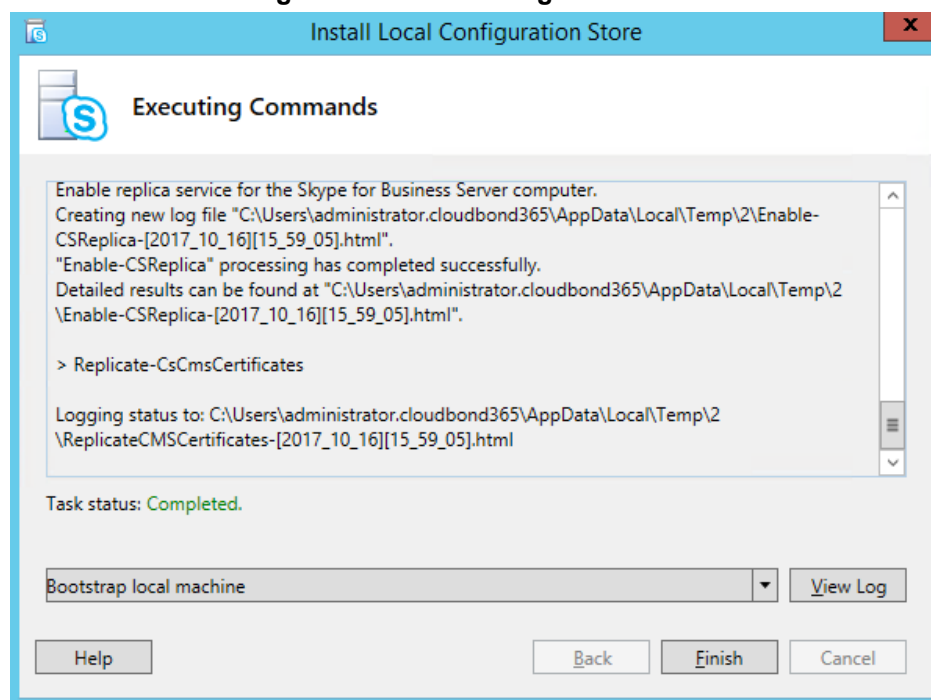
7. Click **"Install or Update Skype for Business Server System"** ; the following screens appear:

Figure 15-27: Determining Deployment State



8. Click **Step 1: "Install Local Configuration Store"**; the installation runs and upon completion, the following screens appears:

Figure 15-28: Executing Commands



9. Click **Finish**.

➤ **To install Skype for Business local CU:**

1. Open PowerShell and stop Skype Services:
Stop-CsWindowsService
2. Browse to <Mounted Disk>:\Updates
3. Run as Administrator *SkypeServerUpdateInstaller.exe* (in case a newer CU already installed on the X-UM, install the same CU version on the X-UM connector instead of the CU from this path).

15.10 Installing X-UM Connector Application

The procedure below describes how to install the X-UM application using the X-UM Connector wizard setup file.

Download the latest X-UM Connector from:

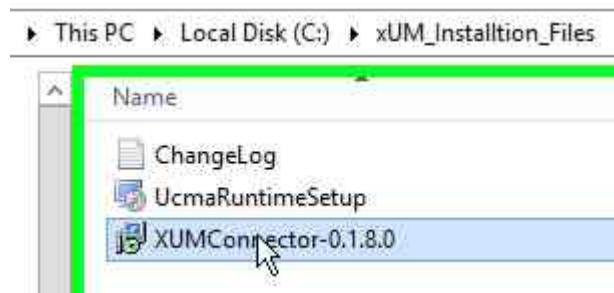
https://s3.eu-central-1.amazonaws.com/downloads-audiocodes/Download/AC_XUM_Install.html

Copy it to C:\xUM_InstalltionFiles on the X-UM Connector VM.

➤ **To install the X-UM Connector Application:**

1. Run the X-UM setup file from **C:\xUM_InstalltionFiles\XUMConnector-x.x.x.x.msi**.

Figure 15-29: Run XUMConnector File

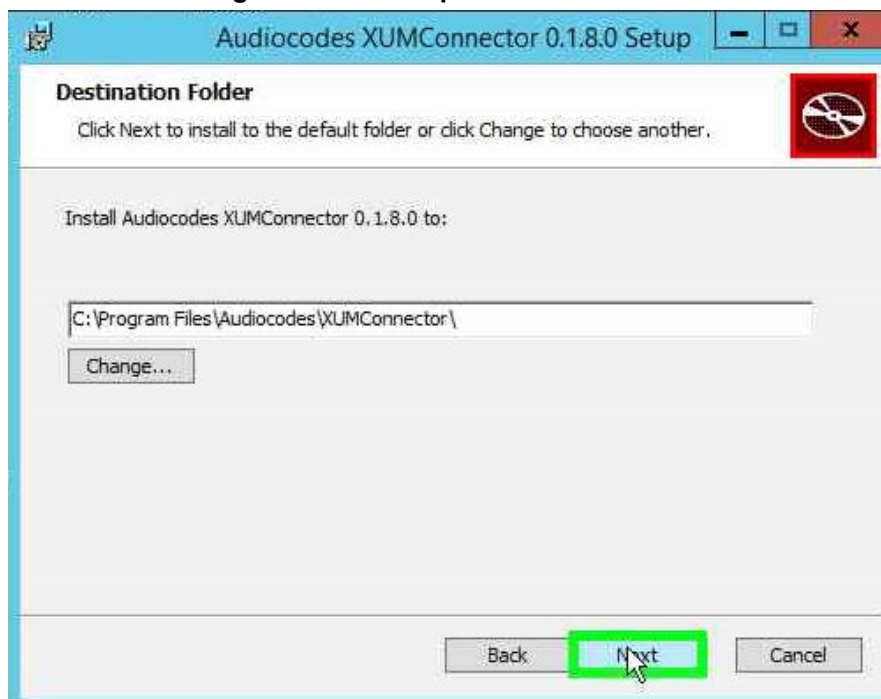


The following screen appears:

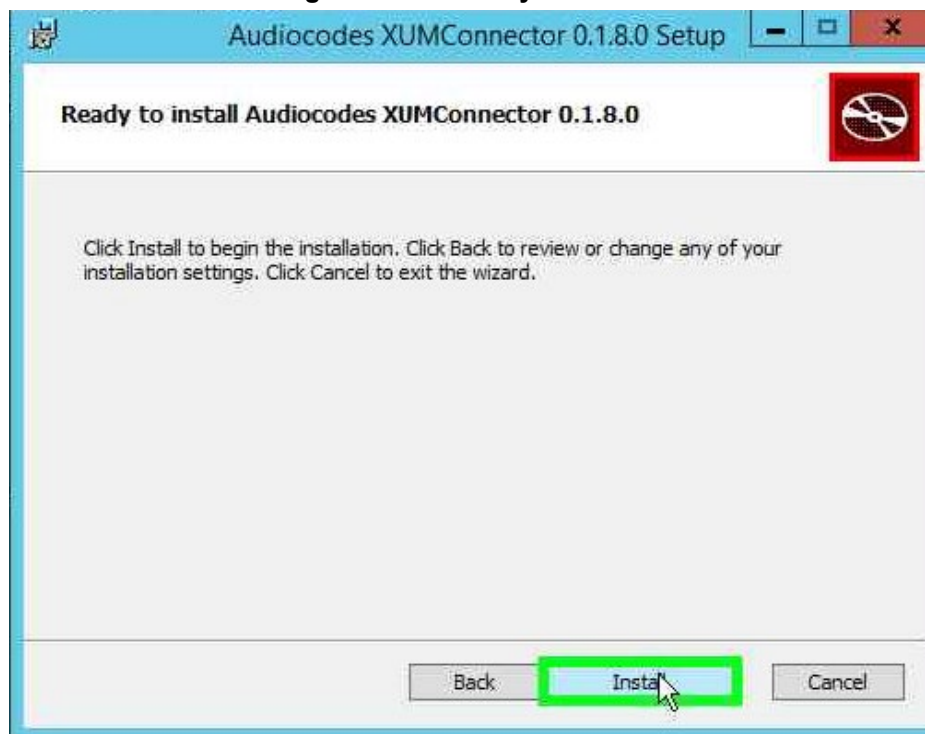
Figure 15-30: XUMConnector File Setup



2. Click **Next**.

Figure 15-31: Setup Destination Folder

3. Confirm the Destination Folder, and then click **Next**.

Figure 15-32: Ready to Install

4. Click **Install**.

Figure 15-33: Setup Complete



5. Click **Finish**.

15.11 Activating X-UM Connector

The procedure below describes how to activate XUMConnector on the Skype for Business environment (Trusted application).

➤ To activate X-UM Connector:

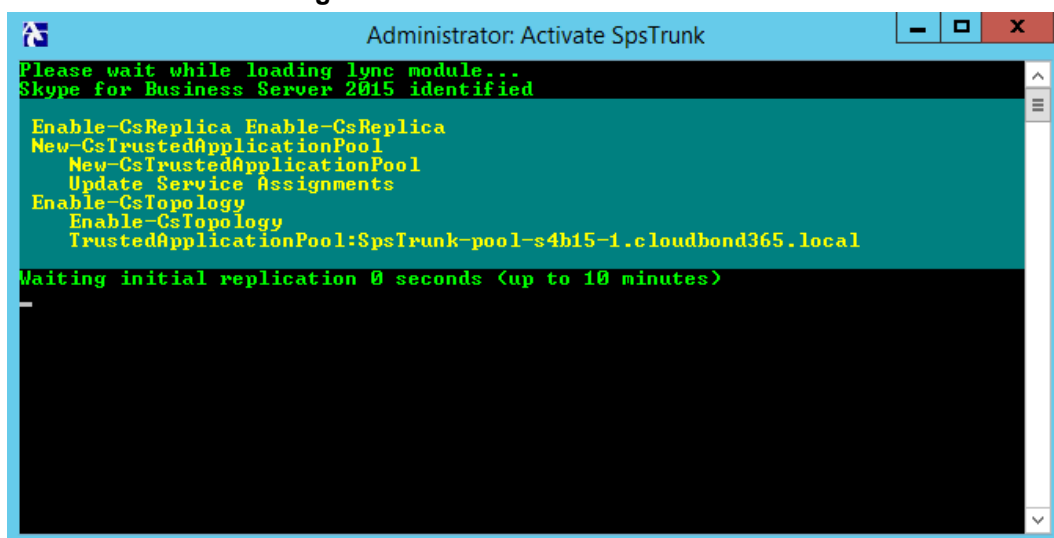
1. From the Windows menu, right-click on **Search** pane.
2. Enter "activate".
3. Right-click **activate XUMConnector**.

Figure 15-34: Search



4. Click **Run as administrator**; the following screen appears:

Figure 15-35: Activate X-UM Connector



5. Follow the script messages.
 In the case of multi-sites, the script will prompt you to select site for the trusted application pool.
 In case there are several pools on the site, the script will prompt you to select the trusted application endpoint registrar.
6. Continue to the next sub-section.

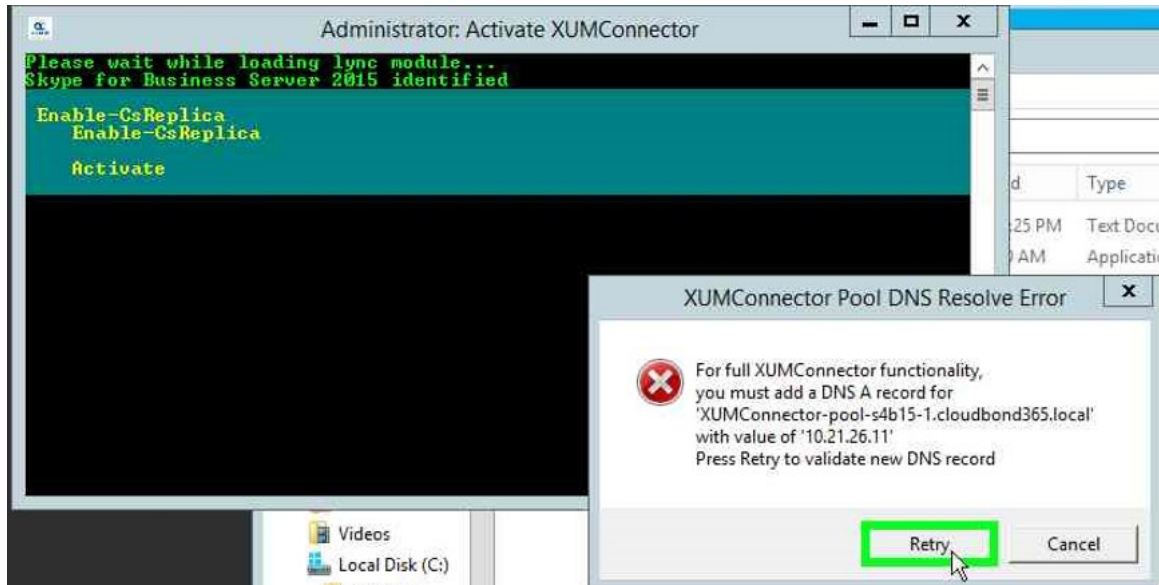
15.12 Adding DNS A Record

The procedure below describes how to add a DNS A record.

➤ **To add a DNS A Record:**

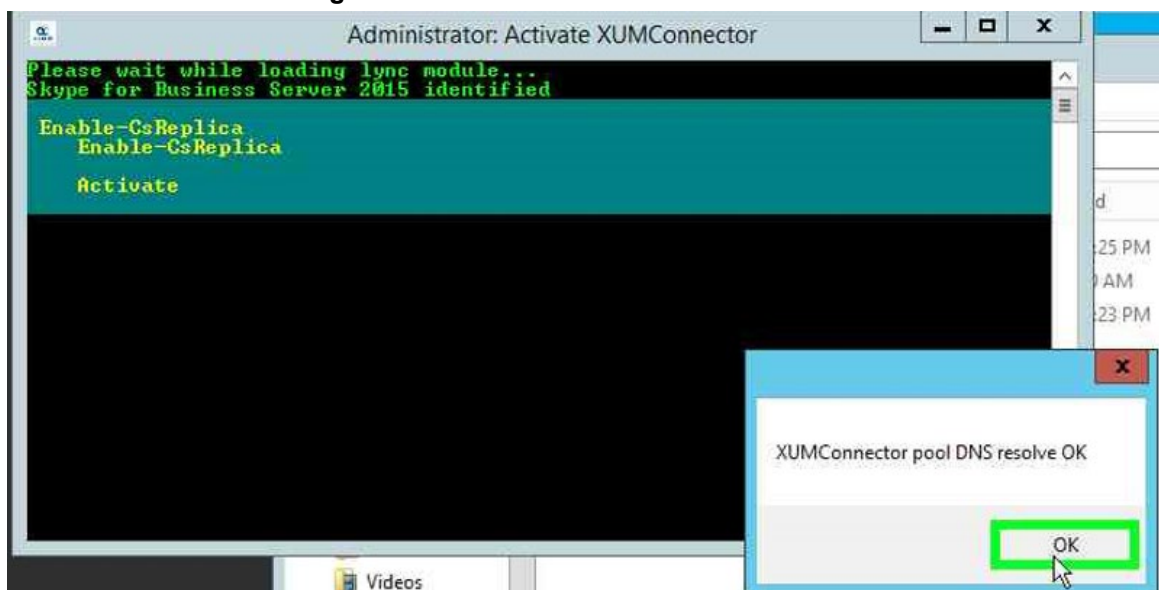
1. During the X-UM Connector Activate process (as shown above), a message appears advising you to add a DNS A record to the X-UM Standard DNS server.

Figure 15-36: Activate X-UM Connector



2. When the message shown above appears, add the DNS record manually on the DNS server that hosted on the X-UM Standard management server and then click **Retry** to recheck it.

Figure 15-37: Activate X-UM Connector - OK



3. Click **OK**.

Figure 15-38: Activate X-UM Connector – Activation Successful



```
Administrator: Activate XUMConnector
Verifying local replication is up to date...
Waiting for local replication update 0 seconds (up to 10 minutes)
Waiting for local replication update 5 seconds (up to 10 minutes)
Waiting for local replication update 10 seconds (up to 10 minutes)
Waiting for local replication update 15 seconds (up to 10 minutes)
Waiting for local replication update 20 seconds (up to 10 minutes)
Waiting for local replication update 25 seconds (up to 10 minutes)
Replication is up to date
Creating application endpoint 'sip:XUMConnector-s4b15-1@xum.com' for 'XUMConnector' on 'XUMConnector-pool-s4b15-1.cloudbond365.local'
Application endpoint 'sip:XUMConnector-s4b15-1@xum.com' for 'XUMConnector' on 'XUMConnector-pool-s4b15-1.cloudbond365.local' created successfully
Verifying local replication is up to date...
Replication is up to date

XUMConnector application activated successfully
You can safely close this windows

XUMConnector
PS C:\Program Files\Audiocodes\XUMConnector\Activation>
```

4. The screen displays a message that the activation was successfully completed.
5. Validate that the X-UM Connector service is running, service name: XUMConnector (Service display name: Audiocodes XUMConnector).
6. Now X-UM Connector is ready to be configured – proceed to Chapter 12 to set the system.

This page is intentionally left blank.

A HA and DR

There are several different levels of high availability / DR in a XUM environment:

- HA/DR on Skype level – for example enterprise users pool, pool pairing, etc.
- HA between XUM servers - the ability to provide XUM services if a XUM server fails.

A.1 HA/DR On Skype Level

X-UM works with Skype pools, pools with multi FE is "transparent" for X-UM that will work with the pool like other skype components. In case the FE is down, the X-UM connects to another FE from the pool like it does other Skype components.

In case pool pairing is used, the X-UM will be activated towards one pool.

While both pools are up, the X-UM provides full functionality for users from all pools.

When a pool is down and this pool holds the local store – you will need to fail over the local store to the active pool.

To supply full service for users from the fail pool, you will need to perform pool fail over as well.

A.2 HA On X-UM Level

XUM provides **automatic** HA for users by distributing the users between XUM servers.

Each user is automatically assigned a unique XUM server. If a server fails then another server takes over responsibility for this user.

XUM HA is implemented without any manual configuration.

There is no limit to the number of XUM servers that can participate in HA. All servers take part in HA (there is no standby server), and they all distribute the users evenly between them, more or less.

Each XUM sends and listens to 'ImAlive' messages using **UDP multicast address**. By using this multicast address, each server automatically discovers all servers, and there is no need to configure the list of servers.

A.2.1 Conditions for HA

Each XUM server is configured with a path to a CSV file containing the list of users.

By default, this CSV file is local file, located at 'Users\users.csv' relative to the XUM installation location.

XUM HA will only be activated if the users file is located at a shared network location. Therefore, HA is disabled by default until a shared network path is defined for the users file.

Specifically, HA is activated only if the users file starts with ".

A.2.2 Incoming Messages Redirection

In an HA environment, incoming messages from the proxy side (SBC/GW) should reach the HA user owner server. This is relevant for the following example scenarios:

- User MWI subscribe session
- User extension dial (if enabled)

Note that VM access call (*151) are not redirected, because an impersonated application endpoint is used in an outgoing call to Lync.

Also note that VM direct deposit prefix (*55) calls are also not redirected, because isn't necessarily an HA owner for the call (it can be from any PSTN number!).

Since the proxy server is not aware of the current user owner server, XUM replies with a **SIP redirect** response to the HA user owner server. The redirect address is taken from the ExtraData field sent by each server.



Important: The redirect messages destination is the server FQDN, not the IP address. This means that the proxy (SBC) must be configured to use a DNS that can resolve the XUM host names.

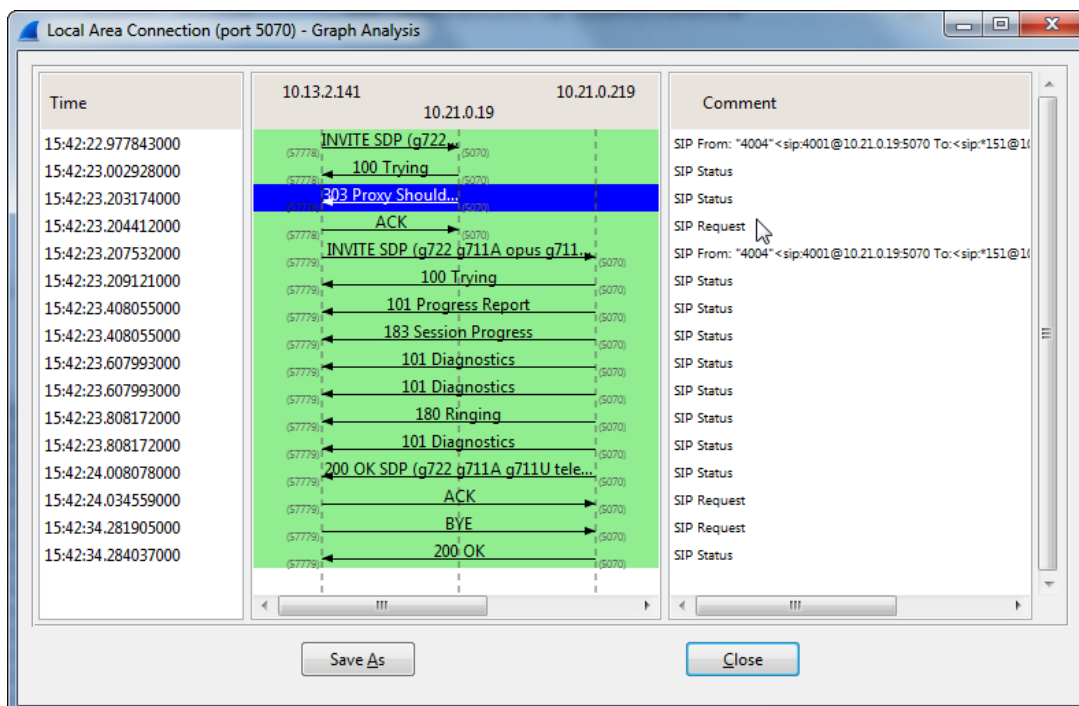
An example contact header of a redirect message:

CONTACT: <sip:ron-devel-02.lync2013.net:5070;transport=Tcp>

Below is a sample redirect call flow by a user to access their voicemail:

1. Proxy server 10.13.2.141 sends invite to XUM1 at 10.21.0.19.
2. XUM1 receives invite from user. It finds that user is not managed locally, but on XUM2 at 10.21.0.219.
3. XUM1 sends the proxy a 303 redirect to 10.21.0.219.
4. Proxy sends a new invite to 10.21.0.219, and call continues normally.

Figure A-1: Local Area Connection



A.2.2.1 Proxy Configuration

Ideally, the proxy (SBC) should be configured to distribute load between all HA servers, while periodically checking that all servers are alive.

The list of servers can be configured manually, or resolved using the common XUM DNS pool address that should be configured in DNS to all XUM servers.

In any case, the proxy periodically verifies that the server is still alive, possibly using SIP options request.

A.2.3 Web GUI Swagger

Web GUI via Swagger is available for:

- Getting HA status – including list of all HA servers and their uptime
- Getting users owner – the calculated owner of each user.

This page is intentionally left blank.

B Known Issues

This appendix describes known issues.

B.1 User File Name does not Support “\$” Char

When setting X-UM to work in HA, the user file name must be a network path. “\$” sign in the user file name is not valid and generates an exception in the log:

```
Feb 20 13:02:13 VM-qa-xum-01 XUMConnector13:02:13 Warn Failed to
parse file '\\USIDMLLYC111\d$\X-UM\users.csv'
EXCEPTION --> UnauthorizedAccessException Access to the path
'\\USIDMLLYC111\d$\X-UM\users.csv' is denied. at
System.IO.__Error.WinIOError(Int32 errorCode, String
```

B.2 Using the REST Swagger Client with Internet Explorer

When using the Swagger REST management interface, its mandatory to work with Google Chrome for full Swagger support. Internet Explorer does not fully support the Swagger client.

B.3 Replication Fail

If the replication fails while performing the activation or during normal operation:

- Validate that the X-UM is able to resolve Skype pools, and vice versa that the Skype Servers is able to resolve the X-UM pool on the DNS.
- Validate that all Server Time/Date are synchronized
- Validate that a Firewall does not block the communication between the X-UM and Skype servers and AD.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com/>

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-26791

