AudioCodes One Voice for Microsoft® Skype for Business

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

Version 0.1





# **Table of Contents**

1	Introduction1				
	1.1	Installation Flow	.12		
2 Planning X-UM Architecture		ning 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 Oser – Call from Lync Client	17		
		2.3.4 Message Waiting Indication (SIP Subscription)	18		
		2.3.5 Outlook Voice Access– User Access to Mailbox via Telephone	18		
		<ul> <li>2.3.6 Play-on-Phone</li> <li>2.3.7 Outlook Voice Access Call Out – User Access to Mailbox via Telephone and Ca</li> <li>out 20</li> </ul>	19 II		
	2.4	Debugging tools	.21		
	2.5	Re-image X-UM Standard	.21		
3	Defa	ault 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		
	32	SBC Mediant 800 Information	23		
	0.2	3.2.1 Login	24		
		3.2.2 IP Address Information	24		
4	Cha	nging 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			
	4.4	Re-Join the X-UM to the Domain	. 30		
5	Ass	igning 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		
	53	Changing IP Addresses			
	0.0	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		
		5.3.4.1 Changing Default SIP Domain	<i>31</i> 37		
		5.3.4.2 Changing Simple URL's	38		
		5.3.4.3 Changing Edge Settings	39		
		5.3.6 Changing Static DNS Records	<del>4</del> 1 41		
		5.3.6.1 Modifying the Edge Server Hosts File	42		

		5.3.7	Changing the IP Address of AudioCodes Devices 5.3.7.1 Changing Mediant 800B IP Address	
6	Cha	nging	or Adding a SIP Domain	45
	6.1	Skype	e 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	
	6.2	Chang	ging X-UM Standard SIP Domain	46
		6.2.1	Process Overview	46
		6.2.2	Connecting to X-UM Standard Controller using RDP	
		0.2.3	6.2.3.1 Adding the New SIP Domain to the Topology	
			6.2.3.2 Changing the Default (Primary) SIP Domain	
			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	
		624	6.2.3.6 Publishing Topology	
		0.2.4	6.2.4.1 Installing or Updating Skype for Business Server Syste	em
		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	
		627	Enabling Configuration	61
_	•			00
1	Con	nectin	ig Edge Server to a Full DMZ Deployment	
	7.1	Conne	ecting the Edge Server	63
8	Des	cribing	g Deployment Requirements	67
	8.1	Before	e Deploying CloudBond X-UM	67
		8.1.1	Public Key Infrastructure	67
		8.1.2	IP Addresses	
		8.1.3	DNS Forest and Domain Levels	80
	00	Intogr	ating CloudPond X LIM	
	0.2	9.2.1	Connecting CloudBond X LIM to the Enterprise Domain	70
		822	Verifying the Time and Time Zone Settings for CloudBond X-UM	Servers 70
		8.2.3	Verifying DNS Settings on NIC Adapters	
		8.2.4	Verifying the Enterprise Domain and Forest Levels	71
		8.2.5	Setting up Cross Forest DNS Stub Zones	
		8.2.6	Active Directory Synchronization	81 00
		828	Certificates	
	83	Skype	of Rusiness DNS Records	84
	0.0	831	Skype for Business Internal Records	
		8.3.2	Skype for Business External Records	
		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	Firewa	all Port Requirements	89
		8.4.1	CloudBond 365 Deployment Overview	89
		0.4.0	8.4.1.1 References	
		8.4.2	Perimeter Network Port Requirements	
			8 / 2 1 Edge Server	02
			8.4.2.1 Edge Server	

		8.4.3	Other Port Requirements	97 97
		8.4.4	8.4.3.2 Ports and Protocols Used by the Skype for Business Internal Servers . Windows Update and SysAdmin Update Port Requirements	99 104
			8.4.4.1 Port Requirements for Integration with Exchange 2010 SP1 Unified	
			Messaging	104
9	Offic	e 365	Integration	109
	9.1	Overvi	ew	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
		016	9.1.5.1 Skype for Business Hydrid Deployment	112
		9.1.0	9161 DirSync	112
		9.1.7	Active Directory Federation Services	114
	92	Pre-Re	equisites	115
	0.2	0.2.1		115
		922	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	Config	uring 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 for Skype for Publices Online	122
		932	Obtaining the Customer Specific Office 365 Information	122
		0.0.2	9 3 2 1 Determining Hosted Migration Service Override URI	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 F	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	Ongoir	ng Replication	130
	9.6	Adding	a Dial Plan to Exchange Online	131
	9.7	Skype	for Business PowerShell	136
	9.8	Power	Shell for Skype for Business Online	137
	0.0	0.8.1	Connecting to Office 365 using PowerShell	138
	0.0	Troubl	ochooting	120
	9.9		Convoluting	109
	9.10	Custor	n 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	Con	figurin	g Certificates	147
	10.1	Backg	round	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 4	Privacy	140
		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	Cloud	Bond 365 Default Certificates	150
		10.2.1	CloudBond 365 Included Certificates	150
		10.2.2	CloudBond 365 External Certificates	150
	10.3	Cloud	Bond 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 Withinfitze the variations in Simple ORLS	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
			10.5.1.5 Using External Web Services	102
			10.5.1.5 Publishing Topology and Deploy.	165
	10.6	Obtain	ing and Deploving 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	1//
		10.8.1	Using the Certificate Wizards	177
	10.0	Deeuse	10.8.1.1 Accessing the Certificate Wizard	177
	10.9	Reque		180
		10.9.1	Enterprise CA Accessible	180
		10.9.2	Requesting Certificates (CA Accessible)	181
		101010	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	190 102
			10.9.4.3 Installing the Certificate on the CloudBond 365 Server	193
			J	

	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	
	10.12.3 Setting Up a Certificate Authonity on Windows Server 2012	200
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	
	12.2 Create Users in CloudBond 365	
	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
		227
	12.2 X LIM Connector SID Interface	201
	13.2 X-UM Connector SIP Interface	238
	<ul><li>13.2 X-UM Connector SIP Interface</li></ul>	238
14	<ul> <li>13.2 X-UM Connector SIP Interface</li></ul>	238 238 239
14	<ul> <li>13.1 MVF Notify.</li> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools .</li> <li>14.1 X-UM Log</li> </ul>	238 238 <b>239</b> 239
14	<ul> <li>13.2 X-UM Connector SIP Interface</li></ul>	238 238 239 239 239
14	<ul> <li>13.2 X-UM Connector SIP Interface</li></ul>	238 238 239 239 239 239 239 239
14	<ul> <li>13.1 MWI Notify.</li> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools</li> <li>14.1 X-UM Log.</li> <li>14.2 X-UM Connector Running in Console Mode.</li> <li>14.3 Syslog</li></ul>	238 238 238 239 239 239 239 239 239 239 239 239 239 239 239
14	<ul> <li>13.2 X-UM Connector SIP Interface</li></ul>	238 238 238 239 239 239 239 239 239 239 239 239 239 239 239 239 239 239 
14 15	<ul> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools</li> <li>14.1 X-UM Log.</li> <li>14.2 X-UM Connector Running in Console Mode</li> <li>14.3 Syslog</li> <li>14.4 OCS Logger and Wireshark.</li> <li>Re-Image X-UM Standard</li> <li>15.1 Download Latest Version</li> </ul>	238 238 239 239 239 239 239 239 240 241
14 15	<ul> <li>13.1 MWI Notity.</li> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools</li> <li>14.1 X-UM Log.</li> <li>14.2 X-UM Connector Running in Console Mode.</li> <li>14.3 Syslog.</li> <li>14.4 OCS Logger and Wireshark.</li> <li>Re-Image X-UM Standard</li> <li>15.1 Download Latest Version.</li> <li>15.2 Create the X-UM Connector VM</li> </ul>	238 238 238 239 239 239 239 239 240 241 241 241
14 15	<ul> <li>13.2 X-UM Connector SIP Interface</li></ul>	238 238 238 239 239 239 239 239 239 240 241 241 241 241 246
14 15	<ul> <li>13.2 X-UM Connector SIP Interface</li></ul>	238 238 239 239 239 239 239 239 240 241 241 241 241 246 249
14 15	<ul> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools .</li> <li>14.1 X-UM Log.</li> <li>14.2 X-UM Connector Running in Console Mode .</li> <li>14.3 Syslog .</li> <li>14.4 OCS Logger and Wireshark.</li> <li>Re-Image X-UM Standard .</li> <li>15.1 Download Latest Version .</li> <li>15.2 Create the X-UM Connector VM .</li> <li>15.3 Configuring X-UM Connector VM .</li> <li>15.4 Starting the X-UM Connector Virtual Machine .</li> <li>15.5 Windows 2012R2 Server Role &amp; Features .</li> </ul>	238 238 238 239 239 239 239 239 239 240 241 241 241 241 241 241 245 249 249 250
14	<ul> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools</li></ul>	238 238 238 239 239 239 239 239 240 241 241 241 241 241 246 240 250 250
14	<ul> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools</li> <li>14.1 X-UM Log.</li> <li>14.2 X-UM Connector Running in Console Mode.</li> <li>14.3 Syslog.</li> <li>14.4 OCS Logger and Wireshark.</li> <li>Re-Image X-UM Standard</li> <li>15.1 Download Latest Version.</li> <li>15.2 Create the X-UM Connector VM.</li> <li>15.3 Configuring X-UM Connector VM.</li> <li>15.4 Starting the X-UM Connector VM.</li> <li>15.5 Windows 2012R2 Server Role &amp; Features.</li> <li>15.6 Set IP.</li> <li>15.7 Add X-UM Connector to Domain.</li> </ul>	238 238 238 239 239 239 239 239 239 240 241 241 241 241 241 241 245 250 250 250
14	<ul> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools</li> <li>14.1 X-UM Log.</li> <li>14.2 X-UM Connector Running in Console Mode</li> <li>14.3 Syslog</li> <li>14.4 OCS Logger and Wireshark.</li> <li>Re-Image X-UM Standard</li> <li>15.1 Download Latest Version</li> <li>15.2 Create the X-UM Connector VM.</li> <li>15.3 Configuring X-UM Connector VM.</li> <li>15.4 Starting the X-UM Connector Virtual Machine</li> <li>15.5 Windows 2012R2 Server Role &amp; Features</li> <li>15.6 Set IP.</li> <li>15.7 Add X-UM Connector to Domain.</li> <li>15.8 Install UCMA 5</li> </ul>	238 238 238 239 239 239 239 239 240 241 241 241 241 241 246 249 250 250 250 253
14	<ul> <li>13.2 X-UM Connector SIP Interface.</li> <li>13.3 SBC Configuration Important points.</li> <li>Using X-UM Connector Debugging tools</li> <li>14.1 X-UM Log.</li> <li>14.2 X-UM Connector Running in Console Mode</li> <li>14.3 Syslog</li> <li>14.4 OCS Logger and Wireshark.</li> <li>Re-Image X-UM Standard</li> <li>15.1 Download Latest Version</li> <li>15.2 Create the X-UM Connector VM</li> <li>15.3 Configuring X-UM Connector VM.</li> <li>15.4 Starting the X-UM Connector VI.</li> <li>15.5 Windows 2012R2 Server Role &amp; Features</li> <li>15.6 Set IP</li> <li>15.7 Add X-UM Connector to Domain.</li> <li>15.8 Install UCMA 5</li> <li>15.9 Installing Skype for Business Component.</li> </ul>	238 238 239 239 239 239 240 240 241 241 241 241 241 241 241 241 241 241

	15.1	1 Activat	ting X-UM Connector	
	15.1	2Adding	DNS A Record	
A	HA a	and DR	2	
	A.1	HA/DR	R On Skype Level	
	A.2	HA On	X-UM Level	
		A.2.1	Conditions for HA	
		A.2.2	Incoming Messages Redirection	
			A.2.2.1 Proxy Configuration	
		A.2.3	Web GUI Swagger	
В	Kno	wn Iss	ues	
	B.1	User F	ile Name does not Support "\$" Char	
	B.2	Using	the REST Swagger Client with Internet Explorer	
	B.3	Replica	ation Fail	

## 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 <a href="https://www.audiocodes.com/library/technical-documents">https://www.audiocodes.com/library/technical-documents</a>.

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 <a href="https://www.audiocodes.com/services-support/maintenance-and-support">https://www.audiocodes.com/services-support/maintenance-and-support</a>.

#### 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 <a href="https://online.audiocodes.com/documentation-feedback">https://online.audiocodes.com/documentation-feedback</a>.

## **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/downloadsaudiocodes/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-forsession-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

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

PSTN

PEX

PEX

B

C

FE Pool

</tab

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

- 1. FE forwards incoming call to user to X-UM
- 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.

# **C**audiocodes

- **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)





- 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.
- 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.
- 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: "<u>Outlook</u> <u>Voice Access– User access to mailbox via telephone"</u>

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 <u>self REFER + REPLACES</u> 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
  - <u>https://meet.cloudbond365.local/meet</u>
- 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 its 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:

N 10			
File Action Vi	ew Help		
🗢 🄿 🔁 🗔	? 🗊		
Hyper-V Mana	ger Virtual	Machines	
	New	•	State
	Import Virtual Machine		Running
	Hyper-V Settings		Running
	Virtual Switch Manager	У	Running
	Virtual SAN Manager		
	Edit Disk		
	Inspect Disk		

Figure 4-1: Hyper-V Manager

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

2	Minimport Virtual Machine				
Before You Begin					
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Summary	This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.				
	<pre></pre>				

Figure 4-2: Before You Begin

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

	righte 4-0. Opeeny rolaer	
<b>A</b>	Import Virtual Machine	x
Locate Folder	r	
Before You Begin	Specify the folder containing the virtual machine to import.	
Locate Folder	Folder: D:\Hyper-V\xUMexport\xUM\ Browse.	
Choose Import Type		
Summary		
	< <u>P</u> revious <u>N</u> ext > Einish Cance	I

#### 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

2	Import Virtual Machine	X
Select Virtua	Machine	
Before You Begin	Select the virtual machine to import:	
Locate Folder	Name	Date Created
Select virtual Machine Choose Import Type Summary	XUM	11/13/2017 2:03:29 PM
	< <u>P</u> revious <u>N</u> ext	t > Enish Cancel

7. Select the 'xUM' virtual machine.

8. Click Next; the following screen appears:

	Figure 4-5. Import Type
2	Import Virtual Machine
Choose Impo	ort Type
Before You Begin	Choose the type of import to perform:
Locate Folder	Register the virtual machine in-place (use the existing unique ID)
Select Virtual Machine	Restore the virtual machine (use the existing unique ID)
Choose Import Type	O Copy the virtual machine (create a new unique ID)
Summary	
	< Previous Next > Finish Cancel

Figure 4-5: Import Type

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

		-
	Import Virtual Machine	X
Choose Fol	ders for Virtual Machine Files	
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	You can specify new or existing folders to store the virtual machine files. Otherwise, th imports the files to default Hyper-V folders on this computer, or to folders specified in t machine configuration.	e wizard he virtual
	<₽revious Next > Einish	Cancel

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

1 🛃	Import Virtual Machine	x
Choose Fold	ers to Store Virtual Hard Disks	
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	Where do you want to store the imported virtual hard disks for this virtual machine? Location: D:\Hyper-V\Virtual Hard Disks\	Browse
	< Previous Next > Enish	Cancel

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

2	Import Virtual I	Machine
Completing I	import Wizard	
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	You are about to perform the following Description: Virtual Machine: Import file: Import Type: Virtual machine configuration folder: Checkpoint folder: Smart Paging file store: Virtual hard disk destination folder:	voperation. xUM D:\Hyper-V\xUMexport\xUM\Virtual Machines\AFF02103-F88F Restore (keep ID) D:\Hyper-V\xUM D:\Hyper-V\xUM D:\Hyper-V\XUM D:\Hyper-V\XUM D:\Hyper-V\Virtual Hard Disks\
	<	III >
	[	< Previous Next > Finish Cancel

#### 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.

Le	Collapse	
	Pin to Start	
8	Manage	
r	Open in new window	
F	Map network drive	
<b>4</b>	Disconnect network drive	
4	Add a network location	
L	Delete	
le	Rename	
Ne	Properties	

#### Figure 4-1:My Computer - Properties

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

🕕 Hanze Kecola 🛛 👩 Stöb Kecola 🖃 Haa ? ↑ 🖳 → Control Panel → System and Security → System Control Panel Home View basic information about your computer 🚱 Device Manager Windows edition 😵 Remote settings Windows Server 2012 R2 Standard Windows Server 2012 R2 Advanced system settings © 2013 Microsoft Corporation. All rights reserved. System Intel(R) Core(TM) i7-5850EQ CPU @ 2.70GHz 2.69 GHz Processor: Installed memory (RAM): 6.00 GB 64-bit Operating System, x64-based processor System type: Pen and Touch: No Pen or Touch Input is available for this Display Computer name, domain, and workgroup settings Change settings Computer name: EXUM Full computer name: EXUM.cloudbond365.local Computer description: EXUM cloudbond365.local Domain: Windows activation Windows is not activated. Read the Microsoft Software License Terms See also Product ID: 00252-40260-33000-AAOEM Activate Windows Action Center Windows Update

Figure 4-2:Change Settings Link

5. On the System Properties screen, click Change.



on the netw	recompared to recompare and the recompare and the recompared to recompare and the recompare and the recompared to recompare and the recompare
	For example: "IIS Production Server" or "Accounting Server".
Full computer name:	EXUM.cloudbond365.local
Domain:	cloudbond365.local
	ά του το

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

System Propertie	S	2
Computer Name/Domain Cha	nges 💌	
ou can change the name and the membership of omputer. Changes might affect access to networ	this k resources.	mputer
omputer name:	-	
XUM		
(UM cloudbond 365 local		
Vember of	More h	ge
Vember of Domain:	More	ge
Vember of Domain: cloudbond365.local	More	ge
Member of Domain: cloudbond365.local	More	ge
Member of Domain: cloudbond365.local I Workgroup: OK	More	ġe

#### 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

	Surtem Drementies	This P		
	System Properties		~ 😮 🛄	
Computer Name Hardwar	re Advanced Remote	System	_ <b>D</b> X	
Windows uses on the network	the following information to identify your computer	System and Security    System	✓ ♂ Search Control Panel ♀	]
Computer description:	For example: "IIS Production Server" or "Accounting Server".	ew basic information about your cor	mputer	2
Full computer name:	WIN-0J9GA7GL9SB	Computer Name/Domain Chan	nges 🗶	
Workgroup:	WORKGROUP	You can change the name and the membership of computer. Changes might affect access to perwork	Windows Security	
workgroup, click Change.	Change	Computer name: XUMV2 Full computer name: XUMV2	Computer Name/Domain Changes Enter the name and password of an account with permission to join the domain.	he
		Member of	Password	
		Domain:     algorithm of 265 loggl	Domain: cloudbond365.local	
	UK Cancel Apply	O Workgroup:           WORKGROUP	Connect a smart card	
	9 item See also	ОК	OK	cel

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.

neral	-		panel 🚱
	Ethernet Properties	t access	e general propertie
Connection IPv4 Cor IPv6 Cor Media St	Networking           Connect using: <u> <u> </u></u>	Internet Protocol Version 4 (TC General	P/IPv4) Properties
Duration Speed: Detail	This connection uses the following items:	Obtain an IP address automatically     Obtain an IP address	ur network administrator
ctivity —	GoS Packet Scheduler     Microsoft Network Adapter Multiplexor     Link-Layer Topology Discovery Mappe     Link-Layer Topology Discovery Respo     Linker Protocol Version 6 (TCP/IPv6)	IP address: 192 Subnet mask: 255 Default gateway:	. 168 . 0 . 100 . 255 . 255 . 0 
Bytes:	Install     Uninstall     Description     Transmission Control Protocol/Internet Protoc     wide area network protocol that provides con     across diverse interconnected networks.	Obtain DNS server address automatically Use the following DNS server addresses: Preferred DNS server: 127 Alternate DNS server:	. 0 . 0 . 1
	ОК	Validate settings upon exit	Advanced

#### 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

04 <b>.</b>	Administrator: Command Prompt		x
C:\Users\Admin Pinging acs-uu f data: Reply from 19: Reply from 19: Reply from 19: Reply from 19:	nistrator>ping acs-uc-fe.acs-unified-communications.net c-fe.acs-unified-communications.net [192.168.0.101] with 2.168.0.101: bytes=32 time<1ms TTL=128 2.168.0.101: bytes=32 time<1ms TTL=128 2.168.0.101: bytes=32 time<1ms TTL=128 2.168.0.101: bytes=32 time<1ms TTL=128	32 bytes	• =
Ping statistic Packets: S Approximate re Minimum = C:\Users\Admin	cs for 192.168.0.101: Sent = 4, Received = 4, Lost = 0 (0% loss), ound trip times in milli-seconds: Øms, Maximum = Øms, Average = Øms nistrator)ning acs-uc-edge.acs-unified-communications.net		
Pinging acs-u of data: Reply from 19: Reply from 19: Reply from 19: Reply from 19: Reply from 19:	c-edge.acs-unified-communications.net [192.168.0.103] wit 2.168.0.103: bytes=32 time<1ms TTL=128 2.168.0.103: bytes=32 time<1ms TTL=128 2.168.0.103: bytes=32 time<1ms TTL=128 2.168.0.103: bytes=32 time<1ms TTL=128	h 32 byte	S
Ping statisti Packets: 9 Approximate r Minimum = C:\Users\Admin	cs for 192.168.0.103: Sent = 4, Received = 4, Lost = 0 (0% loss), ound trip times in milli-seconds: Øms, Maximum = Øms, Average = Øms nistrator}_		
			$\sim$



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

<b>Å</b>		DNS Manager		_ <b>_</b> ×	
File Action View Help					
🗢 🔿 🙍 📰 🗶 🗐 🙆					
<ul> <li>DNS</li> <li>DC</li> <li>Forward Lookup Zones</li> <li>Global Logs</li> <li>Forward Lookup Zones</li> <li>G. msdcs:CB106.com</li> <li>Reverse Lookup Zones</li> <li>Trust Points</li> <li>Conditional Forwarders</li> </ul>	Name Insdcs Its Ltp DomainDnzZones ForetDnzZones (same as parent folder) (same as parent folder)	Type Start of Authority (SOA) Name Server (NS) Name Server (NS)	Data [130], dc.cb106.com, host dc105.cb106.com. dc.cb106.com.	Timestamp static static static static	
	(same as parent folder) (same as parent folder) (stame as parent folder) (sta	Host (A) Host (A) [Pv6 Host (AAAA) [Pv6 Host (AAAA) Host (A) [Pv6 Host (AAAA) Host (A) Host (A) [Pv6 Host (AAAA) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A)	10.21:57.45 10.21:57.45 fd9f:2e78:f603:61c2:7a4cre fd9f:2e78:f603:61c2:0b9c:6 10.21:57.55 10.21:57.55 10.21:57.45 fd9f:2e78:f603:61c2:0b9c:6 10.21:57.55 fd9f:2e78:f603:61c2:7a4cre 10.21:57.51 10.21:57.45 10.21:57.45	1/27/2017 2:00:00 PM 1/27/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 10:00:00 PM 1/31/2017 12:00:00 PM 1/31/2017 12:00:00 PM 1/31/2017 7:00:00 PM	

#### Figure 5-3: Check DNS Updates



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.

Å	DNS Man	ager	-	. 🗆 X
<u>File Action View H</u> elp				
<ul> <li>DNS</li> <li>UC-DC</li> <li>Forward Lookup Zones</li> <li>Gmsdcs.cloudbond36</li> <li>G. ACB.Local</li> <li>G. cloudbond365.com</li> <li>Cloudbond365.com</li> <li>Trust Points</li> <li>Conditional Forwarders</li> <li>M. Global Logs</li> </ul>	Name	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A)	Data [1142], uc-dc.cloudbond365.com, h uc-dc.cloudbond365.com. 172.17.240.100 172.17.240.101 172.17.240.101 172.17.240.101 172.17.240.101 172.17.240.101 172.17.240.101 172.17.240.84 172.17.240.101 172.17.240.101 172.17.240.101	Timestamp static static 10/20/2017 static static static static static static static 10/19/2017 static static static
< III >		III		>

Figure 5-3: Changing	X-UM Pool E	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.

6	Edit Properties	x
SIP domain	SIP domain	
Simple URLs	Default SIP domain: *	
Central Management Server	S4B.interop	
	Additional supported SIP domains:	_
	Add	=
	Update	
	Remove	
	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://. Hyou 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	~
Help	OK	:el

#### 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:	<b>Changing Simp</b>	ole URL's
-------------	----------------------	-----------

	Edit Properties	_	D X
SIP domain Simple URLs Central Management	Simple URLs Simple URLs will be sent to your users and used by them to ac conferencing phone numbers meetings and administration T	cess the web pages for dial-in	▲ ^
Server	meetings are scheduled. Other URLs are used to support any r the past by using those URLs. Meeting and Phone access simp URLs, including https://. If you change a Meeting or Phone acc prevent users from joining existing meetings or conferences. T active URL and leave the current URL inactive. An inactive URL	neetings that have been scheduled in le URLs are required and must be full ess URL after it has been published, y o change the active URL, create a nev can be removed after all conferences	ou v or
	meetings that use it have expired or been deleted. Phone access URLs:		
	Simple URL		
	https://meet.CB106.com/dialin	Add Remove	
	Mak	e Active Edit URL	
	Meeting URLs:		
	Simple URL	SIP domain	
	https://meet.CB106.com/meet CB106.	com Add Remove	
	Mak	e Active Edit URL	
	Administrative access URL:		~
Help		OK	Cancel

## 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



10	Edit Properties			_ □	x
General	External settings			•	^
Next hop Edge Server configuration	Specify the external, fully qualified domain names (FQDNs) an Conferencing Edge, and A/V Edge services. The combinations Enable separate FQDN and IP address for web conferencin Enable IPv4 on external interface Enable IPv6 on external interface	nd ports for Access of FQDN and port ng and A/V	: Edge, Wel t must be u	b unique,	_
	A/V Edge service is NAT enabled				
	FQDN: *	P	orts		
	sip.contoso.com	:	5061	(TLS)	
	IPv4 address: *				_
	192.168.254.103				=
	IPv6 address:				
	Web Conferencing Edge service FODN:				
	sip.contoso.com	: 4	444	(TLS)	
	IPv4 address:				
	192.168.254.103				~
Help			OK	Can	icel

#### Figure 5-7: Changing Edge Server

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

Publish the topology		
In order for Skype for Business Server 2015 to co publish your topology. Before you publish the to completed:	prrectly route messages in your deployment, you must pology, ensure that the following tasks have been	
<ul> <li>A validation check on the root node did not</li> <li>A file share has been created for all file store</li> <li>All simple URLs have been defined.</li> <li>For Enterprise Edition Front End pools and P Archiving Servers: All SQL Server stores are i exceptions for remote access to SQL Server.</li> <li>For a single Standard Edition server, the "Pre completed.</li> <li>You are currently logged on as a SQL Server sysadmin role).</li> <li>If you are removing a Front End pool, all use contact objects, and conference directories.</li> </ul>	return any errors. es that you have configured in this topology. Persistent Chat pools and for Monitoring Servers and installed and accessible remotely, and firewall are configured. epare first Standard Edition server" task was r administrator (for example, as a member of the SQL ers, common area phones, analog devices, application have been removed from the pool	
If you are removing a Front End pool, all use contact objects and conference directories. When you are ready to proceed, click Next.	ers, common area phones, analog devices, application have been removed from the pool Back <u>N</u> ext Cancel	

# 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).

å		DNS Manager			x
File Action View Help					
🗢 🄿 🖄 📰 🗶 🖪 🔒	? 🖬 🔋 🖬				
<ul> <li>NS</li> <li>DNS</li> <li>DC</li> <li>Convert Lookup Zones</li> <li>CB106.com</li> <li>CB106.com</li> <li>Reverse Lookup Zones</li> <li>Trust Points</li> <li>Conditional Forwarders</li> </ul>	Image: Second State Sta	Type       Start of Authority (SOA)       Name Server (NS)       Name Server (NS)       Host (A)       IPv6 Host (AAAA)       IPv6 Host (AAAA)       Host (A)       Host (A)	Data [130], dc.cb106.com, host dc105.cb106.com. dc.cb106.com. 10.21.57.45 10.21.57.55 fd9f:2e78:f603:612:744cte fd9f:2e78:f603:612:20b9c:6 10.21.57.56 fd9f:2e78:f603:612:24537:e 10.21.57.55 fd9f:2e78:f603:612:20b9c:6 10.21.57.51 10.21.57.45 fd9f:2e78:f603:61c2:7a4cte 10.21.57.45 fd9f:2e78:f603:61c2:7a4cte 10.21.57.45	Timestamp static static static static 1/27/2017 2:00:00 PM 1/27/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 8:00:00 PM 1/31/2017 11:00:00 AM static static static static static 1/31/2017 12:00:00 PM 1/31/2017 12:00:00 P	Ē
	meet	Host (A)	10.21.57.46	static	
	🗐 sip	Host (A)	10.21.57.46	static	
	WIN-8MSOS3D3JHF	Host (A)	10.21.57.30	2/1/2017 9:00:00 AM	~

#### 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.

💽 🕕 =		etc			•
File Home Sha	re View				~
€ 🕘 ▾ ↑ 퉱 «	Local Disk (C:)  Windows  Syster	n32 🕨 drivers 🕨 etc	<b>∀ Ċ</b> Se	earch etc	ş
☆ Favorites	Name	Date modified	Туре	Size	
E Desktop	hosts	1/28/2014 3:39 AM	File	1 KB	
🗼 Downloads	Imhosts.sam	8/22/2013 8:38 AM	SAM File	4 KB	
Recent places	networks	8/22/2013 6:25 AM	File	1 KB	
	protocol	8/22/2013 6:25 AM	File	2 KB	
🖳 This PC	services	8/22/2013 6:25 AM	File	18 KB	
📔 Desktop					
Documents					

#### 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.

AudioCodes Media	ent 800			Submit 🧕	Burn	Device Actions	🙆 Hor	1e 🔞 Help	Elog off
Configuration Maintenance Status 8 Diagnostics	IP In	terfaces Table							
Scenarios Search		Add Index				Done			
* System	Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address
Physical Parts Table	0 0	OAMP + Media + Control	IPv4 Manual	192.168.0.2	24	192.168.0.1	1	Voice	192.168.0.1
Ethernet Groups Table					▼ IP Interface S	Status Table			
Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Construction Co									

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 signon 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 rerun 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

Topology Builder	x						
Welcome to Topology Builder. Select the source of the Lync Server topology document.							
Download Topology from existing deployment Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.							
<ul> <li>Open Topology from a local file</li> <li>Open an existing Topology Builder file. Use this option if you have work in progress.</li> </ul>							
<ul> <li>New Topology Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.</li> </ul>							
Help OK Cance	el 🛛						

6. Save the topology.

10	Save Topology As		×
🕘 🕘 🔻 🕇 🚺 Madi	ministrator.ac-onebox\Documents	Search Document	ts P
Organize 🔻 New fold	er		i 🕶 🕜
🔆 Favorites	Name	Date modif	ied Type
Desktop Downloads Recent places	No items matc	h your search.	
I툎 This PC			
🗣 Network			
			/ >
File name: oneb	iox 20140610		×
Save as type: Topo	logy Builder files (*.tbxml)		~
Hide Folders		Save	Cancel

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).

Figur	e e-o: viewing	jai	opology	
	Lync Server 2013, Topol	ogy Bu	ilder	_ <b>D</b> X
File     Action     Help       Image: Action of the second seco	SIP domain Default SIP domain:	ac-one	box.com	<b>.</b>
<ul> <li>Shared Components</li> <li>Branch sites</li> </ul>	Additional supported SIP domains:	Not co	nfigured	
	Simple UKLs			<b>_</b>
	Phone access URLs:	Active	Simple URL https://meet.ac-onebox.com/dialin	
	Meeting URLs:	Active	Simple URL https://meet.ac-onebox.com/meet	SIP domain ac-onebox.com
	Administrative access URL:	Not cor	nfigured	
	Central Management Serve	r		•
	Central Management Server:	Active	Front End UC-FE.ac-onebox.com	Site ACS-2013

Figure 6-5: Viewing a Topology

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

10	Lync Server 2013, Topo	logy B
File Action He	elp	
▲ Lync     ▲	New Central Site Edit Properties	
	New Topology	ac-on
▷ 🖬	Open Topology Download Topology	Not o
	Save a copy of Topology As Publish Topology Install Database	
	Merge Office Communications Server 2007 R2 Topology Remove Deployment	Active
	Help	Active
		$\checkmark$

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.

6	Edit Properties	x
SIP domain	SIP domain	^
Simple URLs Central Management	Default SIP domain: *	
Server	CB106.com	
	Additional supported SIP domains:	=
	Add	-
	Update	
	Remove	
	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	~
Help	OK Canc	el

### 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**.

15	Edit Properties		x
SIP domain Simple URLs Central Management Server	Simple URLs Simple URLs will be sent to your users and used by t conferencing phone numbers, meetings, and admini meetings are scheduled. Other URLs are used to sup the past by using those URLs. Meeting and Phone ac URLs, including https://.lf you change a Meeting or prevent users from joining existing meetings or cond active URL and leave the current URL inactive. An ina meetings that use it have expired or been deleted.	hem to access the web pages for dial-in stration. The active URL is used when new port any meetings that have been scheduled in iccess simple URLs are required and must be full Phone access URL after it has been published, you reences. To change the active URL, create a new active URL can be removed after all conferences or	^
	Phone access URLs: Simple URL https://meet.CB106.com/dialin	Add Remove Make Active Edit URL	=
	Simple URL	SIP domain CB106.com Add Remove	
Help	Administrative access URL:	Make Active Edit URL	v

### 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.aconebox.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**.

5 5	Skype for Business	Server 2015, Topology Builder	- 🗆 X
File Action Help			
Skype for Business Server     A @ ACS-2015	General		. ^
Gorge et a douge et al do	General FQDN: IPv4 addresses: Features and functionality Instant messaging (IM) and presence: Conferencing: PSTN conferencing: Enterprise Voice: Archiving SQL Server store: Archiving SQL Server store: File store: Office Web Apps Server: Edge pool (for media):	FEC8106.com Use all configured IPv4 addresses Enabled Enabled Enabled Enabled Enabled FEC8106.com/bcfault DC.C8106.com/bcfault DC.C8106.com/bcfault VLFEC8106.com/bcfault VLFEC8106.com/bcfault VLFEC8106.com/bcfault	
	Note: To view the federate	on route, use the site property page.	
	Resiliency		
	<	111	>

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

Figure 6-11: Edit Properties

10	Edit Properties	×
General Resiliency Web services Mediation Server	Web services         Listening port defines the IIS configuration on servers in the pool and Published port reflects the configuration of a load balancer, a reverse proxy, or a firewall.         After you make changes to the fully qualified domain name (FQDN) or listening ports, you must run local Setup on all servers in the pool in order for these changes to take effect.         Internal web services         Listening ports: * HTTP:       80         HTTPS:       443         Published ports: * HTTP:       80         HTTPS:       443	^
	External web services FQDN: * ewslync.contosolcom Listening ports: * HTTP: 8080 HTTPS: 4443 Published ports: * HTTP: 80 HTTPS: 443	
Help	Mediation Server <ul> <li></li></ul>	H

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:

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



15	Skype for Business	Server 2015, Topology Builder	>	×
File Action Help				
<ul> <li>Skype for Business Server</li> <li>ACS-2015</li> </ul>	General		•	^
Lync Server 2010     Lync Server 2013     Lync Server 2013     Standard Edition Front End Servers     Terterprise Edition Front End pools     Director pools     Mediation pools     Edge.02106.com     Edge.02106.com	Internal server FQDN: Internal IPv4 address: Federation (port 5061): Skype-Skype federation search (port 443): XMPP federation (port S269): Internal Configuration Replication Port (HTTPS)	Edge.C8106.com 10.21.57.47 Enabled Enabled Enabled 4443		Ш
Video Interop Server pools	Next hop selection			
anarce components     and states     and states	Next hop pool:	FEC8106.com (ACS-2015)		
	External settings		•	
	Access Edge service FQDN: IPv4 address: Port: Protocol:	sip.CB106.com 192.168.254.103 5061 TLS		
	Web Conferencing Edge ser	vice		~

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

Figure 6-13: Edge Server External Access FQDNs

l d	Edit Properties	_ <b>_</b> ×
General Next hop Edge Server configuration	External settings         Specify the external, fully qualified domain names (FQDNs) and ports for Access Edge, I Conferencing Edge, and A/V Edge services. The combinations of FQDN and port must be         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	Neb be unique.
	Access Edge service Ports	
	FQDN: *	
	sip.contoso.com : 5061	(TLS)
	IPv4 address: *	_
	192.168.254.103	=
	IPv6 address:	
	Web Conferencing Edge service FQDN:	
	sip.contoso.com : 444	(TLS)
	IPv4 address:	
	192.168.254.103	~
Help		DK Cancel

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.

10		-	Lync Server 2013, To	opology Builde	r		x
File	Action Help						
4 2	Edit Properties		<b>C</b> 1				Ľ
⊿	Topology +	New				•	1
	Delete	Open			nebox.com		
	Help	Downloa	d Current Topology		_		
	UC-FE.ac-onebox	Save A C	opy				
	Enterprise Edition Fr	Publish					
	Director pools	Install Da	itabase				
	Mediation pools	Merge O	ffice Communications Server	2007 R2			Ξ
	Persistent Chat pool	Remove	Deployment				
	Edge pools	ox com					
	Trusted application set	ervers	Next hop selection			•	
	Shared Components						
	🚞 Branch sites		Next hop pool:	UC-FE.ac-or	nebox.com (ACS-2013)		
			External settings				
			Access Edge service				
			FQDN:	sip.contoso.	com		
			IPv4 address:	192.168.254	.103		
			Port:	5061			
			Protocol:	TLS			
							•

Figure 6-14: Publishing the Topology

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

## Figure 1-15: Publishing the Topology

۰¢	Publish Topology	x
Ρ	ublish the topology	
ln to	order for Lync Server 2013 to correctly route messages in your deployment, you must publish your pology. Before you publish the topology, ensure that the following tasks have been completed:	
	<ul> <li>A validation check on the root node did not return any errors.</li> </ul>	^
W	<ul> <li>A file share has been created for all file stores that you have configured in this topology.</li> <li>All simple URLs have been defined.</li> <li>For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured.</li> <li>For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.</li> <li>You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).</li> <li>If you are removing a Front End pool, all users, common area phones, analog devices, application contact chiects, and conference directories have been removed from the pool the pool.</li> </ul>	<ul> <li>III</li> </ul>
	Help Back Next Cancel	

3. Click Next.

## Figure 6-16: Select Central Management Server

16	Publish Topology	x
Sele	ct Central Management Server	
Only o Centra	one Front End pool in the deployment can have a Central Management store. All pools use the same al Management store.	e
Select	t the Front End pool that will host the Central Management store:	
ACS	-UC-FE.ACS-Unified-Communications.net ACS-2013	•
	Advanced	]
	Pack Neut Cancel	1
He	Back Next Cancel	1

4. Click Next.

## Figure 6-17: Publishing the topology – Create Databases

		Publish	Topology	X
Creat	te databases			
The fol not be databa with ap Create	llowing dedicated databases en created. If you have the a ises when you publish your i opropriate permissions can o the following databases du	are part of your oppropriate perm copology. If you create the databa ring the publish	topology. Some of the databases lister issions on the SQL Server, you can crea do not have the appropriate permission uses later. process:	d below have ste the is, someone
	Store	Site	Database paths	
>	ACS-UC-DC.ACS-Unifie	ACS-2013	Automatically determine database	file locat
Note: (	Only databases on dedicated	l SQL Servers ca mponents must	n be installed from here. Databases on be installed by running local setup on t	Advanced SQL servers that he machine.
)ataba ierver	ases for Lync Server 2010 co 2010 Management Shell.	mponents must	be installed by running Install-CsDatabi	ase in the Lync
Hel	p		Back Next	Cancel



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

5. Click Finish.

Figure 6-16. Fublishing the Topology Completes						
Publish Topology	x					
Publishing wizard complete						
Your topology was successfully published.						
Step	Status ^					
<ul> <li>Publishing topology</li> </ul>	Success View Logs					
<ul> <li>Downloading topology</li> </ul>	Success =					
<ul> <li>Updating global simple URL settings</li> </ul>	Success					
<ul> <li>Publishing global simple URL settings</li> </ul>	Success					
<ul> <li>Downloading global simple URL settings</li> </ul>	Success 🗸					
Year bowindedung global simple out settings       Success       ✓         Next steps:       ◆ Click here to open to-do list       In order for Lync Server 2013 to correctly route traffic, your deployment must match the published topology. The linked text file contains a list of any servers that need to be updated, as well as any databases that need to be created.         To close the wizard, click Finish.         Help       Back       Finish       Cancel						

## 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 6-20: 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

1	Skype for Business Server 2015 - Deployment Wizard	x
Install c	or update member system	
<u>Deploy</u> > I	install or update	2
Step 1:	Install Local Configuration Store Installs local configuration store and populates with data from Central Management Store. Prerequisites > Help > Complete Run Again	^
Step 2:	Setup or Remove Skype for Business Server Components         Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition.         Prerequisites ▶         Help ▶	=
Step 3:	Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition. Prerequisites	
	Help > Complete Run Again	
Step 4: Manual	Start Services After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. You can start the services in a pool with the Skype for Business Server cmdlets. To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. To start the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool. Prerequisites	~
	Back Activat	Exit

### 2. Click Run Again.

#### Figure 6-22: Setup Server Components

a	Set Up Skype for Business Server Components	x
S	Set Up Skype for Business Server Components	
Install an topology	d activate, or deactivate and uninstall Skype for Business Server components based on the definition. This step may take several minutes.	
Help	Back Next Cancel	

#### Figure 6-23: Executing Components

	Set Up L	ync Server Co	omponents		x
Exec	uting Commands				
Checking prere Checking prere Installing any ci Executing Powe Report "C:\Use [13_25_20].htm Enabling new n This step will co Executing Powe \Administrator.	quisite MSSpeech_SR_zh-H quisite MSSpeech_SR_zh-H quisite MSSpeech_SR_zh-T\ quisite UcmaWorkflowRun vollocated databases rShell command: Install-CS s\Administrator.ACSLync\A ples onfigure services, apply perr rShell command: Enable-CS ACSLync\AppData\Local\Te	K_TELEprerequ V_TELEprerequ imeprerequisit Database -Conf ppData\Local\To missions, create SComputer -Cor mp\1\Enable-CS	isite satisfied. iisite satisfied. e satisfied. irm:\$false -Verbose emp\1\Install-CSDa firewall rules, etc. firm:\$false -Verbos SComputer-[2013_(	e -LocalDatabas stabase-[2013_ se -Report "C:\ 07_04][13_25_4	ses - 07_04] Users 7].html"
Task status: Com	pleted.				
Bootstrap local r	nachine			•	View Log
Help			Back	Finish	Cancel

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: \_sipfederationt/s.\_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: ewslync.<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.





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 7-3: Edge Server - Two Legs

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

- 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.

a a a a a a a a a a a a a a a a a a a	Hy 🗈 Settings for Edge on UC-DC 🗕 🗖 🗙
File Action View Help	Edge V 4 b Q
	Ardware     Network Adapter
UC-DC Virtual Machines	Madd Hardware         Specify the configuration of the network adapter or remove the network adapter.           EIOS         Specify the configuration of the network adapter or remove the network adapter.
Name     State     CPU Usage     Assigned M       Edge     Running     0 %     2048 MB       FE     Running     1 %     5858 MB         Checkpoints   The selected vir         Edge         Created:     1/1/1601 1:00:00 AM       Version:     5.0       Generation:     1       Notes:     None	Image: Boot from CD       Boot from CD         Boot from CD       Winday Memory         2018 MB       Processor         4 Virtual processors       Virtual processors         1 Virtual processors       Virtual processors         2 Virtual virtual and the second communications through this network adapter       Virtual virtual memory         2 Virtual virtual processors       Virtual virtual virtual machine will use for all network adapter         2 Virtual virtual virtual machine vi
Summary Memory Networking Replication	OK Cancel Apply

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:

- Vou 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.

	internal.contoso.com Properties	x		
General	Trusts Managed By			
internal.contoso.com				
Domain I	name (pre-Windows 2000):			
Contoso		]		
Descripti	on:			
I		]		
Domain f	functional level:			
Windows Server 2012				
-				
Forest functional level:				
Windows Server 2012				
	OK Cancel Apply Help			

### 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.
- 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.
- 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

Å DNS Manager							
File Action View Help							
DNS DUC-DC DEFINITION	Vame Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same Same	Type Active Directory-Integrated Pr Active Directory-Integrated Pr Standard Primary	Status Running Running Running	DNSSEC Status Not Signed Not Signed Not Signed			
2. Click **Next** to start the wizard and select **Stub zone**. Store the zone in Active Directory by enabling the checkmark.

Figure 8-5: Crea	ting DNS	Stub Zone
------------------	----------	-----------

New Zone Wizard X
Zone Type The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
<ul> <li>Secondary zone         Creates a copy of a zone that exists on another server. This option helps balance         the processing load of primary servers and provides fault tolerance.</li> <li>Stub zone         Creates a copy of a zone containing only Name Server (NS), Start of Authority         (SOA), and possibly glue Host (A) records. A server containing a stub zone is not         authoritative for that zone.</li> <li>Store the zone in Active Directory (available only if DNS server is a writeable domain         controller)</li> </ul>
< Back Next > Cancel

3. Set replication to all servers within the domain.



New Zone Wizard		
Active Directory Zone Replication Scope You can select how you want DNS data replicated throughout your network.		
Select how you want zone data replicated:		
$\bigcirc$ To <u>all</u> DNS servers running on domain controllers in this forest: ac-onebox.net		
To all DNS servers running on domain controllers in this domain: ac-onebox.net		
<ul> <li>To all domain controllers in this domain (for Windows 2000 compatibility): ac-onebox.net</li> </ul>		
O To all domain controllers specified in the scope of this directory partition:		
	~	
< <u>B</u> ack <u>N</u> ext > Ca	ancel	

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

New Zone Wizard	x
Zone Name What is the name of the new zone?	and the second s
The zone name specifies the portion of the DNS namespace for which this serv authoritative. It might be your organization's domain name (for example, micr or a portion of the domain name (for example, newzone.microsoft.com). The not the name of the DNS server.	ver is rosoft.com) zone name is
Zone name:	
internal.contoso.com	
< Back Next >	Cancel

## Figure 8-7: DNS Stub Zone – FQDN

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

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

	New Zor	ne Wizard	×	
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	Delete	
<click a<="" add="" here="" th="" to=""><td>n IP Address or DNS</td><td>Name&gt;</td><td></td></click>	n IP Address or DNS	Name>		
192.168.0.10	Contoso-DC	OK	Up	
			Down	
Use the above servers to create a local list of master servers				
		< Back Next	t > 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

å	DNS M	lanager	_	D X	
File         Action         View         Help                ←					
<ul> <li>DNS</li> <li>UC-DC</li> <li>Global Logs</li> <li>Forward Lookup Zones</li> <li>msdcs.ac-onebox.com</li> <li>ac-onebox.com</li> <li>internal.contoso.com</li> </ul>	Name (same as parent folder) (same as parent folder) (contoso-dc) contoso-dc	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A)	Data [60], contoso-dc.internal.c contoso-dc.internal.conto 192.168.0.10 10.253.2.161	Timestam static static static static	

- 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
----------------------------	------------------------------

ir	nternal.contoso.co	m Prope	erties	?	x
General	Start of Authority (S	OA)	Name	Server	s
WINS	Zone Transf	ers	Se	curity	
A zone transfer se	ends a copy of the zone t	o the serve	rs that requ	iest a c	opy.
✓ Allow zone train	nsfers:				
O To any ser	ver				
<ul> <li>Only to ser</li> </ul>	vers listed on the Name	Servers tab			
Only to the	following servers				
IP Addre	ess	Server FQ	DN		
192.168	.0.100	UC-DC			
				Edit	
To specify secondary servers to be notified of zone Notify					
	OK Cancel	Ар	ply	He	lp

- **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).
- 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 rightclick the CloudBond 365 domain (cloudbond365.local) to select properties.
- 2. Go to the Trusts tab and select New Trust.

<b>a</b>	Active Directory Domains and Trusts
File Action View Help	
← ➡ Ź r  관 II ₪	Actions       General     Trusts     Managed By     Actions       Qomains trusted by this domain (outgoing trusts)     More Actions     More Actions
	New Trust Wizard
	Welcome to the New Trust Wizard           This wizard helps you create a trust between this domain and any of the following:           • A Windows domain in this forest or in another forest.           • A Windows domain in this forest or in another forest.           • A Windows MT 4.0 domain.           • A Kerberos V5 realm trust.           • A nother forest.           • A nother forest.           • A nother forest.           • To continue, click Next.           • Back         Next > Cancel
< III >	

#### Figure 8-11: Creating a Trust

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



New Trust Wizard	x
Trust Name You can create a trust by using a NetBIOS or DNS name.	
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, y must type a DNS name.	ou
Example NetBIOS name: supplier01-int Example DNS name: supplier01-internal.microsoft.com	
internal.contoso.com	
< Back Next > Can	cel

4. Select Forest trust.

#### Figure 8-13: Creating a Trust - Forest Trust

New Trust Wizard
Trust Type This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.
<ul> <li>Select the type of trust you want to create.</li> <li>External trust An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.</li> <li>Forest trust A forest trust A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.</li> </ul>
< Back Next > Cancel

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



New Trust Wizard	x
Direction of Trust You can create one-way or two-way trusts.	
<ul> <li>Select the direction for this trust.</li> <li>Two-way Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in</li> </ul>	
this domain. O One-way: incoming Users in this domain can be authenticated in the specified domain, realm, or forest.	
<ul> <li>One-way: outgoing Users in the specified domain, realm, or forest can be authenticated in this domain.</li> </ul>	
< Back Next > Car	ncel

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

jure 8-15: Creating a Trust - Create Both Sides of th	ne Tru
New Trust Wizard	×
Sides of Trust If you have appropriate permissions in both domains, you can create both sides of the trust relationship.	
To begin using a trust, both sides of the trust relationship must be created. For examp if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.	le,
Create the trust for the following:	
<ul> <li>This domain only This option creates the trust relationship in the local domain.</li> </ul>	
Both this domain and the specified domain This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.	
< Back Next > Ca	ancel

- 8. Specify the enterprise credentials with rights to create the "remote" trust
  - Figure 8-16: Creating a Trust Enter Credentials for the Other Side

	New Trust Wizard
<b>User Name and Pass</b> To create this trust m specified domain.	word elationship, you must have administrative privileges for the
Specified domain: in	emal.contoso.com
Type the user name the specified domain	and password of an account that has administrative privileges in
User name:	2 administrator 🗸
Password:	••••••
	< Back Next > Cancel

- 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

New Trust Wizard	x
Outgoing Trust Authentication Level–Local Forest Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.	
Select the scope of authentication for users from the internal.contoso.com forest.	
<ul> <li>Forest-wide authentication Windows will automatically authenticate users from the specified forest for all resource the local forest. This option is preferred when both forests belong to the same organization.</li> <li>Selective authentication Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you finish this wizard, grant individual access to eac domain and server that you want to make available to users in the specified forest. The option is preferred if the forests belong to different organizations.</li> </ul>	s in th
< <u>B</u> ack <u>N</u> ext > Cance	el

## Figure 8-18: Creating a Trust - Forest Wide

New Trust Wizard
Outgoing Trust Authentication Level-Specified Forest Users in the local forest can be authenticated to use all of the resources in the specified forest or only those resources that you specify.
Select the scope of authentication for users from the local forest.
<ul> <li>Forest-wide authentication Windows will automatically authenticate users from the local forest for all resources in the internal contoso com forest. This option is preferred when both forests belong to the same organization.</li> <li>Selective authentication Windows will not automatically authenticate users from the local forest for any resources in the internal contoso.com forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users from the local forest. This option is preferred if the forests belong to different organizations.</li> </ul>
< <u>B</u> ack <u>N</u> ext > Cancel

- **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
--------	-------	------------	-----------

New Trust Wizard	×
Confirm Outgoing Trust You should confirm this trust only if the other side of the trust has been created.	
Do you want to confirm the outgoing trust?	
$\bigcirc$ No, do not confirm the outgoing trust	
Yes, confirm the outgoing trust	
To confirm the trust now, click Next.	
< Back Next >	Cancel

Figure 8-20: Confirming the Trust



**12.** A successful Trust Creation page should appear.

Figure 8-21:	Completing	the New	<b>Trust Wizard</b>
--------------	------------	---------	---------------------

8	Completing the New Trust Wizard You have successfully completed the New Trust Wizard. Status of changes: The trust relationship was successfully created and confirmed. Route these names to the specified forest: *internal.contoso.com Route these names to the local forest: *.ac-onebox.com	< >
	To close this wizard, click Finish.	
	< Back Finish Car	ncel

# 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

	Active Directory I	Users	and Computers	-	•	x
File Action View Help						
🗢 🔿 📶 📶 🔏 🗐 🗙 🗐	) 🗟 📑 🚺 🖬 🛸	1	2 28			
<ul> <li>Active Directory Users and Com</li> <li>Saved Queries</li> <li>Contoso.local</li> <li>Compute</li> <li>Compute</li> <li>Compute</li> <li>Compute</li> <li>Compute</li> <li>Compute</li> <li>Compute</li> <li>Users</li> </ul> Delegate C Find Change Do Operations New All Tasks Refresh Properties Help	Name Type Second Second Secon	) Gr pup	Description TestUser1 TestUser2 TestUser3 TestUser4 Test DL 1			
Allows you to raise the domain functio	onal level to a level you select.					

3. Click Next.

## Figure 8-23: Delegate Control Wizard

D	elegation of Control Wizard	x
	Welcome to the Delegation of Control Wizard	
	< <u>B</u> ack Next > Cancel Help	

4. Click Add.

Delegation of Control Wizard
Users or Groups Select one or more users or groups to whom you want to delegate control.
Selected users and groups: Administrator (ac-onebox\Administrator)          Administrator (ac-onebox\Administrator)         Add
< <u>B</u> ack <u>Next</u> > Cancel Help

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

Delegation of Control Wizard	x
Tasks to Delegate You can select common tasks or customize your own.	P
Delegate the following common tasks:   Create, delete, and manage user accounts   Reset user passwords and force password change at next logon   Read all user information   Modify the membership of a group   Join a computer to the domain   Manage Group Policy links   Generate Resultant Set of Policy (Planning)   III	
< Back Next > Cancel He	elp

6. Click Finish.

You chose to delegate control of objects in the following Active Directory folder: contoso Jocal/ <ul> <li>The groups, users, or computers to which you have given control are:</li> <li>Administrator (ac-onebox\Administrator)</li> <li>You chose to delegate the following tasks:</li> <li>To close this wizard, click Finish.</li> <li>To close this wizard, click Finish</li> </ul>	<sup>1</sup>	Completing the Delegation of Control Wizard You have successfully completed the Delegation of Control wizard.			
	You chose to delegate control of objects in the following Active Directory folder: <ul> <li>contoso Jocal/</li> <li>The groups, users, or computers to which you have given control are:</li> <li>Administrator (ac-onebox\Administrator)</li> <li>You chose to delegate the following tasks:</li> <li>To close this wizard, click Finish.</li> </ul>				

#### 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

# 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 authoratives 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 .

5				
🚊 dnsmgmt - [DNS\NTDC\Forward L	ookup Zones]			
🚬 Eile Action View Window He	lp			X
⇔ → 🗈 🖬 🖸 😫 🕱 🖬	1 🗐 🗊 🔂			
A DNS	Forward Lookup Zones	4 zone(s)		
E- NTDC	Name	Туре	Status	
E msdcs.ucstatus.int	J_msdcs.ucstatus.int	Active Direct	Running	
1 - Cal ucstatus.com	🛐 ucstatus.com	Active Direct	Running	
. ucstatus.int	🔂 ucstatus.int	Active Direct	Running	
	Ltcp.contoso.com	Active Direct	Running	
Reverse Lookup Zones				
🗄 🔃 Event Viewer				
	I			

#### 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.

Do <u>m</u> ain:	_tcp.contoso.com	
<u>S</u> ervice:	_sipinternaltls	•
<u>P</u> rotocol:	_tcp	*
Pri <u>o</u> rity:	0	
<u>W</u> eight:	0	
Port <u>n</u> umber:	5061	
Host offering this	service:	
ocs.contoso.cor	1	
Allow any aut name. This se	henticated user to update all D tting applies only to DNS record	NS records with the same ds for a new name.

Figure 8-28: New Resource Record

3. View record \_sipinternaltls.\_tcp.contoso.com created in the root of the \_tcp.contoso.com zone.

L dnsmgmt - [DNS\NTDC\Forward	Lookup Zones\_tcp.contoso.c elp	om]	
← →   € 🖪 🗙 🗗 🔒			
DNS	_tcp.contoso.com 3 record	(s)	
	Name	Туре	Data
Composition County Longs and County	( (same as parent folder) (same as parent folder) ( Jane as parent	Start of Authority (SOA) Name Server (NS) Service Location (SRV)	<ul> <li>[1], ntdc.ucstatus.int., ho: ntdc.ucstatus.int.</li> <li>[0][0][5061] ocs.contoso.c</li> </ul>
	•		•

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

🛓 dnsmgmt - [DNS\\NTDC\Forward	Lookup Zones]			_ 🗆 🗙
♣     Elle     Action     Yiew     Window       ←     →     €     10     12     12	jelp D 🗐 🗊 🖓			<u>_8×</u>
A DNS	Forward Lookup Zones 5	zone(s)		
NTDC     Forward Lookup Zones     Forward Lookup Zones	Name	Type Active Direct Active Direct Active Direct Active Direct	Status Running Running Running Running	
	,			

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.

Lookup Zones\ocs.contoso.co	m]	
elp		_8×
ocs.contoso.com 3 record(s	)	
Name	Туре	Data
(same as parent folder)	Start of Authority (SOA)	<ol><li>[1], ntdc.ucstatus.int., hostmaste</li></ol>
(same as parent folder)	Name Server (NS)	ntdc.ucstatus.int.
I (same as parent folder)	Host (A)	10.100.16.25
4		
	elp  Coscontoso.com 3 record(s  Name  (same as parent folder)  (same as parent folder)  (same as parent folder)  (same as parent folder)  (same as parent folder)	elp  coscontoso.com 3 record(s)  Name  Start of Authority (SOA)  (same as parent folder)  Start of Authority (SOA)  (same as parent folder)  Host (A)

#### 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 . /recordaddsip.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:



## Figure 8-32:CloudBond 365 Standard Edition

## 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)
- 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 PortRequirements

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 8-34: 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...)

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	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)

#### Table 8-1: Edge Server

## 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...)

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, CIsController command line (CIsController.exe) or agent (CIsAgent.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, CIsController command line (CIsController.exe) or agent (CIsAgent.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, CIsController command line (CIsController.exe) or agent (CIsAgent.exe) commands and log collection.

Table 8-2: Edge Server



**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).

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

Table	8-3:	AD	Trust
-------	------	----	-------

#### 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 an 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="" server="" web=""> -AppSharingPortCount <at least 100&gt; -AppSharingPortStart <port start=""> cmdlet</port></at </fqdn>		
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="" server="" web=""> - AudioPortCount <at least<br="">100&gt; -AudioPortStart <port start=""> cmdlet</port></at></fqdn>		
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="" server="" web=""> -VideoPortCount <atleast 100&gt; -VideoPortStart <port start=""> cmdlet</port></atleast </fqdn>		



**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	<b>Business</b>	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 <sup>i</sup> 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 operatingsystem 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 <u>Exchange Network Port Reference.</u>

## 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

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

#### Table 8-37: Unified Messaging

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: <u>http://office.microsoft.com.</u>

A reasonable, non-Microsoft, overview of Office 365 can be found at <u>http://en.wikipedia.org/wiki/Office\_365.</u>

### 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 spilt 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.

about Hybrid For information Exchange more deployments, See. https://technet.microsoft.com/en-us/library/jj200581%28v=exchg.150%29.aspx. For more Skype information about for Business Hybrid deployments. see: http://technet.microsoft.com/en-us/library/ji204805.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. <u>https://technet.microsoft.com/en-us/library/jj205403.aspx</u>.



#### 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-foroffice-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: <u>http://technet.microsoft.com/en-us/library/jj151831.aspx</u>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 <u>Active Directory Federation Services (AD FS) 2.0</u>, or <u>Configure Active Directory Federation Services for Windows Azure Pack.</u>
- 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 <u>Hybrid</u> <u>Identity Management.</u>

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

C () I https://portal.office.com	/default.aspx#ActiveUsersPage	으 🖷 이 📕 Integrating Business Processes 🌾 ACS :: SysAdmin >	Overview 8 lync prepare active directory c T
III Office 365			
Office 365 admin center « Search users, admin tasks an P	Dashboard Active User     + キール	S	
	Display name	User name	A Status
DASHBOARD	ACS VPN Trust	acs@OCSHOST.onmicrosoft.com	Synced with Active Directory
⊯ USERS	acs replicate	acsreplicate@OCSHOST.onmicrosoft.com	Synced with Active Directory
Active Users	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: <u>http://blogs.4ward.it/how-to-map-onpremactive-directory-users-to-existing-office365-users/</u>

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.

C C I https://portal.office.com/c	lefault.aspx#ActiveUs	ersPage ♀ ♀ ≧ ¢	Integrating Business Processes	Te ACS :: SysAdmin > Overview	lync prepare active directory c
III Office 365					
Office 365 admin center « Search users, admin tasks ani P	🖉 dashboari + 🏘	ACTIVE USERS			
	Display nat	ne	User name		A Status
SETUP	ACS VPN T	rust	acs@OCSHOST.onmicroso	t.com	Synced with Active Directory
⊿ USERS	acs replica	te	acsreplicate@OCSHOST.or	microsoft.com	Synced with Active Directory
Active Users	ADFSSvcAr	tet	ADFSSvcAcct@activecomm	unications.eu	Synced with Active Directory

#### Figure 9-5: DirSync Working

### 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) (<u>http://technet.microsoft.com/en-us/library/gg398607.aspx</u>) :

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:

#### <u>Copy</u>

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:

#### <u>Copy</u>

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 <a href="http://go.microsoft.com/fwlink/p/?linkld=132204">http://go.microsoft.com/fwlink/p/?linkld=132204</a>.

### 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**.

📔 Active Directory Users and Con	nputers
File Action View Help	
🤄 🗢   🖄 📊 📋 🖳 🧔	🗟   🛛 🖬   🐍 📚 🛅 🍸
Active Directory Users and Comput	rs IERtest 1 ITESTReplication Introller I

Figure 9-6: Delegate Control

3. Click Next.





4. Click Next.

Delegation of Control Wizard	×
Users or Groups Select one or more users or groups to whom you want to delegate control.	P
Selected users and groups:	
Administrator (DCSH0ST \Administrator)	
Add Remove	
< Back Next > Cancel	Help

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

Delegation of Control Wizard	×
Tasks to Delegate You can select common tasks or customize your own.	R
Delegate the following common tasks:	
<ul> <li>Create, delete, and manage user accounts</li> <li>Reset user passwords and force password change at next logon</li> <li>Read all user information</li> <li>Modify the membership of a group</li> <li>Join a computer to the domain</li> <li>Manage Group Policy links</li> <li>Generate Resultant Set of Policy (Planning)</li> </ul>	
C Create a custom task to delegate C Create a custom task to delegate       < Back	Help

6. Click Finish.

Delegation of Control Wizard		×
(Q)	Completing the Delegation of Control Wizard You have successfully completed the Delegation of Control wizard	
	You chose to delegate control of objects in the following Active Directory folder: LyncDev.acs/ The groups, users, or computers to which you have given control are: Administrator (OCSHOST\Administrator) You chose to delegate the following tasks:	
	To close this wizard, click Finish.	
	< Back Finish Cancel Help	

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)

An example PowerShell script that can be used to set the minimum permissions using DSACLS can be found in Appendix  $\underline{A}$ .

# 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 <u>Connecting to Skype for Business Online by using Windows</u> <u>PowerShell.</u>

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: <u>http://www.microsoft.com/en-us/download/details.aspx?id=39366</u> <u>https://support.microsoft.com/en-us/kb/2809243</u>

### 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

ice 365 Settings	
User Name	
admin@ocshost.emea.microsof	ftonline.com
Host:	
sipfed.online.lync.com	
MigrationOverrideUrl:	
https://admin0e.online.lync.com	n/HostedMigration/hostedmigrationservice.svc
OverrideAdminDomain:	
ocshost.onmicrosoft.com	
Password:	
Password:	
Password: Confirm password:	

#### Figure 9-11: CloudBond - Office 365 Connector Information

### 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: <a href="https://webdir0e.online.lync.com/lscp/?language=en-US&tenantID=">https://webdir0e.online.lync.com/lscp/?language=en-US&tenantID=</a> Replace "webdir" in the URL with "admin", resulting in the following: <a href="https://admin0e.online.lync.com">https://admin0e.online.lync.com</a>
- 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 <u>https://technet.microsoft.com/en-us/library/jj673527(v=exchg.150).aspx.</u>

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

```
Set-UMmailboxpolicy -identity "Policy Name in 0365" -
SourceForestPolicy "ACS-0365UM"
```

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

AudioCodes	HOME	USER MANAGEMENT	SYSTEM CONFIGURATION	IP PHONES ABOUT	cloudbond	1365\Administrator LOG (
CLOUDBOND 365 Sta	ndard Box	Edition				
SYSTEM CONFIGURATION System Configuration Server Management		CloudPBX VoiceRe Voice Routing Policies Identity	outingPolicies Management	Actions	PSTN Usage Records	C Actions
Grouping IDs CallPickup Groups Office 365 Configuration Office365 Unified Messaging & CloudPBXPolicies		Global View 1 - 1 of 1	DefaultPolicy	ë ▼ + / ë	Internal           Local           Long Distance           View 1 - 3 of 3           Let < <	© © © 10 ♥ + ©
Music on Hold User Authorization Licensing info "Skype" Control Panel:		Save VRP/PstnUsages	settings	_		
Select a Webserver abclgateway: Select a PSTNGateway	~	Enable Office365 UM RegistrarPool UC sipDomain da Displaynum* *3 Save Office365 UM set	C-FE cloudbond365.com uudbond365.com 1365461223 Check Numbe	▼ ▼		

4. 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

Comparison Comparison (Comparison Comparison)	CN=walter.vanschaik,OU 🔎 🕆 🖒 🏉 Edit Account	×				L	♠ ★ ∅
	GEMENT SYSTEM CONFIGURATION IP P					cloudbond365Administrator	
Code Nove     COURTNAME	COUNTY SYSTEM CONFIGURATION P  Account Information Account Information Account Information Pert Name: Vistame: Vistama: Vistama: Vistame: Vistame: Vistame:	NORES ABOUT	Kottak: Fut Name 1: Domain Name 1: Mail 1:	Water van Schuik       doudbund 365 com       water vanschalk @idoudbord 355 com       Under vanschalk @idoudbord 355 com       Office/365 Eichlange UMPeloy:       Eibable Isaan call	ST Exable call park	etudiood583Admineptate	
	Dial Plan: Description:	M	v	М	M	R	

# 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 mS-DS-ConsistencyGuid attribute, as described in Paul Williams' blog article: <u>http://blog.msresource.net/2014/03/10/windows-azure-active-directory-connector-part-3-immutable-id/</u>, 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.

- Start the initial replication for all Office 365 users through: C:\acs\OFFICE365Sync\SysAdmin.0365.Sync.exe -S 0365
- 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

<b>E</b>					Synchronization Service Manager on DIRSYNCX64
File Tools Actions Help					
Operations Management Agen	ts 🙀 Metaverse Designer 🕡 M	etaverse Search	h 🥡 Joiner		
Management Agents					
Name	Туре	Description		State	
Windows Azure Active Directory Connector	Extensible Connectivity 2.0	Windows Azure	e Active Directory Connec	Idle	
Active Directory Connector	Active Directory Domain Services	Active Director	a		
			₹⊒ <u>R</u> efresh	F5	
			Create	Ctrl+N	
			😭 <u>P</u> roperties	Ctrl + P	
			× Delete	Del	
			🔆 Configure Run Prot	files	
			Run	Ctrl+F5	
			Stop		
			Evnort Managemer	at Agent	
				ic Agencia	
Total number of management agents: 2			🝯 I <u>m</u> port Manageme	nt Agent	
Profile Name: Delta Import Delta Sync User N	ame: ACTIVEVOICE\administrator	D0 4 5 14	🞯 Upd <u>a</u> te Manageme	nt Agent	
Start Time: 12/18/2014 9:57:06 AM	End Time:	12/18/2014 9	🔁 Refres <u>h</u> Schema		
Synchronization Statistics	Connection Sta	atus	Search Connector S	Space	
Staging	COOKIEMONS	TER.ActiveVoid	🧭 Create Extension Pr	ojects 🕨	
Adds 0				,	
Updates 0					

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 onpremises 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.

USER MANAGEMENT	MENU		
User Management	Search User	GoReset	
Create User			
Import User	AC Users  Users/	Licenses-count:121/10000	
Bulk Edit	Status	Full Name	Call Forward
Bulk Import	~	~	~
Group replication	Offline	fsdfsdf fdsfsdf	n/a
Distribution List	Unavailable	Xerox Workcentre M123	Unavailable
	Unavailable	LyncDev 1228	Unavailable
Create Device	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
	View 1 - 10 of 123		14 <4 Page 1 of 13

Figure 9-16: User List

Assign a destination Frontend pool:

#### Figure 9-17: Editing a User Registrar Pool

R MANAGEMENT	Account Informatio	'n
r Management ate User	Account type: Enterpris	se; Remote account: ACTIVEVOICE\0365HV (Office 365 <b>LICATION</b> Cancel Replication
nport User	First Name*	Hybrid
k Edit	Last Nama*	Voice
: Import	Last Maille .	VOIGE
p replication	Sign-in Name*:	O365HV
bution List	Registrar Pool:	Office 365
te Device		
	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\0365Sync\SysAdmin.0365.Sync.exe -S 0365

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

C:\acs\0365Sync\SysAdmin.0365.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\0365Sync\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.

← 🔿 🖳 https://outlook.c	ff	E ×		- □ × ☆ ☆
Cffice 365	Outlo	ok Calendar	Admin 🝷 📿	ø ?
Exchange admin ce	nter			
dashboard	UM dial plans UM IP gateway	S		
recipients				
permissions	Unified Messaging dial plans define the form users, you have to set up at least one dial pla	at for telephone numbers in y	our organization. For UM to answer	calls for your
compliance management	+/=::			
organization	NAME A EXTENS	SION LENGTH	URI TYPE	
protection	ACS-0365 3		SIP URI	
mail flow				
mobile				
public folders				
unified messaging				
		1 selected of 1 total		

Figure 9-19: Exchange Online - UM Dial Plans

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

131

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:	
test	
*Extension length (digits):	
5	
*Dial plan type:	
SIP URI	
*Audio language:	
English (United States)	
*Country/Region code:	
44	<
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	UM dial plans are groups of users who settings for greetings, prompts, audic and outgoing calls.	o are enabled for UM. They share common language, and dialing codes for incoming
settings	Name:	BF Voicemail
dialing rules	Extension length (digits):	4
dialing authorization	Dial plan type:	SIP URI
transfer & search	Audio language:	English (United Kingdom)

### Figure 9-20: New Dial Plan

#### Figure 9-22: Dial Codes

Voicemail Dial Plan

general • dial codes	Set the outside line access code, country/region code, and other dial codes for users in this dial plan.
Outlook Voice Access settings dialing rules dialing authorization	Dial codes for outgoing calls Outside line access code: 
transfer & search	National number prefix
	*Country/Region code: 44
	Number formats for dialing between dial plans Country/Region number format:
	International number format:
	Enter a number format

#### Figure 9-23: Voice Access

Voicemail

general dial codes

general	Add greatings and access numbers for Outlook Voice Access
dial codes	Add greetings and access numbers for Outlook voice Access.
Outlook Voice Access	Welcome greeting: Default greeting
settings	change
dialing rules	
dialing authorization	Informational announcement: <none></none>
transfer & search	change
	Allow announcement to be interrupted
	E.164 routing numbers for your SIP server:
	/ -

Enter an E.164 routing number	+
+4420	
utlook Voice Access numbers	
	1.1
inter a number	т
+4420	

.

general dial codes Outlook Voice Access • settings dialing rules dialing authorization transfer & search	Use this section to set th Primary way to search fo Last first Secondary way to search SMTP address Audio codec: MD3	e options available for users of thi r names: for names:	: UM dial plan.
	Operator extension: "Number of sign-in failu "	res before disconnecting:	
	Timeouts and retries: "Maximum call durat 30 "Maximum recording 20 "Recording idle time 5 "Number of input fai 3	ion (minutes): 1 duration (minutes): out (seconds): lures before disconnecting:	
	English (United Kingdo	m)	×

#### Figure 9-24: Settings

#### Figure 9-25: Dialing Rules

Voicemail Dial Plan

Voicemail Dial Plan

general dial codes Outlook Voice Access	Specify dialing rules to control the types of calls users can make. For rules to t effect, authorize them in the dial plan, UM mailbox policies, and UM auto attendants.			
settinas	In-country/region dialing rules:			
dialing rules				
dialing authorization transfer & search	GROUP NAME	NUMBER PATTERN	DIALED NUMBER	
	All Extensions	•	•	
	All Extensions	•	•	

#### Figure 9-26: Dialing Authorizations

Voicemail Dial Plan

general dial codes Outlook Voice Access settings	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	
dialing rules	Authorized in-country/region dialing rule groups:	
dialing authorization	+ -	
transfer & search	NAME	
	All Extensions	
	Authorized international dialing rule groups:	

NAME	٠

### Figure 9-27: Transfer and Search

Voicemail Dial Plan

general			
dial codes	Specify how callers to users in this dial plan can dial and search for users.		
Outlook Voice Access	Allow callers to:     Transfer to users		
settings	Leave voice messages without ringing a user's phone		
dialing rules dialing authorization transfer & search	Allow callers to search for users by name or alias: O In this dial plan only In the entire organization		
	Only on this auto attendant		
		browse	
	O Only for this extension		
	O In this address list		
		browse	
	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.

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



Figure 9-29: Searching for Skype for Business

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



#### **PowerShell for Skype for Business Online** 9.8

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

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



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: <a href="https://portal.microsoftonline.com/">https://portal.microsoftonline.com/</a> with those credentials and verifying the settings under the users section for the particular account.

+ () thtps://portal.office.co	m/default.aspx#ActiveUsersPage 🔎 = 🚔 🗘 🚺 postal.office.com 🗙
Office 365	
©	
Admin	
Details Settings	You can't edit your own security settings, so not all settings are available here.
Licenses Email address Mailbox permissions	Assign role Choose the admin role that you want to assign to this user and save changes Learn more about administrator roles
More	No Ves Global administrator
	* Alternate email address We'll use this email address as the alternate email address to help the user reset the password. Learn more about recovering your lost password

#### 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:

Active Directory Users and Computers								
File	Action	n View Help						
4	🧢 🔿 📶 🔏 📋 💥 🗊 G 😖 🛛 🖬 🔧 🐮 🍞 🖻 🍇							
	Active Di 🦰 Save	rectory Users and Computers [COOKIEMO] Strang Attribute Editor						
	- i 4	C-No-Policy Walter van Schaik Properties Kalter van Schaik Properties Kal						
	+ + + +	Published Certificates     Member Of     Pa       Security     Environment     Clear     OK       General     Address     Account     Prome       Terminal Services Profile     COM+     Attribute Editor						
	+ + + +	Attributes: Attribute Value msRTCSIP-Archiving <not set=""> msRTCSIP-Deployme SRV: msRTCSIP-Federatio TRUE</not>						

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 0365
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:

2	Windows PowerShell – 🗖 🔜
25 C:\Users\wsc> Get-CsOnlineU	ser   Where-Object {\$sipaddress -match "corp"}
unspaceTd	• 0aa16efa_b5f1_4e00_95f5_5d281db2cceb
serAccountControl	· PasswordNotRequired NormalAccount
	. (ASA000672-4625-4672-0612-2026721024_0)=c5246555-5612-4220-064c_bc562525022_0)=
<b>,</b>	0 CS Tenants DC1-4012-3012-402-012-012-017-00-01-012-017-010-43-00-504C-00-0035232484,00-
untrvAbbreviation	
untrvOrRegionDisplavName	
many	
partment	
scription	
x	
mePhone	
Phone	
ty/	
nager	
bilePhone	
iginatorSid	
herTelenhone	i n
Fice	
stalCode	
eferned anguage	
er er reucanguage	1002855085120845
at o0 nBnow in co	10036FFD8C12084C
aceorprovince	
reel	
reetAddress	
umphai IPhoto	
tie	
one	
bPage	
minDescription	
isignedPlan	: { <xmivalueassignedplan <="" td="" xmins:xsd="http://www.ws.org/2001/XMLSchema"></xmivalueassignedplan>
	xmlns:xs1="http://www.w3.org/2001/XMLSchema-instance">
	<pre><plan <="" assignedlimestamp="2014-10-14108:20:332" pre=""></plan></pre>
	ServicePlanId="0feaeb32-d00e-4d66-bd5a-43b5b83db82c" CapabilityStatus="Enabled"
	SubscribedPlan1d="c4b86aed-a92a-42ea-a84a-d2148/ed014f"
	ServiceInstance="MicrosoftCommunicationsOnline/Instance03-5"
	xmlns="http://schemas.microsoft.com/online/directoryservices/change/2008/11">
	<capability></capability>
	<capability <="" plan="MCOProfessional" td=""></capability>
	xmlns="http://schemas.microsoft.com/online/MCO/2009/01" />
	}
ias	: corporatead
seSimpleUrl	: https://meet.lync.com/ocshost
rSyncEnabled	: True
jectId	: 49290bf3-d625-4df2-9612-a02c93f710ed
ageLocation	: NL
deFromAddressLists	: False
PremHideFromAddressLists	: False
ovisionedPlan	· :
ovisioningStamp	
gradeRetryCounter	: 0
ncingCounter	
ovisioningCounter	: 0
blishingStamp	
blishingCounter	: 0
PremHostingProvider	: SRV:
PremOptionFlags	: 257
PremSIPEnabled	: True
PremSipAddress	: sip:corporatead@activecommunications.eu
PremineliRT	

Figure 9-35: Get-csOnlineUser Attributes

We are specifically interested in the following attributes:

- OnPremHostingProvider: SRV:
- OnPremOptionFlags 257
- OnPremSIPEnabled : True
- OnPremSipAddress : <u>sip:corporatead@activecommunications.eu</u>

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

<del>4</del>						
File Tools Actions Help						
Poperations Management Agents 🔐 Metaverse Designer 🚑 Metaverse Search 🥥 Joiner						
Management Agents						
Name Type		Description	State			
Windows Azure Active Directory Extensible Connectivity 2.0 Windows Azure Active Director Idle						
Properties X						
Management Agent Designer	Select Attributes					
Properties	Attributes:	Show /	Ali			
Select Extension DLL						
Connectivity						
Configure Partitions and Hierarchies	msRtcSipApplicationOptions					
Select Object Types	✓ msRtcSipLine					
⇒ Select Attributes	✓ msRtcSipOptionFlags					
Configure Anchors	✓ msRtcSipOwnerUm					
Configure Connector Filter	msRtcSipPrimaryUserAddress					
Configure Join and Projection Rules	✓ msRtcSipUserEnabled ✓ onPremiseSecurityIdentifier					

#### Figure 9-36: Windows Azure AD Properties

#### Figure 9-37: DirSync AD Connector properties

Active Directory Connector Active Directory Domain Services Active Directory Connector. Idle						
Properties X						
Management Agent Designer	Select Attributes					
Properties	Attributes:	Show	All			
Connect to Active Directory Forest						
Configure Directory Partitions	✓ msOrg-lsOrganizational					
Configure Provisioning Hierarchy	msRTCSIP-ApplicationOption	ns				
Select Object Types	msRTCSIP-DeploymentLoca	tor				
⇒ Select Attributes	msRTCSIP-Line					
Configure Connector Filter	msRTCSIP-OptionFlags					
Configure Join and Projection Rules	msRTCSIP-OwnerUm					
Configure Attribute Flow	I I Instructor - Frimary UserAddr	635				
Configure Deprovisioning						

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.0365.Sync.exe -S 0365

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

ice 365 Settin	js					
loor Namo:						
admin@ocshost.ei	nea microsoftor	line com				
Jaat.						
sipfed online lync.	om					
Vigration Override						
https://admin0e.on	n. ine lync com/Ho	stedMigration/ho	stedmiorationse	ervice svc		
		orounigrationino	otoanngrationioa			
OverndeAdminDon	ain: ft.com					
00311031.0111101030	1.com					 
Password:						
Confirm password:					_	



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: <u>http://en.wikipedia.org/wiki/Public\_key\_infrastructure</u>

# **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
  - <u>https://meet.contoso.com</u>
  - https://admin.contoso.com
  - <u>https://dialin.fabrikam.com</u>

# **C**audiocodes

- https://meet.fabrikam.com
- <u>https://admin.fabrikam.com</u>
- 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.
  - <u>https://meet.contoso.com/dialin</u>
  - <u>https://meet.contoso.com/meet</u>
  - <u>https://meet.contoso.com/admin</u>
  - <u>https://meet.fabrikam.com/dialin</u>
  - <u>https://meet.fabrikam.com/meet</u>
  - <u>https://meet.fabrikam.com/admin</u>
  - 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.
  - <u>https://meet.contoso.com/contoso.com/dialin</u>
  - <u>https://meet.contoso.com/contoso.com/meet</u>
  - https://meet.contoso.com/contoso.com/admin
  - https://meet.contoso.com/fabrikam.com/dialin
  - <u>https://meet.contoso.com/fabrikam.com/meet</u>
  - <u>https://meet.contoso.com/fabrikam.com/admin</u>
    - 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/enus/library/hh690012.aspx http://technet.microsoft.com/enus/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

Topology Builder					
Welcome to Topology Builder. Select the source of the Lync Server topology document.					
<ul> <li>Download Topology from existing deployment Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.</li> </ul>					
<ul> <li>Open Topology from a local file</li> <li>Open an existing Topology Builder file. Use this option if you have work in progress.</li> </ul>					
<ul> <li>New Topology Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.</li> </ul>					
Help OK Cancel					

9. Click Save.

Figure 10-3: Saving the Topology



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

F	igure 10-4: Topo	logy Builder
14 C	Lync Server 2013, Topo	ology Builder
File Action Help	SIP domain Default SIP domain: Additional supported SIP domains:	contoso.com Not configured
	Simple URLs	•
	Phone access URLs:	Active Simple URL https://meet.contoso.com/dialin
	Meeting URLs:	Active Simple URL SIP domain https://meet.contoso.com/meet contoso.com
	Administrative access URL:	Not configured
	Central Management Serv	ver 🔺
	Central Management Server:	Active Front End Site ACS-UC-FE.ACS-Unified-Communic ACS-2013

## 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).

2	Lync Server 2013, Topo	logy Bui	lder	
ile Action Help	SIP domain			
<ul> <li>m ACS-2013</li> <li>m Acs-2010</li> <li>m Lync Server 2010</li> <li>m Lync Server 2013</li> <li>m Shared Components</li> <li>m Branch sites</li> </ul>	Default SIP domain: Additional supported SIP domains: Simple URLs	contos Not co	o.com nfigured	
	Phone access URLs:	Active	Simple URL	
	Meeting URLs:	Active	https://meet.contoso.com/dialin Simple URL	SIP domain
	Administrative access URL:	✓ Not co	https://meet.contoso.com/meet nfigured	contoso.com
	Central Management Serv	rer		
	Central Management	Active	Front End	Site
	Server	1	ACS-UC-FE ACS-Unified-Communic	ACS-2013

### Figure 10-5: Viewing a Topology

2. From the menu options, select Edit Properties.

Figure 10-6: Edit Properties of the Server

New Central Site Edit Properties
New Topology
Open Topology
Download Topology
Save a copy of Topology As
Publish Topology
Install Database
Merge Office Communications Server 2007 R2 Topology
Remove Deployment
Help

#### 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
--------------	------------	-----	---------

10	Edit Properties	
SIP domain	SIP domain	▲ ^
Simple URLs Central Management	Default SIP domain: *	
Server	contoso.com	
	Additional supported SIP domains:	=
	Add	=
	Update	
	Remove	
	Simple URLs	<b>^</b>
	Simple URLs will be sent to your users and used by them to access the web pages for dial-ir conferencing phone numbers, meetings, and administration. The active URL is used when n	n ew
	meetings are scheduled. Other URLs are used to support any meetings that have been sche	duled in
	URLs, including https://. If you change a Meeting or Phone access URL after it has been pub	lished, you
	prevent users from joining existing meetings or conferences. To change the active URL, crea	ite a new 🗡
Help	ОК	Cancel

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

6	Edit Properties	x
SIP domain	SIP domain	^
Simple URLs Central Management Server	Default SIP domain: * contoso.com	
	Additional supported SIP domains:	
	Add	=
	fabrikam.com Update	
	Remove	
	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	~
Help	OK Cance	el

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

#### 10.5.1.1.2Changing 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

	Warning	x
?	Changing your default SIP domain can have a major impact on configured users, devices, and identities in your deployment. Certificates and federation settings may also need to be modified. you sure you want to continue?	Are
	Yes	No



**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

Lync Server 2013, Topology Builder			
SIP domain			
Default SIP domain: Additional supported SIP domains:	contos Not co	o.com nfigured	
Simple URLs			
Phone access URLs:	Active	Simple URL	
Meeting URLs:	Active	Simple URL	SIP domain
Administrative access URL:	Not co	nfigured	
Central Management Serv	er		
Central Management	Active	Front End	Site
	SIP domain  SIP domain  Default SIP domain:  Additional supported SIP domains:  Simple URLs  Phone access URLs: Meeting URLs: Administrative access URL: Central Management Serve	SIP domain           SIP domain         contos           Additional supported         Not co           SIP domains:         Simple URLs           Phone access URLs:         Active           Meeting URLs:         Active           Administrative access         Not co           URL:         Central Management Server	SIP domain         Default SIP domain:         Additional supported         SIP domains:         Simple URLs         Phone access URLs:         Active         Simple URLs         Phone access URLs:         Active         Simple URL         Verting URLs:         Not configured         URL:         Central Management Server

- 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 UR	Ls – Using	Option 2
------------------------	-----------	------------	----------

10	Edit Properties	
SIP domain Simple URLs Central Management Server	Simple URLs 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	
	Meeting URLs:       Simple URL     SIP domain       Image: Add     Add       Image: Add     Remove         Make Active     Edit URL	
Help	OK Cancel	

ð	Edit Properties	x
SIP domain Simple URLs Central Management Server	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 the past by using those URLs. Meeting and Phone access simple URLs are required and must be f URLs, including https://. If you change a Meeting or Phone access URL after it has been publishee prevent users from joining existing meetings or conferences. To change the active URL, create a re active URL and leave the current URL inactive. An inactive URL can be removed after all conference meetings that use it have expired or been deleted.	Lin full J, you tew tes or
	Phone access URLs:       Simple URL       Image: Add the state of the stateo	l
	Meeting URLs: Simple URL SIP domain Add 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 Make Active Edit URL Administrative access URL:	Dove
Help	https://lync.contoso.com/admin OK	Cancel

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



**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:**
- 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.

10	Lync Server 2013, To	pology Builder	- 🗆 X
File Action Help	a second a second		<u>^</u>
<ul> <li>Ipurc Server</li> <li>Ipurc Server 2010</li> <li>Ipurc Server 2013</li> <li>Standard Edition Front End Servers</li> <li>Standard Edition Front End Servers</li> <li>Context Context C</li></ul>	General FQDN: IPv4 addresses: Features and functionality Instant messaging (IM) and presence: Conferencing: PSTN conferencing: Enterprise Voice: Associations SQL Server store: Archiving SQL Server store: Monitoring SQL Server store: File store: Office Web Apps Server: Edge pool (for media): Note: To view the federati	ACS-UC-FE.ACS-Unified-Communications.net Use all configured IPv4 addresses Enabled Enabled Enabled ACS-UC-FE.ACS-Unified-Communications.net/tx ACS-UC-DC.ACS-Unified-Communications.net/Default ACS-UC-DC.ACS-Unified-Communications.net/Default VACS-UC-FE.ACS-Unified-Communications.net/share Not associated ACS-UC-FE.ACS-Unified-Communications.net (ACS-2013) on route, use the site property page.	
< III >	<	881	>

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

0	Edit Properties	x
General Resiliency	Web services Listening port defines the IIS configuration on servers in the pool and Published port reflects the	<u> </u>
Mediation Server	configuration of a load balancer, a reverse proxy, or a firewall. After you make changes to the fully qualified domain name (FQDN) or listening ports, you must run local Setup on all servers in the pool in order for these changes to take effect. Internal web services	
	Listening ports: * HTTP: 80 HTTPS: 443 Published ports: * HTTP: 80 HTTPS: 443	
	External web services FQDN: * evslync.contoso.com	
	Listening ports: * HTTP: 8080 HTTPS: 4443 Published ports: * HTTP: 80 HTTPS: 443	
	Mediation Server	_
Help	Collocated Mediation Server enabled Collocated Mediation Server cannot be removed because it is being used by trunks in table below.	

## **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

10	Lync Server 2013, To	pology Builder		x
File Action Help	General			^
<ul> <li>ACS-2013</li> <li>Iync Server 2010</li> <li>Iync Server 2013</li> <li>Standard Edition Front End Servers</li> <li>Enterprise Edition Front End pools</li> <li>Director pools</li> <li>Persistent Chat pools</li> <li>Edge pools</li> <li>Edge pools</li> <li>Trusted application servers</li> <li>Shared Components</li> <li>Branch sites</li> </ul>	Internal server FQDN: Internal IPv4 address: Federation (port 5061): XMPP federation (port 5269): Internal Configuration Replication Port (HTTPS) Next hop selection Next hop pool:	ACS-UC-Edge ACS-Unified-Communications.net 192.168.0.103 Enabled Enabled 4443 ACS-UC-FE.ACS-Unified-Communications.net (ACS-2013)		=
	External settings Access Edge service FQDN: IPv4 address: Port: Protocol:	sip.conteso.com 10.253.2.165 5061 TLS	•	
< III >				~

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

Figure 10-16: Edge Sever External Access FQDNs

10	Edit Properties			-	
General	External settings				▲ ^
Next hop Edge Server configuration	Specify the external, fully qualified domain names (FQDNs) and ports for A Conferencing Edge, and A/V Edge services. The combinations of FQDN and Enable separate FQDN and IP address for web conferencing and A/V Enable IPv4 on external interface Enable IPv6 on external interface	ccess Edg	ge, Web ust be unio	que.	
	A/V Edge service is NAT enabled				
	Access Edge service FQDN: *	Port	5		
	sip.contoso.com	: 506	1 (П	.S)	
	IPv4 address: * 192.168.254.103				=
	IPv6 address:				
	Web Conferencing Edge service FQDN:				
	sip.contoso.com	: 444	(П	.S)	
	IPv4 address: 192.168.254.103				~
Help			OK		Cancel

- 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:

16	Ly	nc Server 2013, Top	ology	Builder		- • >	¢
File Acti	n Help New Central Site Edit Properties New Topology Open Topology Download Topology Save a copy of Topology As Publish Topology Install Database Merge Office Communications Server 200 Remove Declorament	17 R2 Topology	- ∶ =d	acs-unified-communications.net Not configured			^
	Help		_	Active	https://dialin.acs-unified- communications.net		≡
		Meeting URLs:		Active	Simple URL	SIP do	
				~	https://meet.acs-unified- communications.net	acs-unit commu .net	
		URL: Central Manageme	ess nt Serve	Not con	(tgured		
		Central Manageme Server:	ent	Active	Front End ACS-FE15.ACS-Unified-Commu	Sir nicat <u>ACS-20</u>	
		٢		ш		>	Ť

#### Figure 10-17: Publishing the Topology - Actions

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



Publish Topology	x
Publish the topology	
In order for Lync Server 2013 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:	
<ul> <li>A validation check on the root node did not return any errors.</li> <li>A file share has been created for all file stores that you have configured in this topology.</li> </ul>	^
<ul> <li>All simple URLs have been defined.</li> <li>For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured.</li> <li>For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.</li> </ul>	=
<ul> <li>You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).</li> </ul>	· 📃
<ul> <li>If you are removing a Front End pool, all users, common area phones, analog devices, application contact objects, and conference directories have been removed from the pool.</li> <li>When you are ready to proceed, click Next.</li> </ul>	1 <u>~</u>
Help Back Next Canc	el

2. Click Next.



16	Publish Topology	x
Sele	ct Central Management Server	
Only Centr	one Front End pool in the deployment can have a Central Management store. All pools use the san al Management store.	ne
Select	t the Front End pool that will host the Central Management store:	
ACS	-UC-FE.ACS-Unified-Communications.net ACS-2013	•
	Advanced.	
He	Back Next Cancel	

#### 3. Click Next.

		Publish	Topology		
rea	te databases				
he fo ot be ataba ith a	ollowing dedicated databases een created. If you have the a ases when you publish your i ppropriate permissions can d	are part of your oppropriate perm topology. If you create the databa	topology. Some of the da issions on the SQL Server do not have the appropria ises later.	atabases listed , you can creat te permission:	below have te the s, someone
reate	Store	Site	Databa:	e paths	
~	ACS-UC-DC.ACS-Unifie	ACS-2013	Automatically determ	ine database f	file locat
					Advanced
lote: re co atab erver	Only databases on dedicated Ilocated with other server co ases for Lync Server 2010 co 2010 Management Shell.	d SQL Servers car mponents must mponents must l	n be installed from here. D be installed by running lo be installed by running Ins	Patabases on S cal setup on th stall-CsDataba	QL servers that ne machine. se in the Lync



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

4. Click Finish.

۰,	Publish Topology	,	x
Pub	lishing wizard complete		
Your	topology was successfully published.		_
* * * * *	Step Publishing topology Downloading topology Downloading global simple URL settings Updating role-based access control (RBAC) roles Enabling topology	Status Success Success Success Success Success	View Logs
To cl	lose the wizard, click Finish.		
Н	ielp	Back Finish	Cancel

#### Figure 10-21: Publishing the Topology Completes

#### 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:





1. Select Install or Update Lync Server System.





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

x Lync Server 2013 - Deployment Wizard Lync Server 2013 Welcome to Lync Server deployment. Deploy > Lync Server 2013 2 Step 1: Install Local Configuration Store Installs local configuration store and populates with data from Central Management Store. Prerequisites > ✓ Complete Run Again Help + Step 2: Setup or Remove Lync Server Components Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition. Prerequisites + ✓ Complete Run Again Help 🕨 Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition. Prerequisites + ✓ Complete Run Again Help ▶ Step 4: Start Services Initiates a start request for all Lync Server services. Note: This step does not verify that the services have actually started. To do so, launch the Services MMC tool through the "Service Status" step in the Deployment UI. Prerequisites + Run Help 🕨 Back Exit

Figure 10-24: Updating Skype for Business Components

3. Click Next.

#### Figure 10-25: Setup Server Components

1	Set Up Lync Server Components	x
	Set Up Lync Server Components	
Install ar This step	nd activate, or deactivate and uninstall Lync Server components based on the topology definitio o may take several minutes.	on.
Help	Back Next Cancel	

4. Click Finish.

## Figure 10-26: Finishing the Wizard

ē.	Set Up Lync Server Components	x
	Executing Commands	
Checkin Checkin Installin Executin Report [13_25_ Enablin This ste Executin \Admin	g prerequisite MSSpeech_SR_zh-HK_TELEprerequisite satisfied. g prerequisite MSSpeech_SR_zh-TW_TELEprerequisite satisfied. g prerequisite UcmaWorkflowRuntimeprerequisite satisfied. g any collocated databases g PowerShell command: Install-CSDatabase -Confirm:\$false -Verbose -LocalDatabases - C:\Users\Administrator.ACSLync\AppData\Local\Temp\1\Install-CSDatabase-[2013_07_04] 10].html" new roles o will configure services, apply permissions, create firewall rules, etc. g PowerShell command: Enable-CSComputer -Confirm:\$false -Verbose -Report "C:\Users strator.ACSLync\AppData\Local\Temp\1\Enable-CSComputer-[2013_07_04][13_25_47].html"	^ III
Task stat	ıs: Completed.	
Bootstra	local machine	9
Help	Back Finish Cancel	

# **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



<b>65.</b>	Administrator: Command Prompt	
Microsoft Windows (c) 2012 Microsoft	[Version 6.2.9200] Corporation. All rights reserved.	
$\begin{array}{l} c: Nisers \land Admin is transformed a constant of the second $	ator>certutil -ca.cert c:\EnterpriseRoot.ce alid GATE IGMZONUOF8g+N0pUSdW5n4bTANBgkqhkiG9w0BAQUFA JGDGFN122FHRcwFQVKCZIniZFyLGQBGRWH22NuG9ab KWCGIudGUybmFaHBaWHQYDUQDExZpbnRlen5hbC1DT ExPDQ2MDAINTIIOF78HDZ4NDAINIJGHNAWSS Rlen5hbEcHBGG1UBAWWAWSGZJUGVUG9T ZIhveNAQEBBQADggEPADCCAQeCggEBALy2MManQ9iog JIN9VIWSG9HLUG-JbCHp2122BUBADBgt2SG630HPL Dour?PuGPMWHcOPOgyZ346ie0upZjZHuAxnG?V6kDx5 JHV9IWSG9HLUG-JbCHp2122BUBADBgt2SG630HPL Dour?PuGPMWHcOPOgyZ346ie0upZjZHuAxnG?V6kDx5 b54zHM3u202HLUG-JbCHp2122BUBADBgt2SG630HPL Dour?PuGPMWHcOPOgyZ346ie0upZjZHuAxnG?V6kDx5 b54zHM3u204H2cfbEx9DABADgt2SG630HPL HUHY4tmkxHe62xIxiSF97KHJy2PIYxkgXHd1Y/v2UP 8wCWDWBPBAQDAgGCM8GAIUHEVEZv4PMMBAF8UJ 1EBGQnc+X1j6eHkjvc4nSIEUUtdf5cvgmSR2kuffUby UIXG2GOI+4dmEB182F+4dC60g/BjcUnQDMgEAM JUXG2SJIH291bABACSSGCJJFFRJIZXKIED 05ggkvHQnF2SIJH24FH20F5FWIAB6/c2sk27 gghvHQnF4zFzRIp0F1WB127f2x2120WwJRB0ji T60n-20HzOHLbdH7S4FD0gJ1B TE	р = = DBp zzEY Ø5J BBC Gigo J Git E BBC Gis QVD Gis QVD Gis QVD Gis QVD Gis QVD Haff Ta8
CertUtil: -ca.cert	command completed successfully.	
C:\Users\Administı	ator>	✓
		Windows Server 2012

### 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

2				Console1	- [Console Root]				-		x
	File Action View Fa	avorites Windo	w F	lelp						-	×
	• 🔿 🖬 🗟 🖬	]									
	Console Root	Name						Actions			
			A	dd or Remo	ve Snap-ins				x	t	•
	You can select snap-ins for the extensible snap-ins, you can	his console from th configure which e:	iose av xtensio	vailable on your ons are enabled	computer and configure th	e selected si	et of snap-in:	s. For		ns	•
	Soan-in	Vendor		Se I	Console Root	_	EditEvt	encione			
	Active Directory Do	Microsoft Cor			Certificates (Local Co	omputer)	CONCERN	Charlen art.	_		
	Active Directory Site	Microsoft Cor					Re	move			
	Active Directory Use	Microsoft Cor	=								
	ActiveX Control	Microsoft Cor					Mo	ve Up			
	AUSI Edit	Microsoft Cor					Mour	a Down			
	Certificates	Microsoft Cor		Add >			11000	C DOWN			
	Component Services	Microsoft Cor									
	Ecomputer Managem	Microsoft Cor									
	🚔 Device Manager	Microsoft Cor									
	Disk Management	Microsoft and									
	A DNS	Microsoft Cor									
	Event Viewer	Microsoft Cor	-				Adva	nced			
	Folder	Microsoft Cor	Ľ.,	L			Auto				
k	Description:										
H	You can use the Active Dire	ctory Domains and	Trust	s snap-in to mar	age Active Directory doma	ins and trus	ts.				
L.											
							OK	Canaal			
							UK	Cancel			

5. Click the Computer account option.

#### Figure 10-29: Install the Root Certificate – Computer Account



6. Select Local computer.

#### Figure 10-30: Select Computer

Select the computer you w	ant this snap-in to manage.	
This snap-in will always r	nanage:	
Ocal computer: (the	e computer this console is running on)	
O Another computer:		Browse
Allow the selected only applies if you sa	omputer to be changed when launching from the co ave the console.	mmand line. This

- 7. Click Finish, and then click OK.
- 8. Right-click Trusted Root Certification Authorities > All Tasks and select Import.

Console1 - [Console Root\Certificates (Local	Computer)\Trusted Root Certificatio	n Authorities\ 🗕 🗖 🗙
File Action View Favorites Window Help		_ & ×
Console Root       Issued To         ▲ ② Certificates (Local C       ACS-Unified-Communication         ▶ ③ Personal       Baltimore Cyber Trust Root         ▲ ③ Trusted Root Ce       Cass 3 Public Primary Ce         ● ③ Enterp       All Tasks         ▶ ③ Interrn       View         ▶ ③ Truste       New Window from Here         ▶ ③ Truste       New Taskpad View         ▶ ③ Client       Export List         ▶ ③ Certifi       Help         ▶ ③ Trusted Devices       > ③ Web Hosting	Issued By ations ACS-Unified-Communications-A at Baltimore CyberTrust Root rtificat Class 3 Public Primary Certificatio Import nr Co Nr Co No Norcosoft Authenticode(tm) Root Microsoft Authority Auth Microsoft Root Certificate Authori Auth Microsoft Root Certificate Authori Auth Microsoft Root Certificate Authori (c)97 N LIABILITY ACCEPTED, (c)97 V Thawte Timestamping CA	Expiral         Actions           26/04/ 13/05/ 2/08/2         Certificates
Contains actions that can be performed on the item.		>

#### Figure 10-31: Trusted Root Certificates

9. Complete the Certificate Import Wizard.

Figure 10-32: Importing the Certificate

💿 👼 Certificate Import Wizard	X
Welcome to the Certificate	Import Wizard
This wizard helps you copy certificates, cer lists from your disk to a certificate store.	tificate trust lists, and certificate revocation
A certificate, which is issued by a certificati and contains information used to protect d connections. A certificate store is the syste	on authority, is a confirmation of your identity ata or to establish secure network em area where certificates are kept.
Store Location	
Local Machine	
To continue, dick Next.	
	Next Cancel

**10.** Specify the certificate file copied from the Enterprise CA.

Figure 10-33: Certificate Import Wizard

🕑 🍠 Certificate Import Wiza	rd
File to Import Specify the file you want to in	nport.
File name: C:\temp\EnterpriseRoot.cer	Browse
Note: More than one certifica Personal Information Exch Cryptographic Message Sv	ite can be stored in a single file in the following formats: ange-PKCS #12 (.PFX,.P12) ntax Standard-PKCS #7 Certificates (.P7B)
Microsoft Serialized Certific	ate Store (.SST)
Learn more about <u>certificate file fo</u>	<u>rmats</u>
	Next Cance

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

The console - [Console	Root\Certificates (Local Compu	uter)\Trusted Root Certificatior	Auth
🔚 File Action View	Favorites Window Help		
(= =) 🖄 📰 📋	à 🔒 🛛 🖬		
📔 Console Root	Issued To	Issued By	Expira
⊿ 🗊 Certificates (Local C	ACS-Unified-Communications	ACS-Unified-Communications-A	26/04
Personal	🔄 Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05
⊿ 🚞 Trusted Root Ce	🔄 Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	2/08/2
🦲 Certificates	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/01/2
Enterprise Trust	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	31/12
Intermediate Cei	internal-CONTOSO-DC-CA	internal-CONTOSO-DC-CA	30/04
Trusted Publishe	Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	1/01/2
Untrusted Certifi	Microsoft Root Authority	Microsoft Root Authority	31/12

# **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

Lync Serve	r 2013 - Deployment Wizard
Lync Server 2013 Welcome to Lync Server deployment.	
eploy > Lync Server 2013	4
Step 1: Install Local Configuration Store Installs local configuration store and populates	/ with data from Central Management Store.
Prerequisites  Help	Complete Run Again
the second of the second time the second sec	
Install and activate, or deactivate and uninstall L Prerequisites	ync Server Components based on the topology definition.
Step 2: Setup or kemove Lync Server Components Install and activate, or deactivate and uninstall L Prerequisites > Help >	ync Server Components based on the topology definition. ✓ Complete Run Again
Step 2: Setup or kemove Lync Server Components Install and activate, or deactivate and uninstall L Prerequisites ► Help ► Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create ce this system based on the topology definition.	ync Server Components based on the topology definition. Complete Run Again  tificate request for local system. Install, and assign certificates for
Step 2: Setup or kemove Lync Server Components         Install and activate, or deactivate and uninstall L         Prerequisites ▶         Help ▶         Step 3: Request, Install or Assign Certificates         This step starts the Certificate Wizard. Create ce this system based on the topology definition.         Prerequisites ▶	ync Server Components based on the topology definition. Complete Run Again  tificate request for local system. Install, and assign certificates for

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.

5		Certificate Wiz	zard				
Select a Lync Server Certificate Type and then select a task. Expand the Certificate Type to perform advanced certificate usage tasks.							
Certificate		Friendly Name	Expiration Date	Location	Request		
<ul> <li>Default certificate</li> </ul>	$\checkmark$	ACS FE	1/07/2015 5:02:09 PM	Local	Assian		
<ul> <li>Server default</li> </ul>		ACS FE	1/07/2015 5:02:09 PM	Local	Assign		
✓ Web services internal		ACS FE	1/07/2015 5:02:09 PM	Local	Remove		
Web services external	•	ACS FE	1/07/2015 5:02:09 PM	Local	View		
✓ OAuthTokenIssuer	~	ACS FE OATI	1/07/2015 5:02:11 PM	Local			
<	_	ш		>			
Help Refresh Im	port C	ertificate Process Pending Certifi	icates		Close		

# Figure 10-39: Front-End 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

2	Lync Server 2013 - Deployment V	Vizard	x
	Lync Server 2013 Welcome to Lync Server deployment.		
Deploy			2
	Prepare Active Directory Prepares the Active Directory schema, forest, and domain for Lync Server. Help → ✓ Complete Install or Update Lync Server System Install or update a Lync Server Server deployment member system. This option installs Lync Server core components, and a local replica configuration store. Note: Before installing a server, you need to have a valid topology created and published. Help →	Prepare first Standard Edition server Prepares a single Standard Edition server to host Central Management Service. Note: This task requires local administrator rights. This task does not apply to Standard Edition Servers that are not planned to host the Central Management Service, or for deployments that include Enterprise Edition. Install Administrative Tools ✓ Installs the Administrative Tools of Installs the Administrative Tools to the current system. Your deployment requires at least one installation of the Topology Builder. Deploy Monitoring Reports Deploy Monitoring Reports Deploy Monitoring Reports Click to view getting started videos. Documentation Click to view the latest Lync Server documentation online for deployment, planning, and operations. Tools and Resources Click to access tools and other resources	< III >
		Back Exit	

3. Click the Run Again button in Step 3: Request, Install or Assign Certificates.

#### Figure 10-42: Requesting a Certificate

🗟 Lync Server 2013 - D	eployment Wizard	x
Upic Server 2013 Welcome to Lync Server deployment.		
Deploy > Lync Server 2013		2
Step 1: Install Local Configuration Store Installs local configuration store and populates with data fro	om Central Management Store.	^
Prerequisites + Help +	✓ Complete Run Again	
Step 2: Setup or Remove Lync Server Components Install and activate, or deactivate and uninstall Lync Server (	Components based on the topology definition.	
Prerequisites 🕨		
Help 🕨	Complete Run Again	=
Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate requisits system based on the topology definition. Prerequisites >	uest for local system. Install, and assign certificates for	
Help 🕨	Complete Run Again	

# **C** audiocodes

4. Expand the Default Certificate and ensure the appropriate roles are selected. Click **Request**.

6	Certificate Wizard				x	
Select a Lync Server Certificate Ty	Select a Lync Server Certificate Type and then select a task. Expand the Certificate Type to perform advanced certificate usage tasks.					
Certificate		Friendly Name	Expiration Date	Location	Request	
<ul> <li>Default certificate</li> </ul>	~	ACS FE	1/07/2015 5:02:09 PM	Local	Assian	
<ul> <li>Server default</li> </ul>		ACS FE	1/07/2015 5:02:09 PM	Local	- Assign	5
✓ Web services internal	•	ACS FE	1/07/2015 5:02:09 PM	Local	Remove	_
Web services external	•	ACS FE	1/07/2015 5:02:09 PM	Local	View	
✓ OAuthTokenIssuer	~	ACS FE OATI	1/07/2015 5:02:11 PM	Local		
<				>		
Help Refresh Im	port C	ertificate Process Pending Certifi	cates		Close	

### Figure 10-43: Front-End Certificate for Internal Use



0		Certificate Wiz	ard		x
Select a Lync Server Certificate Ty	be and	then select a task. Expand the Ce	rtificate Type to perform adva	anced certificate	usage tasks.
Certificate		Friendly Name	Expiration Date	Location	Request
<ul> <li>Edge internal</li> </ul>	~	ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local	Assign
✓ Edge internal	•	ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local	Pamawa
<ul> <li>External Edge certificate (pr</li> </ul>	~	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local	View
<		Ш		>	
Help Refresh Im	port C	ertificate Process Pending Certifi	cates		Close

5. Complete the Wizard.

#### Figure 10-45: Certificate Request

6	Certificate Request	x
¢	Certificate Request	
Request Lync Sen	a certificate for the Default certificate (Server default,Web services internal,Web services external ver usages.	1)
Help	Back Next Cancel	

6. Select Send the request immediately.

## Figure 10-46: Delayed or Immediate Requests

6	Certificate Request	x
	Delayed or Immediate Requests	
Do you v certificati	vant to prepare a certificate request to be sent later, or do you want to send it now to an online ion authority?	è
Send	the request immediately to an online certification authority	
O Prepa	are the request now, but send it later (offline certificate request)	
Help	Back Next Cancel	

7. Specify the Enterprise CA.

## Figure 10-47: Creating Certificate Requests

2	Certificate Request
¢	Choose a Certification Authority (CA)
Select a c the select	ertification authority to process your request. The Certificate Wizard will automatically import ted CA's certificate chain if necessary. t a CA from the list detected in your environment.
ACS	-UC-DC.ACS-Unified-Communications.net\ACS-Unified-Communications-ACS-UC-DC-CA
Species	fy another certification authority.
cont	oso-dc.internal.contoso.com\contoso-contoso-dc-CA
Help	Back Next Cancel



8. Enter Enterprise Domain credentials.

#### Figure 10-48: Certification Authority Account

Certificate Request
Certification Authority Account
<ul> <li>Specify alternate credentials for the certification authority.</li> <li>User name:</li> <li>administrator</li> </ul>
Dacsword
Help Back Next Cancel

9. Click Next.

#### Figure 10-49: Specify Alternate Certificate Template

3	Certificate Request	x			
	Specify Alternate Certificate Template				
By default different c	a Lync Server certificate request will use the WebServer certificate template. To specify a ertificate template, select the following check box.				
Use alt Certific	ernate certificate template for the selected certification authority cate template name:	-			
Note: The requireme	custom template must be installed on the certification authority (CA), and must meet the nts for Lync Server certificates.				
The templ For details	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** 

5	Certificate Request	x
Ç	Name and Security Settings	
Type a n Note: Th automat Friendly	ame for the new certificate. The name should be easy for you to refer to and remember. e friendly name should not be confused with the subject name which will be determined cally based on the certificate's usages on this computer. name:	
ACSFE		
Bit lengt 2048	the certificate's private key as exportable	
Help	Back Next Cancel	

**11.** Enter the organization details, and then click **Next** 



5	Certificate Request	x
ر ا	Organization Information	
Enter your o organization For more in	organization's name and your organizational unit. This is typically the legal name of your n and the name of your division or department. formation see the certification authority's website.	
Organizatio	n:	
Contoso		
Organizatio	nal unit:	
Contoso		
Help	Back Next Cance	:

**12.** Enter the Geographical information, and then click **Next**.

Certificate Request	x
Geographical Information	
Country/Region:	
State/Province:	
Victoria	
City/Locality:	
Melbourne	
State/Province and City/Locality must be completed. Official names cannot contain abbreviations.	
Help Back Next Cancel	

#### Figure 10-52: Geographical Information

**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

Certificate Request	x
Subject Name / Subject Alternative Names	
The following will be automatically populated for the subject name and subject alternative name.	
Subject name:	
ACS-UC-FE.ACS-Unified-Communications.net	
Subject alternative name:	
ACS-UC-FE.ACS-Unified-Communications.net	^
meet.contoso.com	
LyncdiscoverInternal.contoso.com	=
ewslync.contoso.com	
Lyncdiscover.contoso.com	~
Help Back Next Canc	el

14. Enable any SIP domains, and then click Next

#### Figure 10-54: SIP Domain Setting on Subject Alternative Names

2	Certificate Request	x	
	SIP Domain setting on Subject Alternative Names		
If your d names fo • Your d • Your d Configure	eployment meets any of the following conditions, you may need additional subject alternative or each configured SIP domain: eployment uses automatic sign-in without DNS SRV configuration eployment performs strict domain matching eployment includes devices that run Lync Phone Edition red SIB domains		
	toso com		
Select one or more SIP domains for which a sip. <sipdomain> entry is to be added to the subject alternative names list.</sipdomain>			
Help	Back Next Cancel		

**15.** Configure additional subject alternative names, and then click **Next**.

Figure 10-55: Configure Additional Subject Alternative Names

5	Certificate Request	×	
	Configure Additional Subject Alternative Names		
Specify any additional subject alternative names to be added to the existing list of subject alternative names.			
		Add	
		Remove	
		Clear All	
Help	Back Next	Cancel	

16. Click Next.

-		-	
	Certificate R	lequest	
Certific	cate Request Summary		
o generate a reque	est with the following information, cl	ick Next.	
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		

### Figure 10-56: Certificate Request Summary

## 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.



2	Certificate Request	x
Б	recuting Commands	
CSCertificat Create a cer Issued thum "Default,We CONTOSO- No changes Creating ne CSCertificat Request-C Detailed res CSCertificat	e-ge4a876a-ee4b-4edd-9039-539458a9f2d7.xml*. tificate request based on Lync Server configuration for this computer. ibprint "757522E95180F39DD6D63973ACC7E935578DD6E* for use bServicesInternal,WebServicesExternal" by "contoso-DC.internal.contoso.com/contoso- DC-CA". were made to the Central Management Store. w log file "C:\Users\Administrator.ACSLync\AppDat\Local\Temp\1\Request- e-[2013_05_01][15_20_03].html*. SCertificate" processing has completed successfully. ults can be found at "C:\Users\Administrator.ACSLync\AppDat\Local\Temp\1\Request- e-[2013_05_01][15_20_03].html*.	
Task status: ( Request Cert Help	ificate View Lo Back Next Cance	× yg

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	Certificate Request	×
¢	Online Certificate Request Status	
A certif local ce	icate with thumbprint 757522E951369F39D6D6E3973ACC7E9535F8DD6E has been a rtificate store.	dded to the
✓ Assig Note: If task in the View Ce	gn this certificate to Lync Server certificate usages. you choose not to assign the certificate now, you can assign it at a later time by usin he Certificates wizard. rtificate Details	g the Assign
Help	Back Finish	Cancel

2. Continue the wizard to automatically assign the certificate to the Skype for Business roles on the server.

Back

Next

Cancel

Figure 10-59. Certificate	Assignment	
2 Certificate Assignme	nt	×
Certificate Assignment		
Assign the returned certificate to the Lync Server usages on this View Certificate Details	server.	

#### Figure 10-59: Certificate Assignment

Help

#### Figure 10-60: Executing Commands

6	Certificate Assignment	x
	Executing Commands	
Default Commu DC=coi The foll WebSet Commu DC=coi The foll WebSet Commu DC=coi	757522E951369F39D6D6E3973ACC7E9535F8DD6E ACS-UC-FEACS-Unified- inications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso, m 72000000044A230E821BA5ECE300000000004 owing certificate was assigned for the type "WebServicesInternal": vicesInternal: 757522E951369F39D6D6E3973ACC7E9535F8DD6E ACS-UC-FEACS-Unified- inications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso, m 7200000044A230E821BA5ECE300000000004 owing certificate was assigned for the type "WebServicesExternal": vicesExternal: 757522E951369F39D6D6E3973ACC7E9535F8DD6E ACS-UC-FEACS-Unified- inications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso, m 7200000044A230E821BA5ECE300000000004	< III >
Task stat Assign C	us: Completed. ertificate	3
Help	Back Finish Cancel	

**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 10-01. Delayed of infineutate requests
-----------------------------------------------

l@	
Ç	Delayed or Immediate Requests
Do you v certificati	vant to prepare a certificate request to be sent later, or do you want to send it now to an online ion authority?
⊖ Send	the request immediately to an online certification authority
Prepa	are the request now, but send it later (offline certificate request)
Uala	Park Nath Count
Неір	Back Next Cancel

6. Specify a file name to store the certificate request.



Certificate Request	x
Certificate Request File	
Specify the full path and file name of the certificate signing request (CSR) file that you want	to create.
File name:	
C:\temp\ACSedgeintreq.csr.req	Browse
Help Back Next	Cancel

Certificate Request	X				
Name and Security Settings					
Type a name for the new certificate. The name should be easy for you to refer to and remember. Note: The friendly name should not be confused with the subject name which will be determined automatically based on the certificate's usages on this computer.					
ACSEdgeInt					
Bit length:       2048       Mark the certificate's private key as exportable					
Help Back Next Cano	el				

#### 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**.

<b>a</b>	certsrv - [Certification A	Authority (Local)\contoso-CONTOSO-DC-CA]					
File Action View Help							
🧇 🏟 🖄 🗐 🗟 🗟	⇔ ⇒ 2 🖫 @ 🕞 🛛 > ■						
Certification Authority (	(Local) Name						
contoso-CONTOSC	All Tasks 🕨	Start Service					
	View 🕨	Stop Service					
	Refresh	Submit new request					
	Export List	Back up CA					
	Properties	Restore CA					
	Help	Renew CA Certificate					
Contains actions that can be	e performed on the item.						

#### Figure 10-64: Manually Generating a Certificate – All Tasks

3. Open the request file and click **Open**.

	<u> </u>		
	Open Request File		x
🕒 🕀 🔻 🚺	« Local Disk (C:) + Temp v 🖒 Searc	:h Temp	Q
Organize 🔻 New	folder		
🔆 Favorites	^ Name	Date modified	Туре
Desktop Downloads	☐ ACSedgeintreq.csr.req	1/05/2013 3:36 PM	REQ File
➢ Libraries ➢ Documents ➢ Music ➢ Pictures ☑ Videos			
	File name:	uest Files (*.req; *.txt; *.c Open Can	> :mc ♥ cel

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

	Save Certi	ficate			x
🔄 🕘 = 🕇 📕 «	Local Disk (C:) 🕨 Temp	~ ¢	Search Temp		<i>م</i>
Organize 🔻 New fold	er			• ==	-
-	^ Name		Date mod	dified	Туре
Libraries	🔄 ACSEdgeInt		1/05/2013	3 3:39 PM	Security C
<ul> <li>J Music</li> <li>S Pictures</li> <li>S Videos</li> </ul>					
🖳 Computer					
•	< <	Ш			>
File name: AC	SEdgeInt				~
Save as type: X.50	09 Certificate (*.cer; *.crt; *.der)				~
) Hide Folders			Save	Can	cel

## 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.

Select a Lync Server Certificate Typ Certificate	e and	then select a task. Expand the Friendly Name	Certificate Type to perform adva Expiration Date	Location	usage tasks. Request
<ul> <li>Edge internal</li> <li>External Edge certificate (pu</li> <li>SIP Access Edge external</li> <li>Web conferencing Edge</li> <li>A/V Edge external</li> <li>XmppServer</li> </ul>		Edge-Ext Edge-Ext Edge-Ext Edge-Ext Edge-Ext	26/04/2015 2:57:28 PM 26/04/2015 2:57:28 PM 26/04/2015 2:57:28 PM 26/04/2015 2:57:28 PM	Multiple Local Local Local	Assign Remove View
Kefresh Im	port C	III ertificate Process Pending Ce	rtificates	>	Close

#### Figure 10-67: Certificate Wizard

3. Specify the certificate file copied from the CA, and then click **Next**.

#### Figure 10-68: Import Certificate

5	Import Certificate	x
	Import Certificate	
Select Cert C:\temp\/	ificate file (.p7b .pfx .cer file) ACSEdgeInt.cer Browse	·
Certific Passwo	ate file contains certificate's private key ord:	
Help	Back Next Cance	ł

4. Click Next.

	<b>J · · · · · · · · · · · · · · · · · · ·</b>						
5	Import Certi	ficate		x			
	Import Certificate Summary						
To import the certi	ficate to the local store, click Next.						
Property	Value						
File Name Contains Private Key	C:\temp\ACSEdgeInt.cer False						
Help		Back	Next	Cancel			

Figure 10-69: Import Certificate Summary

5. Click Finish.

## Figure 10-70: Executing Commands

5	Import Certificate	x
	Executing Commands	
R3m013 CSCertii Creating f91b-48 Import No chai Creating [2013_0 "Import Detailed CSCertii	SuppOrt -Verbose -Report "C:\Users\Administrator\AppData\Local\Temp\Import- icate-[2013_05_01][15_57_13].html" g new log file "C:\Users\Administrator\AppData\Local\Temp\Import- bc-b0d2-360ccdf89d99.xml". the certificate response or read the certificate from file. ges were made to the Central Management Store. g new log file "C:\Users\Administrator\AppData\Local\Temp\Import-CSCertificate- 5_01][15_57_13].html". -CSCertificate" processing has completed successfully. I results can be found at "C:\Users\Administrator\AppData\Local\Temp\Import- icate-[2013_05_01][15_57_13].html".	< 111
Task stat Import C	us: Completed. ertificate View Lo	9
Help	Back Finish Cancel	

## **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

6	Certificate Assignment	X
	Certificate Assignment	
Assign a	certificate for the Edge internal(Edge internal) Lync Server usages.	
Help	Back Next Cancel	

2. Select the certificate just imported to the certificate store.

k	6	Certificate Assi	ignment		x
	Certificate Store				
	Select a certificate from the local certi	ficate store.			
	Friendly Name	Issued On	Issued By		^
	ACSEdgeInt	1/05/2013 3:51:19 PM	CN=contoso- CONTOSO-DC- CA, DC=internal, DC=contoso, DC=com		=
	Edge-Ext	26/04/2013 2:57:28 PM	CN=ACS- Unified- Communication s-ACS-UC-DC- CA, DC=ACS- Unified-		~
	View Certificate Details				
[	Help		Back	Next Cance	:I

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

<b>B</b>	Certificate Ass	ignment X				
Certificate Assignment Summary						
To assign the follow	ving certificate to the Lync Server usa	ges listed, click Next.				
Friendly Name	ACSEdgeInt					
Thumbprint	7B26E5BB0D63AC1AE0A09FDD310 FA006C5FB003D					
Certificate Use	Edge internal					
Issue date	1/05/2013 3:51:19 PM					
Expiration date	1/05/2015 3:51:19 PM					
Subject Name (SN)	ACS-UC-Edge.ACS-Unified- Communications.net					
Help		Back Next Cancel				

5. Click Finish.

#### Figure 10-74: Executing Commands

6	Certificate Assignment	x					
E E	Executing Commands						
> Assign C Set-CSCert Confirm:\$f [16_05_44] The follow Internal: 7I Communic 72000000	> Assign Certificate Set-CSCertificate -Type Internal -Thumbprint 7B26E58B0D63AC1AE0A09FDD310FA006C5FB003D - Confirm:\$false -Report "C:\Users\Administrator\AppData\Local\Temp\Set-CSCertificate-[2013_05_01] [16_05_44].html" The following certificate was assigned for the type "Internal": Internal: 7B26E58B0D63AC1AE0A09FDD310FA006C5FB003D ACS-UC-Edge.ACS-Unified- Communications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso, DC=com 7200000070FDDAC2D8F70E75600000000007						
Task status: Completed.							
Assign Cert	ficate View Lo	9					
Help	Back Finish Cance						

- 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

ß			Certificate \	Wizard		x
:	Select a Lync Server Certificate Type	and	then select a task. Expand the	Certificate Type to perform adva	inced certificate	usage tasks.
	Certificate		Friendly Name	Expiration Date	Location	Request
	<ul> <li>Default certificate</li> </ul>	✓	Multiple	1/07/2015 5:02:09 PM	Local	Assian
	Server default	•	ACSFEv2	4/07/2015 1:28:35 PM	Local	
	Web services internal	•	ACSFEv2	4/07/2015 1:28:35 PM	Local	Remove
	<ul> <li>Web services external</li> </ul>	٩	ACS FE	1/07/2015 5:02:09 PM	Local	View
	✓ OAuthTokenIssuer	✓	ACS FE OATI	1/07/2015 5:02:11 PM	Local	
					/	
	Help Refresh Impo	ort Ce	rtificate Process Pending Ce	ertificates		Close



6			Certificate Wiz	ard			x
5	Select a Lync Server Certificate Type	and	then select a task. Expand the Cer	tificate Type to perform adva	anced certificate	usage tasks.	
	Certificate		Friendly Name	Expiration Date	Location	Request	
	✓ Edge internal	~	ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local	Assign	
	<ul> <li>External Edge certificate (pu</li> </ul>	✓	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local	Remove	-
	SIP Access Edge external	•	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local	TREMIOVE	_
	Web conferencing Edge	•	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local	View	
	A/V Edge external	•	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local		
	XmppServer	٩	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local		
	<		ш		>		
[	Help Refresh Impo	ort Ce	ertificate Process Pending Certific	ates		Close	

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, <u>https://dial-in.contoso.com</u>).

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.

Component	Subject Name	Subject Alternative Name Entries/Order	Certification Authority (CA)	Enhanced key usage (EKU)	Comments
Single consolidated Edge	access.contoso.com	webcon.contoso.co m 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

#### 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	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	Iswebext.contoso.co m 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 Isweb.contoso.net Iswebext.contoso.co m 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 EKU 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

You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A shade part of the component will be installed. To see what's included Details.	d box means that only d in a component, click
Components:	
🗹 😰 Certificate Services	1.8 MB 🔼
🔲 🛄 E-mail Services	1.1 MB
🔲 🚳 Fax Services	7.9 MB
🖂 💬 Indexing Service	0.0 MB
🖂 🚎 Internet Explorer Enhanced Security Configuration	оомв 🗵
Description: Installs a certification authority (CA) to issue certi public key security programs.	ficates for use with
	Details
Total disk space required: 0.3 MB	

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

U U	
Certificate Services	×
To add or remove a component, click the check box. A shaded box of the component will be installed. To see what's included in a compo Sub <u>c</u> omponents of Certificate Services:	means that only part onent, click Details.
🗹 📴 Certificate Services CA	0.4 MB 🔼
Certificate Services Web Enrollment Support	1.4 MB

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:

	<u> </u>
Add Roles Wizard	×
Before You Begin	As a contract of the second se
Before You Begin Server Roles Confirmation Progress Results	This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site. Before you continue, verify that: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The latest security updates from Windows Update are installed If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again. To continue, click Next. Skip this page by default
	< Previous Next > Install Cancel

Figure 10-79: Before You Begin

4. Select Active Directory Certificate Services:

Figure 10-80: Introduction to Active Directory Certificate Services





5. Select the Certification Authority, the Certification Authority Web Enrolment as well as the Online Responder.



Add Roles Wizard		×
Select Role Serv	ices	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key	Select the role services to install for Active Directory Certificate Role services:	Services: Description: Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

6. Select Enterprise.



Add Roles Wizard	×
Specify Setup Ty	pe
Before You Begin Server Roles AD CS Role Services	Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA. C Enterprise Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.
Setup Type CA Type Private Key Cryptography CA Name Certificate Request Certificate Database	Certainales. C Standaione Select this option if this CA does not use Directory Service data to issue or manage certificates. A standaione CA can be a member of a domain.

#### 7. Select Root CA.

Figure	10-84:	Specify	CA	Туре
--------	--------	---------	----	------

Add Roles Wizard	X
Specify CA T	Туре
Before You Begin Server Roles AD CS Role Services	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 installion the first or only certification authority in a public key infrastructure.
Setup Type CA Type Private Key	Subordinate CA     Select this option if your CA will obtain its CA certificate from another CA higher in a public key
Cryptography CA Name	infrastructure.

#### 8. Select Create a New Private Key.



**9.** Use the default Cryptography, Common name and Distinguished name suffix in the next two pages.

#### Figure 10-86: Configure Cryptography for CA

ld Roles Wizard	
Configure Cr	yptography for CA
efore You Begin erver Roles D CS Role Services Setup Type CA Type Divate Kevi	To create a new private key, you must first select a <u>croptographic service provider</u> , <u>hash algorithm</u> , 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): Key character length: RSA#Microsoft Software Key Storage Provider V issue Select the hash algorithm for signing certificates issued by this CA:
Cryptography	sho1
CA Name	md4
Validity Period	
Veb Server (IIS)	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)
Confirmation	



Add Roles Wizard		×
Configure CA	Name	
Before You Begin Server Roles AD C5 Role Services Setup Type CA Type	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. Common name for this CA: orshost-UYNCRTM-CA Distinguished name suffix: DC=ocshost,DC=ni	_
Cryptography CA Name	Preview of distinguished name:	
Validky Period Certificate Database Confirmation	ON=ocshost-LYNORTM-CA,DC=ocshost,DC=nl	

**10.** Choose a Validity Period for the CA.

Figure	10-88:	Set	Validity	Period
--------	--------	-----	----------	--------

Add Roles Wizard	×
Set Validity P	eriod
Before You Begin Server Roles AD CS	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.
Role Services Setup Type CA Type Private Key Cryptography	Select validity period for the certificate generated for this CA: 5 Years CA expiration Date: 1/26/2016 1:37 PM Note that CA will issue certificates valid only until its expiration date.

**11.** Keep the default data location.

F	igure 10-89: Configure Certificate Database	
Add Roles Wizard		X
Configure Ce	ertificate Database	
Before You Begin Server Roles AD CS	The certificate database records all certificate requests, issued certificates, and revolv certificates. The database log can be used to monitor management activity for a CA. Certificate database location:	ed or expired
Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period	C:\Windows\system32\CertLog Use existing certificate database from previous installation at this location Certificate database log location: C:\Windows\system32\CertLog	Browse

**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.

Add Roles Wizard		×
Confirm Installation	on Selections	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	To install the following roles, role service	as, or features, click Install. ges below arted after the installation completes. ervices if this computer cannot be changed after Certification Authority has Enterprise Root RSA#Microsoft Software Key Storage Provider SHA1 2048 Disabled 1/26/2016 2:20 PM Ctiwindowslaystem32\CertLog Ctiwindowslaystem32\CertLog Ctiwindowslaystem32\CertLog Ctiwindowslaystem32\CertLog
	, Print, e-mail, or save this information	
		<pre></pre>

#### 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

<b>a</b>	Add Roles and Features Wizard
Before you begin Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard  DESTINATION SERVER Contoso-DC contoso com  This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.  To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed:  The Administrator account has a strong password  Network settings, such as static IP addresses, are configured The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the wizard,
	To continue, click Next.       Skip this page by default       < Previous

# Figure 10-92: Select Installation Type

<b>b</b>	Add Roles and Features Wizard	_ <b>_</b> X
Select installation	on type	DESTINATION SERVER Contoso-DC.contoso.com
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select the installation type. You can install roles and features on a runn machine, or on an offline virtual hard disk (VHD). Role-based or feature-based installation Configure a single server by adding roles, role services, and features Configure a single server by rultual Desktop Infrastructure (VDI) Install required role services for Virtual Desktop Infrastructure (VDI) or session-based desktop deployment.	ing physical computer or virtual to create a virtual machine-based
	< Previous Next >	Install

# Figure 10-93: Select Destination Server

<b>b</b>	Add Roles and Features Wizard
Select dest	ination server Contoso-DC.contoso.com
Before You Begi Installation Type Server Selection	Select a server or a virtual hard disk on which to install roles and features.      Select a server from the server pool     Select a virtual hard disk
Server Roles Features Confirmation	Server Pool Filter:
Results	Name         IP Address         Operating System           Contoso-DC.contoso.com         10.253.2.161,1         Microsoft Windows Server 2012 Standard
	1 Computer/ol found
	This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
	< Previous Next > Install Cancel

2. Select Active Directory Certificate Services:

#### - 🗆 X Add Roles and Features Wizard DESTINATION SERVER Select server roles Contoso-DC.internal.cont Select one or more roles to install on the selected server. Before You Begin Installation Type Roles Description Server Selection Active Directory Certificate Services ~ Active Directory Certificate Services (AD CS) is used to create certification authorities and related Server Roles Active Directory Domain Services (Installed) Features role services that allow you to issue and manage certificates used in a Active Directory Federation Services Active Directory Lightweight Directory Services variety of applications. Active Directory Rights Management Services Application Server DHCP Server DNS Server (Installed) Fax Server Þ ✓ File And Storage Services (Installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services < Previous Next > Install Cancel

#### Figure 10-94: Select Server Roles

3. Click Add Features.

#### Figure 10-95: Add Features that are Required

Add Roles and Features Wizard	×
Add features that are required for Active Director Certificate Services?	ory
The following tools are required to manage this feature, but have to be installed on the same server.	do not
Remote Server Administration Tools	
<ul> <li>Role Administration Tools</li> </ul>	
<ul> <li>Active Directory Certificate Services Tools</li> </ul>	
[Tools] Certification Authority Management T	Fools
<ul> <li>Include management tools (if applicable)</li> </ul>	
Add Features	Cancel

Follow the instructions on the screens as shown below. 4.



#### Figure 10-96: Select Features

#### 5. Click Next.



6. Click Next.

#### Figure 10-98: Select Role Services

	Add Roles and Features Wizard	
Select role servic	es	DESTINATION SERVER Contoso-DC.internal.contoso.com
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services Confirmation Results	Select the role services to install for Web Server (IIS) Role services	Description Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
	ODBC Logging  Request Monitor	ladall <b>Canad</b>

7. Click Install to complete the Wizard.



# **10.12.3.1 Configure the Certificate Services**

You must now configure the Active Directory Certificate Services for correct operation.

- 1. In the Server Manager, select AD CS.
- 2. Click **More...** in the top right corner.

<b>b</b>	Server Manager		. 0	x
Server Ma	anager 🕻 AD CS 🔹 🕫 🏹 Manage	Tools View	v He	lp
Eccal Server     Local Server     All Servers     All Servers     AD OS     DNS     DNS     File and Storage Services ▷	SERVERS         All servers [1 total         ▲ Configuration required for Active Directory Certificate Services at CONTOSO-DC         Filter       P         (ii) ← (ii) ← (iii) ←         Server Name       IPv4 Address         Manageability       Last Update         CONTOSO-DC       10.253.2.161,192.168.0.10         Online - Performance counters not started       30/04/2013.3.1022 PM	TASK <u>More</u> Windows Activatio	S V X On 07-AA1	H
	K     III   EVENTS All events   0 total	TASK	> (S •	
	Filter     P     Image: The second se		$\odot$	
		Re 11 6	3:11 PM 30/04/20	VI 013

#### 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

Ē.	Server Manage	er	_	o x
Server M	anager • AD CS	- ©   P	Manage Tools View	Help
Dashboard Local Server All Servers All Servers AD CS AD DS DNS File and Storage Services	SERVERS All servers [1 total Configuration required for Active Directory Certificate Filter P (2) • Server Name IPv4 Address Manageability CONTOSO-DC 10.2532.161,192.168.0.10 Online - Perfor	I Services at CONTOSO-DC (€) ▼ Last Upda mance counters not started 30/04/20	TASKS           More_         (           ste         Windows Activation           13 3.10.22 PM         00183-80850-73807	× × •
	C EVENTS All events [0 total		TASKS	>
	Filter     P     Image: Control of the second secon	(£) ▼ e		9
			Pa 12 da 30	3:11 PM 0/04/2013

**4.** Follow the instructions on the screens below.

### Figure 10-102: AD CS Configuration - Credentials

<b>a</b>	AD CS Configuration
Credentials	DESTINATION SERVER Contoso-DC.internal.contoso.com
Credentials Role Services Confirmation Progress Results	Specify credentials to configure role services To install the following role services you must belong to the local Administrators group: • Standalone certification authority • Certification Authority Web Enrollment • Online Responder To install the following role services you must belong to the Enterprise Admins group: • Enterprise certification authority • Certificate Enrollment Policy Web Service • Certificate Enrollment Web Service • Network Device Enrollment Service Credentials: Contoso\Administrator Change
	More about AD CS Server Roles
	< Previous Next > Configure Cancel

## 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

<b>b</b>	AD CS Configuration				
Setup Type	DESTINATION SERVER Contoso-DC.internal.contoso.com				
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	<ul> <li>Specify the setup type of the CA</li> <li>Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.</li> <li>     enterprise CA     Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.     </li> <li>     Standalone CA     Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD     DS and can be used without a network connection (offline).     </li> </ul>				
More about Setup Type					
	< Previous Next > Configure Cancel				



#### Figure 10-105: AD CS Configuration – CA Type

Figure 10-106: AD CS Configuration – Private Key

<b>b</b>	AD CS Configuration
Private Key	DESTINATION SERVER Contoso-DC.internal.contoso.com
Credentials Role Services	Specify the type of the private key
Setup Type CA Type Private Key	<ul> <li>O generate and issue certificates to clients, a certification authority (CA) must have a private key.</li> <li>Create a new private key</li> <li>Use this option if you do not have a private key or want to create a new private key.</li> </ul>
Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	<ul> <li>Use existing private key</li> <li>Use this option to ensure continuity with previously issued certificates when reinstalling a CA.</li> <li>Select a certificate and use its associated private key</li> <li>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.</li> <li>Select an existing private key on this computer</li> <li>Select an existing private key on this computer</li> <li>Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.</li> </ul>
	More about Private Key

Cryptography f	or CA	Cont	DESTINATION SERVER
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider		Key length:
Private Key	Select the hash algorithm for signing certificates issued	by this CA:	
Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	SHA256 SHA384 SHA512 SHA1 MD5 Allow administrator interaction when the private key	is accessed	by the CA.
	More about Cryptography		

Figure 10-107: AD CS Configuration – Cryptography for CA

#### Figure 10-108: AD CS Configuration – CA Name



<b>B</b>	AD CS Configuration				
Validity Period	DESTINATION SERVER Contoso-DC.internal.contoso.com				
Credentials	Specify the validity period				
Role Services					
Setup Type	Select the validity period for the certificate generated for this certification authority (CA):				
СА Туре	5 Years 💌				
Private Key	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.				
Cryptography CA Name					
Validity Period					
Certificate Database					
Confirmation					
More about Validity Period					
	< Previous Next > Configure Cancel				

## Figure 10-109: AD CS Configuration – Validity Period



2	AD CS Configuration	_ <b>_</b> X
CA Database	Cor	DESTINATION SERVER
Credentials Role Services	Specify the database locations	
Setup Type	Certificate database location:	
СА Туре	C:\Windows\system52\CertLog	
Private Key	Certificate database log location:	
Cryptography	C:\Windows\system32\CertLog	
CA Name		
Validity Period		
Certificate Database		
Confirmation		
Progress		
Results		
	Mare about CA Database	
	More about CA Database	
	< Previous Next >	Configure Cancel
6. Click **Configure** to complete the wizard.

	AD CS Con	figuration – 🗖 🗙
Confirmation		DESTINATION SERVER Contoso-DC.internal.contoso.com
Credentials Role Services	To configure the following roles, <ul> <li>Active Directory Certificat</li> </ul>	, role services, or features, click Configure. e <b>Services</b>
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress	Certification Authority CA Type: Cryptographic provider: Hash Algorithm: Key Length: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location:	Enterprise Root RSA#Microsoft Software Key Storage Provider SHA1 2048 Disabled 30/04/2018 3:16:00 PM CN=internal-CONTOSO-DC- CA,DC=internal,DC=contoso,DC=com C:\Windows\system32\CertLog
	Certificate Database Log Location:	C:\Windows\system32\CertLog
		< Previous Next > Configure Cancel

Figure 10-111: AD CS Configuration - Confirmation

7. Click Close.

<b>b</b>	AD CS Configuration	_ <b>D</b> X
Results		DESTINATION SERVER Contoso-DC.internal.contoso.com
Credentials	The following roles, role services, or features w	ere configured:
Role Services	<ul> <li>Active Directory Certificate Services</li> </ul>	
Setup Type	Certification Authority	Configuration succeeded
СА Туре	More about CA Configuration	configuration succeeded
Private Key	Castification Authority Web Frankerst	Confirmation and ad
Cryptography	More about Web Enrollment Configuration	Configuration succeeded
CA Name	······	
Validity Period	Online Responder	Configuration succeeded
Certificate Database	Nore about OCSP Conliguration	
Confirmation		
Progress		
Results		
	< Previous	Next > Close Cancel

### 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 <u>http://www.audiocodes.com/swactivation</u>.

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 <u>http://localhost:9999/swagger/</u>.
- 2. To get the System ID go to License > GET /License/machineld > Try it out!..

\varTheta swagger	http://localhost:9999/swagger/docs/v1	api_key	Explore
RestServer API			
AppConfig		Show/Hide   List Operations   Exp	and Operations
License		Show/Hide List Operations Exp	and Operations
GET /license/machinel	d	Get machine ID that is used for cre	eating a license
Response Class (Status 2 string Response Content Type ap Try it out!	200) plication/json 🗸		
GET /license		Get all lice	nsed properties
POST /license		Applies new license. No r	estart required

### 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).

O http://localhost-9999/owagger/ui/inc. Q > C O Suppose III Y	
Residence Ari	
AppConfig	Show/Hide   List Operations   Expand Operations
License	Show/Hide List Operations Expand Operations
GET /license/machineld	Get machine ID that is used for creating a license
Response Class (Status 200) string Response Content Type application/json V Ty it out! Hide Response Curl curl -X GETheader 'Accept: application/json' 'http://localhost:9999/license	z/machineId'
Request URL	
http://localhost:9999/license/machineId	
Response Body	
"69a31e1f74b45264cdabe367d014961745157667"	
Response Code	
200	
Response Headers	

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

Enter a product key
Your product key should be on the box that the Windows DVD came in or in an email that shows you bought Windows.
The product key looks similar to this: PRODUCT KEY: 30000-300003-300003-300003-300003
Product key
Dashes will be added automatically
Cancel



**Note:** It is recommended that you photograph or copy the Windows product key slickers 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: <u>https://technet.microsoft.com/en-us/library/dn518328.aspx</u>



**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

Local Server         Computer name         ACS-DC         Call initialid updates         Noner           AU Servers         Domain         Active Computer name         ACS-DC         Call initialid updates         Domain         Domain <t< th=""><th>Dashboard</th><th>PROPERTIES For ACS-DC</th><th></th><th></th><th>TASKS</th></t<>	Dashboard	PROPERTIES For ACS-DC			TASKS
A D DS     AD DS	Local Server     All Servers     AD CS	Computer name Domain	ACS-DC hostlync.com.au	Last installed updates Windows Update Last checked for updates	Never Download updates only, using a man. Never
Operating system version Microsoft Windows Server 2012 R2 Standard Processors Intel(R) Core[1M] i7-3612QE CPU (# 2 Core (M) i7-3612	ar AD DS DNS magnetic field of the services ▷ magnetic field of the services ○ magnetic field of the se	Windows Firewall Remote Dasktop NIC Teaming Ethernet VEthernet (DMZ) vEthernet (LAN)	Domain: On Enabled Enabled Disabled Nat connected IPv4 address assigned by DHCP, IPv6 enabled 10253.0.154, IPv6 enabled	Windows Error Reporting Customer Experience Improvement Program IE Enhanced Security Configuration Time zone Product ID	Off Not participating Off (UTC + 10:00) Canberra, Melbourne, Sy Not activated
		Operating system version	Microsoft Windows Server 2012 R2 Standard	Processors	Intel(R) Core(TM) i7-3612QE CPU @ 2

89	Windows Up	date 🗕	
(a) < ↑ (Souther the second secon	System and Security   Windows	s Update v C Search Control Panel	٩
Control Panel Home Check for updates Change settings View update history Restore hidden updates	Windows Update You're set t No updates are Most recent check for updates: Updates were installed: You receive updates:	o automatically download updates available. Never Never Managed by your system administrator Check online for updates from Windows Update	0
See also Installed Updates			

### Figure 11-8: Checking for New Updates

### Figure 11-9: Checking for New Updates

339	Windows Up	date		_ <b>D</b> X
🍥 💿 🔻 🕈 🚱 ד Control Panel 🕨	System and Security   Windows	Update v 🔿	Search Control Pan	el 🔎
Control Panel Home Check for updates	Windows Update			Ø
Change settings View update history Restore hidden updates	Checking for u	pdates		
	Most recent check for updates: Updates were installed: You receive updates:	Never Never Managed by your syste Check online for updat	m administrator es from Windows Update	
See also Installed Updates				

<b>13</b>	Windows Up	date	L_	□ X
🍥 💿 🔻 🕈 🐼 🕨 Control Panel 🕨	System and Security   Windows	s Update v 🖒	Search Control Panel	Q
Control Panel Home Check for updates Change settings View update history Restore hidden updates	Windows Update You're set t 60 important u available Most recent check for updates: Updates were installed: You receive updates:	o automatically down pdates are Today at 10:08 AM Never Managed by your system Check online for updates f	Iload updates administrator rom Microsoft Update	0
See also Installed Updates				

### Figure 11-10: New Updates Found



<b>6</b>	Select upda	ates to install			_ <b>D</b> X
€ ⊚ - 1	🐼 « Windows Update 🕨 Select updates to install		Ý	Ċ	Search Control Panel 🔎
Select the	updates you want to install				
	Name	Size			Security Update for Microsoft Situation (KB2055910)
Important (60)	Silverlight (1) Security Update for Microsoft Silverlight (KB30	12.5 MR			Silverlight (KB3050819)
	Security Update for Nucrosoft Silvenight (kB30 Microsoft SQL Server 2012 (2)     Microsoft SQL Server 2012 Service Pack 2 (KB2 Security Update for SQL Server 2012 Service Pa Visual Studio 2010 (4)	1,015.2 MB 156.4 MB		^	This security update to Silverlight includes fixes outlined in KB 3056819. This update is backward compatible with web applications built using previous versions of Silverlight.
	Security Update for Microsoft Visual Studio 20     Update for Microsoft Visual Studio 2010 Servic     Window: Server 2012 82 (52)	1.7 MB 1.5 MB 9.1 MB 6.6 MB			Published: 5/13/2015 Update is ready to download More information Support information
	Cumulative Security Update for ActiveX Killbit     Cumulative Security Update for Internet Explor     Microsoft.NET Framework 4.5.2 for Windows     Rules Update for RRAS Best Practice Analyzer f     Security Update for Microsoft.NET Framewor     Security Update for Microsoft.NET Framewor	33 KB 33.8 MB 71.6 MB 373 KB 9.9 MB 3.3 MB 322 KB 35.3 MB 4.9 MB			×
	Total selected: 60 imp	ortant updates (1,90	07.8 MB -	1,907	.9 MB) Install Cancel

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 severs at <a href="https://technet.microsoft.com/en-us/library/mt629173.aspx">https://technet.microsoft.com/en-us/library/mt629173.aspx</a>.

## 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.

6	l	ync Server 2013 - Deployment V	Vizard	x
	Lync Server 2013 Welcome to Lync Server deployme	nt.		
Deploy				2
Prepare Active Directory Prepares the Active Directory schen Help ► Install or Update Lync Server Syst Install or update a Lync Server Serv This option installs Lync Server core		na, forest, and domain for Lync Server. tem er deployment member system.	Prepare first Standard Edition server Prepares a single Standard Edition server to host Central Management Service. Note: This task requires local administrator rights. This task does not apply to Standard Edition Servers that are not planned to host the Central Management Service, or for dealourneart that include Enterprise Edition	^
	Configuration store. Note: Before installing a server, you and published. Help ►	Determining deployment sta	all Administrative Tools alls the Administrative Tools to the ent system. deployment requires at least one illation of the Topology Builder.	Ξ
			Deploy Monitoring Reports Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances. First Run Videos Click to view getting started videos.	
			Documentation Click to view the latest Lync Server documentation online for deployment, planning, and operations.	
			Tools and Resources Click to access tools and other resources	~
			Back Exi	t

### Figure 11-12: Skype for Business Deployment Wizard





6	Set Up Lync Server Components
ę	Set Up Lync Server Components
Install an This step	d activate, or deactivate and uninstall Lync Server components based on the topology definition. may take several minutes.
Help	Back Next Cancel

### Figure 11-14: Updating the Skype for Business Deployment

### Figure 11-15: Skype for Business Deployment Results

0	Set Up Lync Server Components	x
¢	Executing Commands	
Checkin Checkin Installin Executir Report [11_01_] Enabling This ste Executir \Admini	g prerequisite MSSpeech_SR_zh-HK_TELEprerequisite satisfied. g prerequisite MSSpeech_SR_zh-TW_TELEprerequisite satisfied. g prerequisite UcmaWorkflowRuntimeprerequisite satisfied. g any collocated databases g PowerShell command: Install-CSDatabase -Confirm:\$false -Verbose -LocalDatabases - 'C:\Jsers\Administrator.Hostlync\AppData\Local\Temp\Install-CSDatabase-[2015_07_25] 32].html" g new roles p will configure services, apply permissions, create firewall rules, etc. ing PowerShell command: Enable-CSComputer -Confirm:\$false -Verbose -Report "C:\Jsers strator.Hostlync\AppData\Local\Temp\Enable-CSComputer-[2015_07_25][11_01_38].html"	< 111
Task stat Bootstrap	us: Completed.	og
Help	Back Finish Cance	2

## **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.

🖄 l 🍃 🕕 🔻 l		Shortcut Tools	Application Tools	Administ	ative Tools	_ □	x
File Home Share	View	Manage	Manage			~	0
🍥 💿 🔻 🕇 🔂 « Syster	n and Sec	urity 🕨 Admini	strative Tools 🕨	v d	, Search Admini	strative Tools	ρ
🔆 Favorites	Name	•		Date modified	Туре	Size	^
E Desktop	🐌 Termi	nal Services		8/23/2013 1:39 AM	File folder		
\rm Downloads	Active	Directory Admir	nistrative Center	8/22/2013 9:50 AM	Shortcut	2 KB	
🔚 Recent places	Active	Directory Doma	ins and Trusts	8/22/2013 4:55 PM	Shortcut	2 KB	
	Active	Directory Modu	le for Windows Po	8/22/2013 4:55 PM	Shortcut	2 KB	
🌉 This PC	Active	Directory Sites a	nd Services	8/22/2013 4:55 PM	Shortcut	2 KB	
3402	Active	Directory Users	and Computers	8/22/2013 4:55 PM	Shortcut	2 KB	_
📬 Network	ADSI E	dit		8/22/2013 4:55 PM	Shortcut	2 KB	-
	Certifica	cation Authority		8/22/2013 4:56 PM	Shortcut	2 KB	
	Comp	onent Services		8/22/2013 4:57 PM	Shortcut	2 KB	
	🛃 Comp	uter Manageme	nt	8/22/2013 4:54 PM	Shortcut	2 KB	
	Defrag	ment and Optin	nize Drives	8/22/2013 4:47 PM	Shortcut	2 KB	
	🖁 DNS			8/22/2013 4:55 PM	Shortcut	2 KB	
	뒴 Event	Viewer		8/22/2013 4:55 PM	Shortcut	2 KB	
	🚮 Group	Policy Manager	nent	8/22/2013 4:56 PM	Shortcut	2 KB	
	🗊 Intern	et Information Se	ervices (IIS) 6.0 Ma	8/22/2013 4:50 PM	Shortcut	2 KB	
	🔒 Intern	et Information Se	ervices (IIS) Manager	8/22/2013 4:50 PM	Shortcut	2 KB	
	🔒 iscsi i	nitiator		8/22/2013 4:57 PM	Shortcut	2 KB	
	Local	Security Policy		8/22/2013 4:54 PM	Shortcut	2 KB	
	DDBC	Data Sources (32	2-bit)	8/22/2013 9:56 AM	Shortcut	2 KB	
	DDBC	Data Sources (64	1-bit)	8/22/2013 4:59 PM	Shortcut	2 KB	
	Perfor	mance Monitor		8/22/2013 4:52 PM	Shortcut	2 KB	~
34 items 1 item selected 1.2	0 KB					8==	

### Figure 11-17: DNS MMC Tool

	Figure 11-18: Setting DNS Server Prope	erties
<u>.</u>	DNS Manager	
File Action	n View Help	
(= ->   2		
🚊 DNS	Name	
D UC-D	C Configure a DNS Septer	
	Create Default Application Directory Partitions	
	New Zone	
	Set Aging/Scavenging for All Zones	
	Scavenge Stale Resource Records	
	Update Server Data Files	
	Clear Cache	
	Launch nslookup	
	All Tasks	
	View +	
	Delete	
	Refresh	
	Export List	
	Properties	
	Help	

5. Select the Forwarders tab and add the IP address of the more authoritative DNS server

#### Close the DNS mmc. 6.

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.

	UC-DC P	rope	erties		?	x
Debug Logging	Event Loggin	g	Monitoring		Sec	curity
Interfaces	Forwarders	A	dvanced	F	Root H	lints
queries for records th	nat this server can	not re	esolve.	Jive L	CNIC	
fee0:0:0.0ffff1		serv	er ruittin able to resolució			
fee0.0.0.ffff2		<un <un< td=""><td>able to resolve?</td><td></td><td></td><td></td></un<></un 	able to resolve?			
fec0:0:0###.:2		<un zUn</un 	able to resolve?			
192 169 0 10		Cont	able to resolves			
Use root hints if r	no forwarders are a	availa	ble		Edit.	
Note: If conditional f	orwarders are defi	ned fo	or a given doma	in, th condi	ey wil tional	be
used instead of serv forwarders, navigate	to the Conditiona	l Forw	arders node in	the s	cope t	tree.

### Figure 11-19: Adding Corporate DNS to Forwarders



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:userl@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:userl@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 Meditation 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 Meditation 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 sentvia 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/downloadsaudiocodes/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:

11			
File Action	View Help		
(n 🔿 🖄			
Hyper-V M	lanager		
UC-N	New	Nitual Machine	
	Import Virtual Machine	Hard Disk	PUI
	Hyper-V Settings	Floppy Disk	
	Virtual Switch Manager	Running	1%

### Figure 15-1: Hyper-V Manager

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



4. Click Next; the following screen appears:



lefore You Begin	Choose a name and location for this virtual machine.	
Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	The name is displayed in Hyper-V Manager. We recommend that you use a name identify this virtual machine, such as the name of the guest operating system or Name: XUM You can create a folder or use an existing folder to store the virtual machine. If folder, the virtual machine is stored in the default folder configured for this serve of Store the virtual machine in a different location Location: C: ProgramData/Microsoft/Windows/Hyper-V/ If you plan to take checkpoints of this virtual machine, select a location thal space. Checkpoints include virtual machine data and may require a large an	e that helps you easily workload. you don't select a er. Brpwse t has enough free rount of space.

- 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



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



<b>b</b>	New Virtual Machine Wizard
Specify Gen	eration
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	<ul> <li>Choose the generation of this virtual machine.</li> <li>Generation 1 This virtual machine generation provides the same virtual hardware to the previous versions of Hyper-V. </li> <li>Generation 2 This virtual machine generation provides support for features such as Secu PXE boot using a standard network adapter. Guest operating systems must Windows Server 2012 or 64-bit versions of Windows 8. Once a virtual machine has been created, you cannot change its generation</li></ul>
	< Previous Next Fir

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
--------	----------------	------------

<b>3</b> .	New Virtual Machine Wizard
Configure N	letworking
Before You Begin Specify Name and Location Specify Generation Assign Memory	Each new virtual machine includes a network adapter. You can configu virtual switch, or it can remain disconnected. Connection: Not Connected Not Connected DMZ
Configure Networking Connect Virtual Hard Disk Installation Options Summary	WOS K
	< Previous Next >

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



Version 0.1

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

				Hyper-	V Manager
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp					
🗢 🄿 🗡 💽 🚺					
Hyper-V Manager	V <u>i</u> rtual Machines				
	Name 📩	State	CPU Usage	Assigned Memory	Uptime
	Edge	Running	0%	8192 MB	2.21:02:58
	EXUM-Connector	Running	0%	6144 MB	2.21:06:41
	Front-End	Running	23%	12288 MB	2.21:04:01
	≝ xUM	Off			
	XUM-Scratch	Off			

2. Right-click on 'xUM', and then select **Settings**.

Figure 15-11: Virtual Machines

Name *	State	CPU Usage	Assigned Memory	1
Edge	Running	0%	8192 MB	(
EXUM-Connector	Running	0%	6144 MB	(
Front-End	Running	18%	12288 MB	(
XUM XUM-Scratch	Connec	t.,		
	Settings	in.		

3. From the 'Settings' drop-down list, select **Processor**.

xUN	4	~
*	Hardware	^
	🚺 Add Hardware	
1	Boot from CD	
1	Memory 6144 MB	
÷	Processor 1 Vir vel 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**.

	Name	State	CPU Usage	Assigned Memory	Uptime	Status
	Edge	Running	0%	8192 MB	02:46:48	
	EXUM-Connector	Running	0%	6144 MB	02:50:31	
	Front-End	Running	19%	12288 MB	02:47:51	
	XUM	Off				
	XUM-Scratch	Off	Connect			
			Settings			
			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.



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

Computer description:	EXUM		
	"Accounting Server".		
Full computer name:	EXUM.cloudbond365.local		
Domain;	cloudbond365.local		
To rename this compute vorkgroup, click Chang	e: Charge its domain or Charge		

6. Change the **Computer Name** and **Domain**, and then click **OK**.

System Properties	
Computer Name/Domain Changes	
'ou can change the name and the membership of this omputer. Changes might affect access to network resources.	omputer
Computer name:	
EXUM	
More Member of	] hge
doudbood 365 local	
O Workgroup:	
O Workgroup:	]

#### 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

		This PC				
	System Properties			✓ ②		
Computer Name Hardware Advanced Remote		System		_ 🗆 X		
Windows uses the following information to identify your computer on the network.		System and Security    System	× ¢	Search Control Panel 🔎		
Computer description:	East automatics: "IIS Production Service" as	ew basic information about your computer				
	"Accounting Server".	ndows edition				
Full computer name:	WIN-0J9GA7GL9SB	Computer Name/Domain Char	nges 🗙			
Workgroup:	WORKGROUP	You can change the name and the membership of	Wind	lows Security		
To rename this computer workgroup, click Change	r or change its domain or Change e.	computer. Changes might affect access to network	Computer Name/Domain Changes			
OK Cancel Apply		Computer name: XUMV2	domain.	an account with permission to join the		
		Full computer name: XUMV2	User name			
		Member of	Password			
		Domain:     cloudbond365 local	Domain: cloud	oond365.local		
		O <u>Workgroup</u> : WORKGROUP	Connect a si	mart card		
	9 item See also	ОК		OK Cancel		

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

Skype for Business Server 2015	x
Skype for Business Server	
To install Skype for Business Server 2015, Core Components and start the Deployment Wizard click Install	d,
Check for Updates?	
<ul> <li>Connect to the internet to check for updates</li> </ul>	
○ Don't check for updates right now	
Specify the location for the installation files. Any additional Skype for Business Server components that you install will also go to this folder Installation Location:	
C:\Program Files\Skype for Business Server 2015 Browse	. ]
Help Install Cancel	

5. Click the **Connect to the internet to check for updates** option, and then click **Install**.

Figure 15-25:End User License Agreement

End User License Agreement	x
License Agreement	
Please read the following license terms carefully	
MICROSOFT SOFTWARE LICENSE TERMS	^
SKYPE FOR BUSINESS SERVER 2015 STANDARD AND ENTERPRISE EDITIONS (NOT FOR RESALE)	
If you licensed Skype for Business Server 2015 through Microsoft's Volume Licensing of MSDN Programs, your use of this software is subject to the terms and conditions of th applicable Program agreements. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.	e Ie
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the	~
✓ I accept the terms in the license agreement	
OK Can	cel

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:



Install or update member system  Deploy > Install Local Configuration Store Installs local configuration store and populates with data from Central Management Store. Prerequisites > Help >  Step 2: Setup or Remove Skype for Business Server Components Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition. Prerequisites > Help >  Determining deployment state Run  Step 3: Request, Install or Assign Certificates Help >  Certificate Run  Step 4: Start Services Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. You can start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server cmdlets. To start the services in a non-user pool, run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server cmdlet on every server in the pool.	G	Skype for Business Server 2015 - Deployment Wizard					
Step 1: Install or update       Image: Step 1: Install Local Configuration Store Installs local configuration store and populates with data from Central Management Store.         Prerequisites >       Help >         Step 2: Setup or Remove Skype for Business Server Components       Run         Step 3: Request, Install or Assign Certificates       Run         Prerequisites >       Help >         Help >       Determining deployment state       Run         Step 3: Request, Install or Assign Certificates       Run         This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.       Run         Step 4: Start Services       Run         Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. You can start the services in a pool with the Skype for Business Server cmdlets.       To start the services in a pool with the Skype for Business Server before you use the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. All the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         To start the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.       V         Back       Exit	Install	or update member system					
Step 1: Install Local Configuration Store       Installs local configuration store and populates with data from Central Management Store.         Prerequisites >       Help >         Step 2: Setup or Remove Skype for Business Server Components       Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition.         Prerequisites >       Help >         Help >       Determining deployment state         Step 3: Request, Install or Assign Certificates         This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.         Prerequisites >       Help >         Help >       Run         Step 4: Start Services       Run         Manual       After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services.         You can start the services in a pool with the Skype for Business Server cmdlets.       To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. All the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         w       Back       Exit	Deploy >	Install or update		¢			
Prerequisites >       Run         Step 2: Setup or Remove Skype for Business Server Components Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition.       Prerequisites >         Help >       Determining deployment state       Run         Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.       Run         Step 4: Start Services       Run         Manual       After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. You can start the services in a pool with the Skype for Business Server cmdlets. To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. All the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         Back       Exit	Step 1:	Install Local Configuration Sto Installs local configuration store	re and populates with data from Central Management Store.	^			
Help       Run         Step 2: Setup or Remove Skype for Business Server Components Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition.       Prerequisites > Help >         Prerequisites > Help >       Determining deployment state       Run         Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.       Run         Step 4: Start Services       Run         Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. You can start the services in a pool with the Skype for Business Server cmdlets. To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. All the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         Back       Exit		Prerequisites >					
Step 2: Setup or Remove Skype for Business Server Components Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition.         Prerequisites > Help >       Determining deployment state       Run         Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.       Run         Prerequisites > Help >       Run         Step 4: Start Services       Run         Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. You can start the services in a pool with the Skype for Business Server cmdlets. To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. To start the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         Back       Exit		Help 🕨	Run				
Step 3: Request, Install or Assign Certificates         This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.         Prerequisites >         Help >         Step 4: Start Services         Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services.         You can start the services in a pool with the Skype for Business Server cmdlets.         To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. To start the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         w       Back       Exit	Step 2:	Setup or Remove Skype for Bu Install and activate, or deactivate definition. Prerequisites > Help >	usiness Server Components e and uninstall Skype for Business Server Components based on the topology Determining deployment state	=			
Help ▶       Run         Step 4: Start Services       Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services. You can start the services in a pool with the Skype for Business Server cmdlets. To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. To start the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.       ▼         Back       Exit	Step 3:	Request, Install or Assign Cert This step starts the Certificate W for this system based on the top Prerequisites	ificates izard. Create certificate request for local system. Install, and assign certificates bology definition.				
Step 4: Start Services         Manual After you've installed Skype for Business Server on all of the servers in the pool, you'll need to start the services.         You can start the services in a pool with the Skype for Business Server cmdlets.         To start the services in a user pool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All the servers in the pool should be running Skype for Business Server before you use the Start-CsPool cmdlet. To start the services in a non-user pool, run the Start-CsWindowsService cmdlet on every server in the pool.         v         Back       Exit		Help >	Run				
Back Exit	Step 4: Manual	<ul> <li>Start Services</li> <li>After you've installed Skype for You can start the services in a pin To start the services in a user por the servers in the pool should b To start the services in a non-user</li> </ul>	Business Server on all of the servers in the pool, you'll need to start the services. ool with the Skype for Business Server cmdlets. ool, connect to one of the servers in the pool and run the Start-CsPool cmdlet. All e running Skype for Business Server before you use the Start-CsPool cmdlet. er pool, run the Start-CsWindowsService cmdlet on every server in the pool.	~			
			Back	Exit			

8. Click Step 1: "Install Local Configuration Store"; the installation runs and upon completion, the following screens appears:

Figure 15-28: Executing Commands	
Install Local Configuration Store	x
Executing Commands	
Enable replica service for the Skype for Business Server computer. Creating new log file "C:\Users\administrator.cloudbond365\AppData\Local\Temp\2\Enable- CSReplica-[2017_10_16][15_59_05].html". "Enable-CSReplica" processing has completed successfully. Detailed results can be found at "C:\Users\administrator.cloudbond365\AppData\Local\Temp\2 \Enable-CSReplica-[2017_10_16][15_59_05].html". > Replicate-CsCmsCertificates Logging status to: C:\Users\administrator.cloudbond365\AppData\Local\Temp\2 \ReplicateCMSCertificates-[2017_10_16][15_59_05].html	< 111
Task status: Completed.	
Bootstrap local machine	g
Help     Back     Finish     Cance	I

- 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/downloadsaudiocodes/Download/AC XUM Install.html

Copy it to C:\xUM InstalltionFiles on the X-UM Connector VM.

 $\geq$ To install the X-UM Connector Application:

Run the X-UM setup file from C:\xUM\_InstalltionFiles\XUMConnector-x.x.x.x.msi. 1.

### Figure 15-29: Run XUMConnector File This PC Local Disk (C:) xUM\_Installtion\_Files $\mathbf{x}$ Name ChangeLog 🚮 UcmaRuntimeSetup KUMConrector-0.1.8.0

The following screen appears:

# × 樹 Audiocodes XUMConnector 0.1.8.0 Setup Welcome to the Audiocodes XUMConnector 0.1.8.0 Setup Wizard The Setup Wizard will install Audiocodes XUMConnector 0.1.8.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard. Back Myst Cancel 2. Click Next.

#### Figure 15-30: XUMConnector File Setup

y.	Audiocodes XUMConnector 0.1.8.0 Setup	×
Destina Click Ne	tion Folder ext to install to the default folder or dick Change to choose another.	
Install A	udiocodes XUMConnector 0.1.8.0 to:	
C:\Prog Chang	ram Files\Audiocodes\XUMConnector\ je	
	Back Cancel	

Figure 15-31: Setup Destination Folder

3. Confirm the Destination Folder, and then click **Next**.

#### Figure 15-32: Ready to Install

₿	Audiocod	ies XUMConnecto	or 0.1.8.0 Setup	- • ×
Ready t	o install Audioco	des XUMConnector	0.1.8.0	S
Click In installa	stall to begin the insta tion settings. Click Car	llation. Click Back to rev icel to exit the wizard.	iew or change any of	your
				F
		Back	Insta	Cancel

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 ypu 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

<u>.a.</u>	Administrator: Activate XUMConnector		-		x		
Please wait Skype for I	t while loading lync module Business Server 2015 identified				^		
Enable-Csl Enable-	Replica -CsReplica						
Activat	te					d	Туре
						25 PM	M Text Doci Applicati
	XUMO	Connector P	ool	DNS	Reso	lve Erro	or X
5	For fu you n 'XUM with Press	ull XUMConnec must add a DN3 IConnector-po value of '10.21. Retry to valida	ctor f S A re ol-s4 26.11 te ne	unctio cord b15-1 w DN	onality, for .cloudt IS recor	oond365. d	local'
	Videos		C	Re	try 🖓		Cancel

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.



nable-CsRepl Enable-CsRepl	lica kenlica	2015 1080	. 11 160		
Activate					d
					25 I
					:23 !
				XUMConnector pool D	NS resolve OK
					OK
	-				UK

3. Click OK.

1005 CT

1.0

Administrator: Activate XUMConnector
<pre>Userifying local replication is up to date Waiting for local replication update 0 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 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication update 20 seconds (up to 10 minutes) Waiting for local replication endpoint 'sip:XUMConnector-s4h15-10exum.com' for 'XUMConnector' on 'XUMConnector-pool-s4h15-1.cloudbond365.local' Application endpoint 'sip:XUMConnector-s4h15-10exum.com' for 'XUMConnector' on 'X WMConnector-pool-s4h15-1.cloudbond365.local' created successfully Verifying local replication is up to date Replication is up to date </pre>
XUMConnector application activated successfully You can safely close this windows
KUMADINIZZZZ
PS C:\Program Files\Audiocodes\XUMConnector\Activation>

Figure 15-38: Activate X-UM Connector – Activation Successful

- 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 <u>UDP multicast address</u>. 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 <u>SIP</u> <u>redirect</u> 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:

269

- 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

